http://www.fdata.global/north-america

February 3, 2021

Comment Intake – Section 1033 ANPR
Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20052

SENT VIA ELECTRONIC MAIL TO 2020-ANPR-1033@cfpb.gov.

Re: Advance Notice of Proposed Rulemaking Regarding Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Docket ID CFPB-2020-0034)

The Financial Data and Technology Association of North America ("FDATA North America") appreciates the opportunity to provide comments to the Consumer Financial Protection Bureau ("CFPB" or "the Bureau") in response to its Advance Notice of Proposed Rulemaking ("ANPR") regarding implementation of Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act"). FDATA North America strongly supports the authority given to the CFPB by Congress in 2010 to promulgate, by rule, a consumer financial data right that will spur greater financial services innovation and competition and improve consumer financial access and inclusion. We are encouraged that the Bureau has formally begun the process of crafting a rule in this critically important area following many years of careful examination of the customer-permissioned data access and financial services ecosystems.

Countries around the world are quickly embracing the notion that the customer should be in control of their own financial data. By contrast, the unlevel playing field that currently exists for consumers and small- and medium-sized businesses ("SMBs") in the United States in this regard represents both a failure to American consumers and SMBs as well as a global competitive disadvantage. This unlevel playing field has been dictated by opaque bilateral data access agreements between their financial institution and aggregation firms that enumerate what choices they have to utilize their own financial data and the protections they are afforded when they do so. It also represents both a failure to American consumers and SMBs and a global competitive disadvantage. The Bureau's ANPR represents a meaningful step forward towards progress to ensure more equitable access, consistent consumer outcomes, and a more technology-driven and innovative financial services market in the United States.

FDATA North America has long advocated for the Bureau to act on its authority pursuant to Section 1033 of the Dodd-Frank Act and, as we will detail in the course of this submission, we

believe there are several principles that the Bureau should address in a Section 1033 rulemaking to improve financial access and competition. These principles include:

1. **The Bureau should use its Section 1033 authority to create a legal customer financial data right in the United States**. Countries around the world – from the United Kingdom, Australia, Singapore, Chile, and Canada – are embracing the notion that the consumer and SMB owner should have full control of their financial data. The U.S. risks falling behind as a global leader in digital innovation, financial equality, market competition, and consumer wellbeing by not recognizing this modernized approach. With its Section 1033 authority, the Bureau has the potential to improve financial access and inclusion: providing greater access to safe and affordable credit for thin or no-file borrowers; facilitating access to savings tools; and enabling secure, technology-enabled payment and budgeting tools for Americans with little or no access to traditional bank accounts. To accomplish this objective, FDATA North America strongly believes that any non-proprietary data element that is available to an end user through their online banking portal or is included on a paper statement, and that is not the intellectual property of the data holder, should be considered in scope as the Bureau contemplates promulgating a customer financial data right by creating protected classes of data under Section 1033 of the Dodd-Frank Act.

2. **It is important to define the limited circumstances in which custodians of financial data may override consumer consent**. As part of a rulemaking under Section 1033 of the Dodd-Frank Act, the Bureau should prescribe a well-defined set of circumstances under which financial institutions may withhold or restrict access to a customer's data access right to avoid a suppression of customer choice, voice, and consent. These circumstances should be limited to instances in which a data access request poses an imminent security risk or a situation in which the financial institution, the aggregator, and the customer each reasonably understands why the holder of the data determined that it was not in the customer's best interest to share the data due to evidence that the entity to which the customer permissioned access to their data posed a clear risk to the customer's financial wellbeing. A clear and timely solution must be implemented to prevent continued access issues and should include in its scope hindrances to both customer authentication and customer data access scope.

3. **Endorse a framework through which the Bureau conducts direct supervision over aggregators.** The best way to address financial institutions' concerns regarding third-party supervision issues associated with financial data access, and to remove the need for onerous bilateral data access agreements, is for the Bureau to create a federal supervisory regime for data aggregation platforms. Such a supervisory regime should establish a

principles-based baseline for data, cyber, and information security practices as well as governance over aggregation firms.

4. **Coordinate with the prudential regulators on Regulation E modernization.** To ensure liability is appropriately allocated throughout the financial ecosystem, FDATA North America advocates for a modernization of Regulation E that stipulates that the entity responsible for customer loss of funds related to a data breach or fraud be responsible for making that customer whole based on custody and responsibility.

5. **Recognize the need to permit current and legacy technology.** FDATA North America has long advocated for regulatory oversight and supervision of aggregation firms with a uniform minimum standard for aggregators who access a customer's financial data with their consent. While FDATA North America is technology neutral and supports the transition to application programming interface ("API") access of customer-permissioned financial data, the ecosystem is not yet ready to completely prohibit existing technological methods of accessing customer data without massive detriments to consumer financial health. In the absence of a fully developed, robust API environment, direct access, sometimes also referred to as "screen scraping" of the consumer interface, is a necessary tool to enable consumer and SMB data access, particularly for customers of all but the largest U.S. financial institutions. In Europe, the transition to its modernized second payment services directive ("PSD2"), which supported full consumer utility over their financial data, recognized the benefits of API access but embraced screen scraping as a fallback option in the event that APIs were not readily accessible for covered data fields. This approach has the benefit of providing an incentive for banks to build robust APIs more quickly; ineffective APIs that are deployed into the market will simply not be used.

6. **A strong federal data privacy regime would benefit consumers and SMBs.** While the Bureau is not granted under Section 1033 of the Dodd-Frank Act the authority to promulgate a national data privacy regime, FDATA North America and its members offer that such a framework would be additive to consumer and SMB protection and would better align the United States with other jurisdictions, including Europe, that have implemented national or supranational data privacy requirements.

