December 29, 2023

By electronic submission to:
Comment Intake— Proposed Rulemaking on Personal Financial Data Rights
c/o Legal Division Docket Manager
Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20552

Re: Notice of Proposed Rulemaking on Personal Financial Data Rights Docket No. CFPB-2023-0052; RIN 3170-AA78

Dear Sirs and Madams:

The Online Lenders Alliance (OLA) welcomes the opportunity to respond to the Bureau's *Notice of Proposed Rulemaking on Personal Financial Data Rights Docket No. CFPB-2023-0052* **.**

About OLA

OLA represents the growing industry of innovative companies that develop and deploy pioneering financial technology, including proprietary underwriting methods, sophisticated data analytics, and non-traditional delivery channels, to offer online consumer loans and related products and services. OLA's members include online lenders, vendors, and service providers to lenders, consumer reporting agencies, payment processors, and online marketing firms.

Fintech companies are at the vanguard of innovative online tools that reach new customers, prevent, and mitigate fraud, manage credit risk, and service loans. As technology evolves and the public's consumer comfort with online financial transactions grows, protecting consumers will be more important than ever. OLA is leading the way to improve consumer protections, with a set of consumer protection standards to ensure that borrowers are fully informed, fairly treated, and use lending products responsibly. To accomplish this, OLA members voluntarily agree to hold themselves to a set of Best Practices, a set of rigorous standards above and beyond the current legal and regulatory requirements. These are standards that OLA members, the industry, and any partners with whom OLA members work use to stay current on the changing legal and regulatory landscape. OLA Best Practices cover all facets of the industry, including advertising and marketing, privacy, payments, and mobile devices. Most importantly, OLA Best Practices

are designed to help consumers make educated financial decisions by ensuring that the industry fully discloses all loan terms in a transparent, easy-to-understand manner.[1]

Much of the innovation undertaken by OLA members has given consumers greater control over their financial future. This is especially the case when it comes to access to capital. Whether purchasing a home, starting a business, financing an education, or even paying for auto repairs, the ability to find and secure credit is often a determining factor in a consumer's financial well-being. Online lenders provide benefits to consumers, particularly those in underserved communities, with fast, safe, and convenient choices that simply are not available through traditional lending markets.

Introduction

While often considered in its infancy, electronic financial data and the need for consumers to access their personal information have been key parts of our nation's financial market for over two decades. The development of these new consumer financial products like mobile apps and online lending has been and will continue to be dependent on consumers' ability to access their data.

The process for accessing this data for app developers or a third party can be very different compared to how mainstream financial institutions access the consumer information they hold. While mainstream institutions have a direct pipeline to this information, third parties or app developers must connect to this data using a designated conduit or additional programs. This can be at times unreliable and restrictive. Ultimately, consumers are the most impacted by these disruptions as their ability to rely on these resources is diminished. This might result in consumers making financial decisions based on incomplete information or seeing their access to innovative online credit or payment products restricted. Regardless of these hurdles, fintech firms have been able to lead the way in developing new products benefiting the consumer.

A lack of security and potential liability exposure is often cited by traditional financial institutions as rationales for limiting third-party access to data. OLA and its members take data security very seriously, which is why we have established Best Practices that stipulate high standards for data safeguards and security. In addition, the same technology that has allowed fintech firms to develop new products has also been instrumental in the development of strong security protocols. These providers must also comply with the provisions of Gramm/Leach/Bliley to the extent that they obtain and redisclose personally identifiable financial information from banks.

With an overlapping and mismatched structure, the current environment for consumers' ability to access data is very much a mixed bag. Consumer demands for new and expanded services have led to growing partnerships between traditional lending institutions and fintech firms to meet these needs. Still, there exists hesitation on the part of some traditional financial institutions.

The only way to change this dynamic is to foster an innovative and collaborative environment among all stakeholders involved.