About FDATA North America

FDATA North America was founded in early 2018 by several firms whose technology-based products and services allow consumers and SMBs to improve their financial wellbeing. We count innovative leaders such as the Alliance for Innovative Regulation, API Metrics,

Betterment, Direct ID, Equitable Bank, Envestnet Yodlee, Experian, Fintech Growth Syndicate, Fiserv, Flinks, Interac, Intuit, Kabbage, Mogo, Morningstar, M Science, MX, Petal, Plaid, Questrade, Quicken Loans, TransUnion, Trustly, ValidiFI, VoPay, Wealthica, Xero, and others among our members. We are a regional chapter of FDATA Global, which was the driving force for Open Banking in the United Kingdom, and which continues to provide technical and policy expertise to policymakers and to regulatory bodies internationally that are contemplating, designing, and implementing open finance frameworks. With chapters in North America, Europe, Australia, South America, and India, FDATA Global has established itself as an expert in the design, implementation, and governance of open finance standards and frameworks globally since its inception in 2013.

As the leading trade association advocating for consumer-permissioned, third-party access to financial data, FDATA North America's members include firms with a variety of different business models. Many provide technology services to large financial institutions or partner with state and national banks to enable innovation and expand financial access and inclusion. Others offer their own customer-facing financial products or services that may, for example, expand access to low-interest credit for thin or no-file borrowers, provide a gateway to automated savings or investments, onboard SMBs to accept and make digital payments, or support the SMB community by enabling technology-powered advisory and accounting services. Collectively, our members enable tens of millions of American consumers and SMB customers to access vital financial services and products, either on their own or through partnerships with financial institutions. Regardless of their business model, each FDATA North America member's product or service shares one fundamental and foundational requisite: it depends on the ability of a customer to actively permission access to some component of their own financial data that is held by a financial institution.

Benefits and costs of customer data access

Like the broader economy, the banking and financial services industry is experiencing unprecedented change fueled by digital innovation. As the world adapts to the new digital age, customers are increasingly becoming more reliant on third-party financial technology tools to manage their finances and improve their financial wellbeing. This reliance has been sharply increased by the COVID-19 pandemic. Modernized ecosystems, from the United Kingdom to Australia, have embraced this evolution. These ecosystems are empowering their consumers and SMBs to own, control, and share their financial data, thereby creating new opportunities and business models that would benefit all users of the system. The heart of open finance is the structured sharing of data by consumers and SMBs with, and between, their financial service providers, based on the individual needs of and consent by the end user. Executed properly, open

finance preserves the security and stability of the financial system while empowering customers to use their own data to improve their financial wellbeing.

Open finance and the mandate of consumer financial data portability have already brought many benefits for consumers and SMBs who provide consent for third parties to access their financial data. We have seen examples of these benefits from use cases around the world and in the United States over the last several years and promulgation of a rule implementing a customer data right under Section 1033 of the Dodd-Frank Act presents the potential to greatly expand the open finance market across the U.S. The benefits to end users of these ecosystems include: enhanced access to affordable and safe credit; improved price transparency across financial products and services; better, real-time insights for customers into their current financial status; technology-enabled budgeting, savings, and investing tools; faster and more secure payment acceptance and initiation services; and, improved access during the COVID-19 pandemic to the Paycheck Protection Program, among many others.

Critically, successfully deployed open finance regimes also mitigate risks and protect customers by creating level playing fields for market participants. A well-designed open finance framework with a legally binding customer data right should also require accreditation and regulation of financial data intermediaries and requirements for third-party service providers to ensure customers are made whole in the event of a data breach or other event that results in a loss of customer funds. An additional benefit of this regime is the establishment of clear and universally applied requirements around consent that should include the ability for customers to opt out of using a service and to revoke access to their data at any time. The significant competitive and innovative benefits to customers aside, these customer protection mechanisms alone represent a compelling rationale for the Bureau to ultimately promulgate a rule implementing Section 1033 of the Dodd-Frank Act. Industry cannot, on its own, universally and uniformly provide these important customer protections.

The open finance regulatory environments embraced by nations including the U.K., Australia, and Singapore are improving global competitiveness and enhancing financial inclusion among their citizenries. The U.K.'s Open Banking Implementation Entity recently announced that more than two million net new consumers across the country have adopted tools deployed under its Open Banking regime[1]. In Canada, the Department of Finance is moving forward with a deployment of open finance and is in the midst of the final element of its consultative process, which likely will culminate with the Minister of Finance tabling legislation in Parliament implementing the country's version of an open finance regime next year.[2] Likewise in Australia,

[1] https://www.openbanking.org.uk/insights/two-million-users/.

[2] FDATA North America has been heavily engaged with the Department of Finance on its ongoing "Customer Directed Finance" consultations.

a Consumer Data Right was launched earlier this year through which consumers will eventually have full utility over the totality of the data they generate. Financial data is one of the first elements of the Australian Customer Data Right ecosystem to be implemented.

By stark contrast, there exists no distinct legal assertion of a customer's legal right to access and permission access to their financial data in the United States. Although Section 1033 of the Dodd-Frank Act establishes a direct financial data access right for consumers, unless that data right includes authorized data access to third parties chosen by the consumer, it will provide inadequate access to critical financial products and services. The benefits outlined in this section demonstrate a clear need for an authorized data access right for consumers and SMBs that is commensurate with the determined data access right. That status quo, under which financial institutions continuously exercise control over their customers' data, provides little benefit to the end user. Financial institutions have used this control to determine whether and how their customers may utilize third-party financial services providers, including outright blocking the ability of their customers to do so. While, in some cases, financial institution throttling or blocking of third-party tools may be framed as oversight or regulatory rationales, competitive concerns unquestionably have fueled some of this behavior as well. In these instances, the end user typically is unaware as to why the product or service they are trying to use – or even have depended on for their financial wellbeing in the past – is not functioning or supported. This artificially stifles both consumer choice and marketplace competition.

The Bureau has the ability under Section 1033 of the Dodd-Frank Act to solve this problem. FDATA North America believes that Section 1033 equips the Bureau with the authority to mandate a customer financial data right that could bring to fruition the many benefits of an open finance ecosystem to consumers and SMBs across the United States. The Bureau should use its statutory authority to promulgate a legal customer financial data right in the U.S. that also sees direct supervision of financial data intermediaries as a means of providing for enhanced customer protection. Countries around the world are embracing the notion that the consumer and SMB owners should have full utility over their financial data. The open finance rules embraced by these countries are improving the global competitiveness of, and enhancing financial inclusion within, these nations. FDATA North America respectfully encourages the CFPB to follow suit.

Competitive incentives and authorized data access

Consumers and SMBs enjoy a competitive market for financial services applications that use their financial data to power innovative products and services, from online lending platforms to payment apps to financial management applications. Consumers and SMBs routinely direct these services to access their financial data through an authorized provider, which is often in the

possession of financial institutions. This customer-directed data access has become the norm over the last two decades, and data aggregators currently securely transmit this data at the direction of consumers and SMBs to enable a highly competitive market for data-driven financial services. This competitive marketplace is essential to ensure the existence of high-quality financial products and services that improve consumers' financial lives and provide needed assistance to SMBs, which is even more important during the current economic crisis.

As the business and technological arrangements underpinning customer-directed financial data sharing evolve, it is essential to maintain competition in the market for these data-driven financial services. Unfortunately, market developments over the last several years underscore that industry alone will not be able to deliver this outcome. As the customer-directed data market has grown, so too have the barriers erected by the data holders to accessing this data. To be fair, while we view some of these restrictions as anticompetitive, others are understandable given regulatory and customer protection expectations.

FDATA North America sees competition in data-driven financial services stifled by financial institutions that override customer direction to authorize sharing of their financial data. These restrictions include broad, as well as specific, attempts to directly limit third parties' access to data despite customer authorization; degradation of data sharing that effectively thwarts customer-directed access to financial data; and self-imposed mandatory reauthentication requirements and targeted blocking of sharing specific data fields in ways that effectively disable competing services. A recent FDATA North America study determined that more than 650 million existing consumer and small and mid-size accounts held by tens of millions of customers in the United States could be rendered useless by industry-led initiatives to move to APIs at just the largest 25 financial institutions.[3] These institutions do not supply sufficient data to fuel existing use cases upon which customers depend to manage their financial wellbeing. In each of these cases, competition in data-driven financial services would be substantially inhibited, to the direct and severe detriment of consumers. Recent investments by the largest financial institutions in the U.S. in a commercial entity that seeks to grant greater control to data holders regarding whether and how they will abide by their customers' instructions to grant access to their financial data have further eroded faith in the third-party provider marketplace that industry alone can deliver the outcome envisioned by Section 1033 of the Dodd-Frank Act.

Aside from competitive concerns, the logistics of providing customer-permissioned data access have become a significant blocker to a more vibrant marketplace. A growing number of large U.S. financial institutions are requiring third parties to negotiate and execute bilateral data access agreements if they desire to establish customer-permissioned data connectivity. While these

[3] Please refer to Appendix A.

bilateral agreements are intended to provide critical governance in banks' transitions from existing data-gathering technologies to the use of APIs, market participants generally recognize that individually negotiated bilateral agreements are an inefficient means of dealing with customer-permissioned data access. Such agreements lack uniformity, transparency, and insight, which can be challenging and expensive for third-party partners. These agreements result in differences between direct access and authorized access to desired tools by consumers based on the institution with which they have banking relationships and the aggregator that provides the services to the desired tool.

Several FDATA North America's member organizations that have executed data access agreements with large financial institutions report that the negotiations can take as long as three years to execute and often require extensive legal costs. Smaller financial institutions will not bear such costs and are thus discouraged from adopting new technology and user services. Additionally, the technology lift and technical resources required to develop independent APIs is a disincentive to smaller financial institutions that desire to allow their customers to permission access to products and services that they do not offer. An ongoing dependence on bilateral data access agreements therefore presents a significant challenge to smaller financial institutions that will struggle to keep pace with larger banks nationwide regarding API integration due to the substantial expense of negotiating bespoke agreements with any third party wishing to connect to that API.

Every financial institution has an individual process, created based on a combination of existing internal capabilities and expertise, of its existing technology infrastructure as well as any entities it has acquired, and regulatory requirements under the agencies' third-party partner risk management guidance that informs a bespoke bilateral data access agreement requires that any third party wishing to connect to its API must sign. The cost, in terms of both time and resources, of the process of onboarding and maintaining a relationship with a third-party technology provider often stymies the ability of smaller financial institutions and financial technology companies to engage in such agreements, which ultimately results in fewer, slower, and more expensive choices for customers.

Any fair assessment of the ecosystem must also conclude that, in the absence of a legally binding mandate to make customer data available with that customer's consent, commercial interests can factor into decisions that financial institutions make regarding what data to include in their APIs or how onerous the terms of third-party bilateral agreements will be. One of the principal rationales for government-led open finance regimes is the fact that holders of a customer's financial data, who themselves have a commercial interest in retaining that data to offer their customer additional financial products or services, have a competitive disincentive to make that data available because they use it offer their customer additional financial products or services.

To wit, as of December 1, 2020, approximately 650 million customer accounts would lose access to a critical data field required to enable a service on which a consumer or small business depends to manage their financial wellbeing if customers were only permitted to make portable data made available by financial institutions through their APIs.