[1] Online Lenders Alliance Best Practices, https://onlinelendersalliance.org/best-practices/

Background

There have been substantial efforts towards open banking, most recently when the Bureau issued market monitoring orders looking to secure information from data aggregators related to contracts, payments, data security, error resolution, liability, fraud, data accuracy, customer controls, privacy, and uses of data including metrics and traffic.

For providers, the CFPB has requested information related to consumer direct access, screen scraping, third-party portals, and third-party service providers. Additionally, as a part of this process, the CFPB published outlines and followed the requirements defined under SBRFEA, publishing their panel report in April 2023. As the Bureau moves forward with implementing section 1033 it will be critical that it consult with other regulators, including the Federal Reserve, the Office of the Comptroller of the Currency the FDIC, and the Federal Trade Commission, to ensure that any proposal does not impose substantially similar requirements on covered entities. The CFPB also must take into consideration certain account conditions under which covered entities do business in the U.S. and internationally and should not require or promote the use of any particular technology for the development of compliance procedures.

There have been concerns expressed by some that any open banking proposal needs to make sure that data aggregation services are fair, transparent, and competitive. The current patchwork of rules setting different standards at the state and federal level, for a broad range of market participants, creates confusion and inhibits growth. This current regulatory structure could result in putting consumers and their financial information at risk. Stakeholders have hoped to see the CFPB engage and define these rules and level the playing field for all participants, especially given the broad range of entities that will be collecting, storing, and dealing with consumer information. A key outcome will be to ensure that all participants are subject to the same financial standards and supervision.

Proposed Rule

OLA would like to take this opportunity to explore the intricacies and implementations of the proposed rule, addressing its potential impacts on consumer privacy, data security, and financial services. OLA's comments will examine many of the key provisions, regulatory framework, and potential challenges of this proposed rule on the evolving landscape of personal financial regulations.

The proposed rule provides new rights and imposes new obligations related to consumer financial data. This includes the right of access for consumers and third parties, including a data portability component. The rule requires that data access be accomplished through interfaces and imposes significant limits on how third parties may use data. The specific impacts are still unclear, and OLA hopes that the Bureau will provide further clarity on this issue in future rulemaking efforts.

The proposed rule would also expand the scope of data security regulations, especially the Gramm-Leach-Bliley Safeguards rule which the FTC updated earlier this year[2]. The proposed rule's broad scope may bring significant impacts on several fronts.

The rule would impact two very specific categories of covered persons, data providers, and third parties. For purposes of the proposed rule, data providers are institutions defined under Reg E, card issuers under Reg Z, or any other entity that controls or possesses information concerning a covered consumer financial service or product. This would cover such entities as banks, credit unions, and other providers of checking, savings, or credit card accounts, as well as various other payments and account products. The latter category would encompass a wide range of non-financial institutions, such as digital wallets, which the Bureau specifically touches on in the rule's preamble.

The other impacted entities are third parties, which are defined as any person or entity that is not the consumer to whom the covered data pertains or the data provider that controls or possesses the consumer-covered data. Given this definition, a third party could be another financial institution that is a data provider in its own right but also could include fintech and data aggregators. The proposed rule has some specific requirements for data aggregators, which would be defined as an entity that is retained by or provides services to the authorized third party to enable access to covered data.

Overall Impact of the Rule

It should be no surprise that the impact of the proposed rule will be significant. Some of the benefits from a data provider perspective would be a move away from the use of consumer account information by third parties to access accounts. This can create liability issues, especially when entities access more information than necessary to provide the product or service sought by the consumer. It also will establish more transparent standards, giving consumers some additional control over their ability to share their data with other entities, which may make it easier to move from one financial institution to another.

However, there are also concerns that whenever a federal rule like this is implemented, states often follow suit with more stringent provisions. The proposed rule does nothing to take future actions by the states into account.