Even if financial institutions' APIs did contain all of the data required to fuel the third-party services their customers use today, the ambiguity under the existing framework in the United States regarding consumers' rights to access their financial data would still result in a cumbersome system for sharing data between financial institutions and financial technology firms that is restricted to well-resourced actors. Additionally, it is generally cumbersome for all parties, including the customer, and lacks transparency to the end user.

Competition issues in the marketplace hinder Americans' ability to maintain access to life-changing technology-powered financial tools as consumers and SMBs alike deal with a challenging economic landscape. Robust competition in data-driven financial services can deliver lower costs, improved services, and better outcomes for consumer and SMB financial equality[4], outlook and productivity. Overriding consumers' and SMBs' direction to share data to obtain the benefit of these financial services poses significant harm to competition and to consumers and SMBs nationwide.

Standard setting

In other jurisdictions that have implemented open finance frameworks, including the U.K., technology mandates have been prescribed by government. While Section 1033 of the Dodd-Frank Act explicitly provides the Bureau with the authority to follow this example and establish and promulgate technology standards to deliver customer financial data utility, FDATA North America does not believe it would be prudent for the CFPB to do so for several reasons.

First, the United States, unlike many other jurisdictions around the world, has a large base of consumers and SMBs who are already reliant upon existing data access technologies to power the financial tools on which they depend. Any prescribed technology standard presents the very real risk of the ability of millions of Americans to continue to benefit from these technology-powered tools. Additionally, unlike the U.K. or Australia, the U.S. financial services market is large and diverse, with more than 5,000 Federal Deposit Insurance Corporation insured banks alone.[5] By contrast, in the U.K., where one standardized API was mandated under its Open

[4] A 2019 FinRegLab study found that "FinTech's use of cash-flow variables and scores were predictive of credit risk across a diverse set of populations and products."
[5] https://www.fdic.gov/bank/statistical/stats/2020jun/industry.pdf.

Banking system, there are only approximately 40 banks.[6] Even in this much smaller and centralized market, only the largest nine banks have actually implemented and deployed the U.K.'s Open Banking API.

To ensure continued and expanded customer benefit from a vibrant open finance regime in the U.S., it is imperative that the Bureau provide for flexibility regarding the technology standards that can be deployed to meet the policy requirements it will promulgate under an eventual Section 1033 rulemaking. Any acceptable technology under this regime should be required to meet the access scope, privacy, and consent requirements the CFPB should include in its future rulemaking. However, providing for the ability of financial institutions and financial technology firms alike to choose from a range of technology options as technology continues to evolve will herald a more competitive and flexible marketplace that considers the unique breadth and diversity of the U.S financial system. Furthermore, mandated technology standards may not be able to account for future use cases.

Access scope

As the Bureau looks to establish a final rule implementing Section 1033 of the Dodd-Frank Act, it is important to properly interpret the scope of those who will receive access to customer-permissioned financial data and what data should be protected under the CFPB's forthcoming rule. To be clear, FDATA North America strongly believes any non-proprietary data element available to an end user, either through their online banking portal or included on a paper statement, should be considered in scope as the Bureau contemplates promulgating a customer financial data right by creating protected classes of data under Section 1033. Full parity between direct and authorized access must be maintained without disincentivizing access to what data is available directly to the consumer today.

In 2018, the United States Treasury Department released a report that determined that the definition of "consumer" under Section 1033 "is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies."[7] The report is clear – consumers and SMBs should have the right to authorize access to their own financial data and the Bureau has the ability to help ensure they can do so safely and securely.

[6] https://www.ecbs.org/banks/united-kingdom/.
[7] https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

To date, market innovation regarding customer protection in the data access space has relied heavily on restricting customers' abilities to have full utility over their financial data. Artificially limiting the ability for third-party providers to access customer's financial data with that customer's consent is demonstrably detrimental to customers' financial wellbeing as it restricts consumer choice and marketplace competition. Consumers and SMBs have the best knowledge of their individual financial needs and circumstances and only they can determine what products and services will suit those needs. While all stakeholders in the financial system prioritize customer protection, restricting customer opportunity is not, in our view, an appropriate means of achieving this critical objective.

Instead, the Bureau should provide for direct supervision of financial data aggregation platforms pursuant to its authority under Section 1033 or through its "larger participant" rule. Through this action, the CFPB should establish a baseline for data, cyber, and information security practices as well as governance for these firms. Doing so would: 1) satisfy financial institutions' concerns that they could remain responsible for customer protection even after a customer's data has left their servers under Regulation E and 2) afford the Bureau with significantly more oversight of the consumer and SMB financial data access ecosystem. Regulated aggregation firms, or application providers relying on financial account data aggregators, would under this construct be responsible for governance over the customers on their platforms in accordance with the supervisory regime established by the Bureau. In FDATA North America's view, this framework represents a logical construct for implementing Section 1033 of the Dodd-Frank Act under which customers would have full use over the totality of the non-proprietary data their financial institution holds on their behalf, and financial institutions would have the assurance that the aggregators providing data connectivity are supervised and regulated by Bureau.

The Bureau should also consider, as it contemplates a rulemaking under Section 1033 of the Dodd-Frank Act, the unique challenges that SMBs face with regards to authorized financial data access. As many SMB owners designate an employee or contractor to assist in managing the business' finances, financial institutions may block or restrict access to financial data when that employee's or contractor's information does not match that of the account holder. The Bureau should consider as part of Section 1033 rulemaking a limited safe harbor for financial institutions that provides the ability of SMB owners to delegate data access rights to their employees or other authorized parties.

Consumer control and privacy

The deployment of financial technology applications within the financial services ecosystem has fostered the ability of consumers and SMB owners to use their financial data to make payments, manage their budgets, access capital, increase their savings, and invest safely and securely. The

empowerment consumers receive under this open finance framework provides them with the opportunity to improve their financial wellbeing, access value-based services, and take control over which entities always have access to their financial data. Achieving this outcome requires transparent, uniform consent requirements which all stakeholders must comply with to ensure that end users understand precisely what data they are providing to a third-party service provider. This also includes the ability to revoke that consent at any time. A supervisory framework under which data aggregation platforms are subject to CFPB examinations has the potential to provide for this evenly deployed outcome.

Improved customer control and transparency are this space is already in market with many participants. Financial institutions, in partnership with data aggregation firms, present to their customers a dashboard that enumerates the various data connections they have established to their accounts and what data elements they have permissioned to fuel the use cases they have connected. Over the last several years, when account connectivity was first established with a third-party service provider, aggregation platforms presented significantly more conspicuous disclosures regarding what data was being accessed, for what purpose, and for what length of time. FDATA North America respectfully suggests that the Bureau examine these customer-centric practices and tools as it considers whether more prescriptive requirements are needed. It is in the customer's and ecosystem's best interest to understand who is accessing what data and for what purposes, and FDATA North America's members are, in partnership with financial institutions, providing innovative solutions in this regard today.

The concept of data minimization is also central to customer protection and security. No third party should have access to any data element permissioned by a customer that is not required to fuel the use case for which that customer has opted in. This tenet should be a foundational element of the customer data right the Bureau includes in its forthcoming Section 1033 rulemaking. This should also be central to any supervisory regime it establishes for financial data aggregation firms, as these firms provide the data connectivity for the thousands of third parties in the financial technology ecosystem. Supervision of aggregators would provide the Bureau with the ability to ensure data minimization requirements are adhered to by market stakeholders.

As articulated in one of our principles, FDATA North America also strongly supports the creation of federal data privacy standards by Congress that are consistently applied to all market participants and designed and implemented with the customer's best interests in mind. As increasing numbers of financial services customers interact with their providers on mobile devices, it is unreasonable to expect a customer to have to consider, when they access a financial application, which data privacy or data protection regime applies to that tool. It is important to acknowledge the rapid pace of technological innovation and to ensure that a data privacy regulatory framework does not become an unnecessary hindrance to customers' ability to benefit

from new and innovative products and services. Therefore, flexibility must be introduced into any such privacy regime to ensure that consumer protections implemented can evolve and improve over time.

Lastly, the potential for bad actors to access customer data will always exist, regardless of security controls. Even the largest, most complex financial institutions have been victims of cybercrime in recent years. A key component of a well-designed open finance system is a requirement for shared responsibility across the system. Thus, assuring the consumer or SMB that, in the event they have sustained harm because of a data breach, the party responsible for the breach will be responsible for making the customer whole. While this is a self-evident requirement, accomplishing this outcome will require modernization of existing rules and statutes that currently apportion responsibility for consumer protection in the event of a consumer loss. Many of those rules and statutes have shared jurisdiction across multiple regulatory agencies, most notably including Regulation E. We respectfully encourage the CFPB, along with its peer financial regulatory agencies, to modernize Regulation E to provide for a system under which the impacted holder of a customer's data is ultimately responsible for making them whole in the event of financial loss related to a data breach stemming from fraudulent account access.

Some financial institutions argue that Regulation E provides them with a responsibility to, in some cases, restrict their customers' ability to share their financial data with third parties. These restrictions sometimes take the form of missing data fields embedded within the APIs financial institutions make available to fintech applications. Other times, they involve an authentication regime that requires intensive user input, or is not optimized for the user's experience, resulting in low connectivity and/or conversion rates for the consumer or SMB. This can include, for example, mandatory authentication redirection for use cases for which such a regime does not provide added customer protection. For customers who depend on third-party application providers to help them manage their financial wellbeing, it is imperative that they be able to access those tools whenever they need to with an optimal user experience across different types of devices. The customer-permissioned data access marketplace does not uniformly provide for this outcome today.

This belief, which in some cases is well-founded based on outdated regulatory expectations, creates an unlevel playing field that results in inconsistent and unfair bilateral data access agreements, and leaves the third-party at the mercy of the access rules established by the financial institution. Modernizing the regulation would provide for increased customer protection in an open finance ecosystem under a final rule implementing Section 1033 of the Dodd-Frank Act.

Data accuracy

The integration into underwriting tools of cash-flow data (data derived from customers' bank account records with their consent) has allowed scores of Americans with no or little traditional credit bureau data to access low-cost credit safely and avoid turning to more predatory products. The inclusion of cash-flow data into underwriting models has allowed scores of lenders to better assess the credit risk of thin- and no-file applicants. The Fair Credit Reporting Act ("FCRA") was first enacted in 1970, when the only data used for underwriting was supplied to lenders by traditional credit bureaus, who themselves secured the data from consumers' creditors. Accordingly, careful consideration must be given to how the FCRA should be applied in the context of customer-permissioned data access. The FCRA sought to promote the accuracy, fairness and privacy of consumer information contained in the files of consumer reporting agencies. It also sought to provide Americans with: transparency for consumers to see and interact with their financial data in an opaque system in which they were merely a passive participant; more control of and insight into the data their creditors were reporting to the credit bureaus; and, the right to have erroneous or incorrect data that might influence credit decisions corrected.