This rule will also result in significant costs to undertake the system changes to create the data-sharing process it outlines. If the rule is enacted as proposed, companies will need to undertake significant organizational reviews and where necessary revise consumer documentation, data compliance policies, disclosures, and even previous commercial agreements with those third parties that deal with data. Companies will also need to prepare and maintain systems that can receive and process both data access and revocation requests, track duration-limited authorizations, and delete data when required due to revoked or lapsed authorizations, or when retaining the data is no longer reasonably necessary. These actions will incur sizable costs that the rule fails to consider.

[2] https://www.ftc.gov/business-guidance/blog/2023/10/ftc-announces-new-safeguards-rule-provision-your-company-whats-required

Impact on Privacy

The proposed rule would significantly expand privacy rights. The limitations on the use of data by third parties are an area that will have a huge impact especially if the use of de-identified information remains curtailed.

OLA has significant concerns about the definitions of covered data. The proposed rule would define covered data to encompass six categories of information, individual transaction information, both pending and historical; account balances; information to initiate payments to or from a Reg E account, including any checking, savings, or similar account held primarily for personal, family or household purposes; upcoming billing information; and basic account verification information. It should be noted that the proposed rule does not carve out or exempt aggregated, anonymized, or de-identified data. Because the use of de-identified and aggregate data by third parties like fintech companies is so prevalent, the Bureau should amend the proposed rule to allow for de-identified data to be carved out in some form. If not, many companies will need to expend significant costs in reworking their algorithms and product operations because so many are designed to run off de-identified data.

The proposed rule will also lead to an increase in notices and consent. Companies are constantly struggling to keep up with the changing compliance landscape due to new laws and regulations that demand proper disclosure. The proposed rule will only add to that burden. One example is the data provider publication requirements that would necessitate frequent updates meaning companies will have to allocate more hours and resources to compliance.

Data Security

As previously mentioned, the expansion of the Gram Leach Bliley Act Safeguard rule could create new burdens for third parties that previously have not been subject to this rule, especially given the recent update to the rule by the FTC. This will require companies to undergo major operational changes related to encryption at rest, and multi-factor authentication (MFA) any time account information access occurs, leading to more requirements for written policies and procedures. While this may not be a significant burden for more established companies, it will have an impact on smaller companies that lack the resources to undertake such large-scale operational changes. In addition, this proposal will also introduce more paperwork to review during the diligence process, both in the process of developing contracts with third parties and in the context of mergers and acquisitions.

The proposed rule also will result in more sensitive data being made available in a portable format, which inevitably will raise security risks. The proposed rule leaves unaddressed who would be held accountable for data breaches.

Conclusion

As more consumers choose nontraditional service providers to meet their financial needs, the regulatory framework must balance the need to ensure security and privacy with fostering innovation.

For innovation to reach its full potential to create the next generation of financial service products, all stakeholders must be able to operate on a level playing field with clear rules and regulations. An open marketplace that does not favor one technology over another or gives any one industry the ability to dominate or dictate trends is necessary to enable innovation to

flourish. Such an ecosystem should allow for the teaming of platforms and services that work in concert with each other, giving consumers much more effective access to their financial services.

In addition, consumers should always have the right to access all their data on their terms, for any purpose that they wish, which is why OLA advocates for strong consumer financial data rights and supports efforts to strengthen consumers' access to their financial information. Yet today there exists a significant inequity in a consumer's ability to control their data. The Bureau needs to rectify this imbalance by guaranteeing that consumers have unfettered access to their data and the ability to determine whom they share that data with.

The consumer's desire to have cutting-edge financial products has played an important role in driving market development, and it will remain the most critical motivation for future innovation. OLA members support unencumbered consumer access to their financial data, which enables greater consumer control over their financial choices, ultimately improving their financial health. It is incumbent on all stakeholders, banks, agencies, app developers, and third-party aggregators to work in concert towards marketplace enhancements that provide this power to consumers.

The members of OLA appreciate the opportunity to share our views. We look forward to working collaboratively to reduce barriers and enhance consumer financial options. If you have questions or would like additional information, please feel free to contact me at mday@OLADC.org.

Respectfully submitted,

Michael Day
Policy Director
Online Lenders Alliance