The rationale for the enactment of the FCRA five decades ago simply does not exist for cash-flow data. Unlike traditional credit data, cash-flow data is controlled by the consumer at all times. It is the end users who decide to integrate this data into an underwriting environment, not their creditors. Moreover, the consumer always has complete transparency into the data. After all, this is their transactional data, which they can view and interact with online at all times through their financial services provider's online portal. Critically, the tools created by the FCRA to afford consumers with the ability to have credit bureaus address incorrect information about them similarly are unnecessary in a cash-flow underwriting environment because customers are already empowered to see their financial account transactions in real time and to immediately contact their financial services providers to advise them in the event of fraudulent charges. Given the significant transparency and customer control afforded to users of financial technology tools, the responsibility for ensuring the accuracy of customer data should rest with the original holder of that data so long as no entity that had access or permission to view that data amended it. From a pragmatic perspective, a data recipient or data intermediary, which merely displays or transmits raw financial data from the original data holder, may not have the ability to amend incorrect transaction data. Moreover, to the extent that they did, two different data records for the same transaction record would now exist: one generated by the customer's financial institution and the other by a third-party service provider.

Financial Data and Technology Association

http://www.fdata.global/north-america

Conclusion

FDATA North America appreciates the opportunity to provide the perspective of financial technology companies, aggregation platforms or application providers relying on aggregators, regarding the importance of the Bureau's promulgation of a final rule implementing Section 1033 of the Dodd-Frank Act. As the trade association representing firms that provide critical financial wellness tools to millions of Americans, and as a chapter of a global organization that has overseen the implementation of open finance ecosystems across the globe, we believe that the United States has an opportunity to improve competition, financial access, and consumers' and SMBs' financial outcomes by embracing the kind of customer-directed, open finance regime that is taking hold in other markets around the world. In any open finance system, consumer protection and security are paramount, which is why every market globally with an open finance framework has a legally binding data right as its centerpiece.

We encourage the CFPB to fully utilize its Section 1033 authority to create a customer financial data right to allow consumers and SMBs to have unrestricted access to technology-based tools that can help them improve their financial wellbeing, along with the other important bedrocks of an open finance regime we have articulated in this submission. We appreciate the Bureau's continued focus on this critically important space and look forward to continuing to work with you.

Sincerely,

Steven Boms
Executive Director
FDATA North America

Enclosures

Financial Data and Technology Association

http://www.fdata.global/north-america

Appendix A: Missing API Data Fields and End User Impact[8] [9]

Financial Institution Size, By Total Assets	*Impacted Use Cases*	*Total Number of End User Accounts Impacted*
Top 10	Consumer Personal Financial Management, Account Verification, Lending, Small Business; Money Management, Money Movement, Wealth Management, Retirement Savings, Tax, Bookkeeping, Loan Underwriting, Fraud	557,395,494
11-25	Consumer Personal Financial Management, Lending, Small Business, Money Movement, Wealth Management, Retirement Savings, Tax, Bookkeeping, Loan Underwriting, Fraud	103,572,965

[8] As of December 1, 2020.

[9] Because some of the largest 25 U.S. financial institutions have not yet implemented an API, data is extrapolated to reflect the total impact to end users if those APIs, once established, mirror those that have already been deployed by other large financial institutions.

http://www.fdata.global/north-america

Appendix B: Competition Issues in Data-Driven Consumer and SMB Financial Services

Executive Summary

Consumers and small- and medium-size businesses (SMBs) enjoy a competitive market for financial services applications that use their financial data to power innovative products and services—from online lending platforms to payment apps to financial management applications. Consumers and SMBs routinely direct these services to access their financial data, which is often in the possession of financial institutions. This customer-directed data access has become the norm over the last two decades, and data aggregators now securely collect and transmit this data at the direction of consumers at SMBs to enable a highly competitive market for data-driven financial services. These financial services help to improve consumers' financial lives and provide needed assistance to SMBs—which is all the more important in the current perilous economic times.

As the business and technological arrangements underpinning customer-directed financial data sharing evolve, it is essential to maintain competition in the market for these data-driven financial services. Members of the Financial Data and Technology Association (FDATA) of North America see competition in data-driven financial services stifled by financial institutions that override customer direction to share their financial data. These restrictions range from broad attempts to directly limit third parties' access to data despite customer authorization (outside of individual instances of suspected fraud or unauthorized access); degradation of data sharing that effectively thwarts customer-directed access to financial data; and targeted blocking of sharing specific data fields, in way that effectively renders competing services useless. In each of these cases, as evidence shows, competition in data-driven financial services is being substantially inhibited to the direct severe detriment of consumers.

Efforts to override customer-directed data access for competing financial services in these ways should be addressed under existing competition laws. As both the holders of customer financial data and competitors with third-party service providers, financial institutions can exercise market power in a way that dramatically limits direct competition with competing financial services. Outside of stopping fraudulent or similar unlawful conduct, broad restrictions on customer-directed data sharing to competitors, or targeted restrictions of certain data fields used by competitors, are not justified by existing law or regulations, regulators' third-party oversight obligations, or consumer protection concerns. Nor do they have procompetitive benefits that would outweigh anticompetitive effects. Particularly as consumers and SMBs face a difficult economic climate, they directly benefit from a vibrant market of competitive options to improve their financial outlook.

http://www.fdata.global/north-america

Introduction

Consumers and small- and medium-size businesses (SMBs) have enjoyed burgeoning competition for financial services in recent years, including for products driven by their own data. These services allow consumers and SMBs to take greater control over their financial lives and opportunities: to find new sources of credit based on innovative underwriting models, to initiate payments to friends, family and vendors in real time and without fees, and to help manage their financial outlook across multiple accounts and plan effectively for the future. In a time of enormous economic uncertainty, these services are more important than ever to help consumers and SMBs navigate difficult financial circumstances.

The innovation in financial services is powered by consumers and SMBs granting permission for access and use of their data, often in conjunction with cutting edge machine learning and other data analytics technology. Much of this financial data is associated with consumers' and SMBs' existing accounts with financial institutions – including transaction history, loan products, and spending habits. For more than two decades, consumers and SMBs have chosen to provide access to this data to additional financial institutions and new competitors (such as financial technology companies, or fintechs) to obtain additional financial services to meet their economic needs.[10]

As consumers and businesses face a deteriorating economic landscape, it is critical to maintain competition in the market for these data-driven financial services. It is even more essential when certain market participants either individually or collectively have the ability to override a consumer's or SMB's decision to direct a potential competitor to access its financial information. Market participants have been dealing for years with issues related to data protection and regulatory compliance, but steps to override customer-directed access raise critical competition issues under U.S. law. Indeed, the costs of restricting competition in data-driven financial services are severe. A recent Financial Data and Technology Association (FDATA) of North America study indicates that *nearly two billion* existing consumer and SMB third-party accounts could be rendered useless by overriding access to financial data that was specifically directed by those consumers and businesses. A direct result will be far fewer options to help consumers and businesses in perilous times—particularly in critical areas like credit for SMBs—and inevitably higher prices for consumers.

Competition issues cannot take a back seat as the regulatory and technological framework in data sharing continues to evolve. FDATA and its members have long advocated for a regulatory approach that facilitates the sharing of data by customers with, and between, their financial service providers, based on consent and with safeguards for privacy and security. Such "open finance" systems that achieve those two objectives have been implemented in the United

[10] FDATA North America (FDATA) is the trade association that represents financial and technology firms whose technology-based products and services allow consumers and SMBs in Canada, the United States, and Mexico to improve their financial wellbeing.

Kingdom, the success of which, including increased competition in the financial services market, has motivated other countries, including Canada, Australia, New Zealand, and South Africa, among others, to pursue similar regimes. As this regulatory approach develops, competition laws provide a critical backstop to ensure that existing competition in the market for data-driven consumer financial services is not stifled.

I. Consumers Benefit From a Competitive Market for Data-Driven Consumer and SMB Financial Services.

A. The Market For Data-Driven Consumer and SMB Financial Applications is Robust.

A wide range of applications use consumer and SMB financial data to power innovative products and services to meaningfully improve their customers' financial lives. As discussed in more detail below, these include: online lending platforms for consumers and SMBs that leverage the availability of data for underwriting decisions; payment apps that access customers' accounts to enable faster and more efficient payments; and financial management applications that advise consumers and SMBs on options to improve their financial outlook.[11]

These types of applications depend on consumers and SMBs granting access to their financial data—data often in the possession of depository and other legacy institutions with which consumers and SMBs have a relationship. To facilitate data sharing with these financial services providers, companies known as data aggregators have emerged, via the competitive market, to safely and securely collect and transmit financial data at customers' direction. All of the companies in this ecosystem depend directly on and answer to their customers, who give explicit permission for access to their financial data. Additionally, companies operating data-driven financial services must compete on critical issues like data integrity, reliability, and customer service.

The past decade has seen an explosion of growth and competition in financial technology, including in the market for data-driven financial products and services. A July 2018 U.S. Department of the Treasury report notes that from 2010 to the third quarter of 2017, more than 3,330 new technology-based firms serving the financial services industry were founded, and the financing of such firms reached $22 billion globally in 2017.[12] Accenture has estimated that

---

[11] This is not meant to be an exhaustive list of applications. For example, tax preparation services can use customer-directed access to data to help taxpayers quickly and accurately complete tax returns.

[12] U.S. Dep't of the Treasury, *A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation* (July 2018), at 5, *available at* https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf [hereinafter "Treasury Report"].

investments in fintech companies reached $53 billion globally in 2019.[13] As of 2018, lending by such firms made up more than 36% of all U.S. personal loans, up from less than 1% in 2010.[14]

Moreover, "survey data indicate that up to one-third of online U.S. consumers use at least two fintech services — including financial planning, savings and investment, online borrowing, or some form of money transfer and payment"[15] – which compete directly with traditional financial institutions' products. In 2020, for example, *Forbes* listed a dozen personal finance startups among its top 50 fintech companies.[16] As the 2018 Treasury report notes, some digital financial services reach up to 80 million members, while financial data aggregators can serve more than 21 million customers.[17]

These more recent market entrants compete both with each other and with traditional depository financial institutions to provide innovative financial products that greatly benefit consumers, including by lowering costs and expanding access by filling gaps in the market. The direct line between competition and innovation is well-chronicled, as the 2018 Treasury report notes:

> The increasing scale of technology-enabled competitors and the corresponding threat of disruption has raised the stakes for existing firms to innovate more rapidly and pursue dynamic and adaptive strategies. As a result, mature firms have launched platforms aimed at reclaiming market share through alternative delivery systems and at lower costs than they were previously able to provide. Consumers increasingly prefer fast, convenient, and efficient delivery of services. New technologies allow firms with limited scale to access computing power on levels comparable to much larger organizations. The relative ubiquity of online access in the United States, combined with these new technologies, allows newer firms to more easily expand their business operations.[18]

Depository institutions also use the financial account data they collect to offer data-driven financial services, including lending products, wealth management services, and digital payments solutions. Indeed, banks' competition with one another in offering these products is often based on customer-directed data aggregation services that enable relevant data sharing

---

[13] Michael Del Castillo et al., *The Forbes Fintech 50: The Most Innovative Fintech Companies In 2020*, Forbes (Feb. 12, 2020), https://www.forbes.com/fintech/2020/#6ba7e6904acd.

[14] Treasury Report at 5.

[15] *Id.* at 18.

[16] Kelly Anne Smith, *The Future of Personal Finance: Fintech 50 2020*, Forbes (Feb. 12, 2020), https://www.forbes.com/sites/kellyannesmith/2020/02/12/the-future-of-personal-finance-fintech-50-2020/#346ce4a6fd43.

[17] Treasury Report at 5.

[18] *Id.* at 6.

between banks.[19] While fintechs have emerged as a significant part of the market, and often fill specific gaps to market to certain underserved customers, traditional depository institutions remain competitors in this market.

Data-driven innovative financial services include (but are not limited to) products and services in the following areas, each of which explicitly depends on explicit consumer direction to access the consumer's financial data:

Financial management. Personal financial management applications enable consumers to leverage information drawn from a range of accounts, including bank accounts, to assist with important budgeting, cash flow management, and strategies for better financial success. These services can also help consumers avoid overdraft and other unnecessary fees. SMBs can also use financial management tools to aggregate and analyze financial information to better manage financial performance and cash flow and to improve decision making.

Lending. Lenders can rely on detailed consumer and SMB data, such as cash flow data for SMBs, in making lending decisions. The analysis of such large data sets, rather than simply relying on traditional credit scoring, has been shown to expand access to credit for SMBs.[20]

Payments. Consumers enjoy having a wide range of payment options that meet their needs with respect to convenience, speed, and privacy. In particular, peer-to-peer and consumer-to-merchant payment applications allow consumers to quickly send funds remotely, without needing to rely on cash or checks.

Importantly, in each of these use cases, consumers and SMBs make an active choice to allow access to their financial data in order to facilitate services that benefit them directly. Consumers seeking the benefit of personal financial management applications, for example, rely on real-time access to their financial accounts to obtain the benefit of the service—indeed, that is

---

[19] *See* Vaibhav Gujral, Nick Malik, and Zubin Taraporevala, *Rewriting the rules in retail banking*, McKinsey & Company (Feb. 2019), https://www.mckinsey.com/industries/financial-services/our-insights/rewriting-the-rules-in-retail-banking; Rip Empson, *Yodlee Partners With Bank Of America To Bring Its Financial Apps To Online Banking* Tech Crunch (Oct. 26, 2011), https://techcrunch.com/2011/10/26/yodlee-partners-with-bank-of-america-to-bring-its-financial-apps-to-online-banking/.

[20] For example, FinRegLab found evidence that its study participants were serving borrowers who may have historically faced constraints on their ability to access credit. *See* FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Market Context & Policy Analysis, at 5, 26-27 (Feb. 2020), *available at* https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf [hereinafter "FinRegLab Policy Report"]; FinRegLab, Empirical Research Findings, at 30. 32 (July 2019), *available at* https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf .

the very point of the service. Likewise, SMBs that obtain loans based on their cash-flow data rely on real-time data access to provide evidence that their business is viable. Competitors in these areas are incentivized to be fully transparent with their consumers in the process of obtaining authorization for account access.

The ability to process and analyze large data sets has enabled—and will continue to unleash—substantial advances in the ability of these services to assist consumers and SMBs. As one example, SMB lending based on cash-flow data is dependent on large sets of transaction data and a steady stream of account-level data. Additionally, innovative companies continue to explore how machine learning and artificial intelligence (AI) can be applied to large and complex data sets to help enable underwriting decisions or financial management applications. As the Treasury report notes, technologies like cloud computing and machine learning/AI "enable firms to store vast amounts of data and efficiently increase computing resources," and "[u]nsurprisingly, for financial services firms, data analytics and machine learning (or artificial intelligence) are two of the top three areas of tech investment."[21] Thus, we can expect data-driven innovative financial services to continue to expand.

B. The Market for Data-Driven Financial Services is Premised on Decades of Customer-Directed Data Sharing.

1. Customer Financial Data Access and Sharing is the Status Quo.

The range of data-driven financial services exists because customer-directed data sharing is the status quo of the online financial services market. As a practical matter, the market for services powered by consumer and SMB financial data has existed since at least the early 2000s, when traditional financial institutions and others began using customer-directed data sharing to offer new products and services to consumers.[22] Indeed, some FDATA members have been dealing with permissioned access to account-level data for more than two decades, even before the recent growth of fintechs – including by facilitating data sharing between financial institutions. The Office of the Comptroller of the Currency (OCC) issued guidance on bank approaches to data aggregation services as far back as 2001[23] and most recently released updated

[21] Treasury Report at 8.

[22] Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83806, 83808 (Nov. 22, 2016).

[23] Office of the Comptroller of the Currency, OCC Bull. 2001-12, Bank-Provided Account Aggregation Services: Guidance to Banks (2001), *available at* https://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-12.html/.

guidance in March 2020. In short, data-driven financial services have evolved in a market where customers' permissioned access to their financial information is the norm.

This status quo in the United States is buttressed by consumer data access obligations codified in the Dodd-Frank Wall Street Reform and Consumer Protection Act. In particular, Section 1033(a) requires that:

> [s]ubject to rules prescribed by the [Consumer Financial Protection] Bureau, a covered person *shall make available* to a consumer, *upon request*, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges, and usage data."[24]

That section further provides that "[t]he information *shall be made available* in an electronic form usable by consumers."[25] While some stakeholders have argued that, in the absence of Consumer Financial Protection Bureau (CFPB) rules, some limitations on consumer access may be justified, the plain language is clear that consumers can access such information, and that it should be in a usable electronic form—therefore facilitating sharing with third parties.[26]

In sum, data-driven financial services operate in a unique market with an established history and reliance on customer-directed data sharing. In the United States, FDATA and others have argued that new legislation or regulations would speed the path toward practical implementation of open finance and improve the existing market, while further encouraging competition. That said, as the regulatory landscape develops, the status quo is that consumers and SMBs can—and by the many millions, do—access their financial data and provide it to third parties to enable competitive financial services.

2. As the Market Evolves, Restrictions on Customer-Directed Data Sharing Disrupt Competition.

---

[24] 12 U.S.C. § 5533(a) (emphasis added).

[25] *Id*. (emphasis added).

[26] Nor is there an issue with designating an agent for purposes of access and sharing. As the Treasury report notes:

> The definition of "consumer" in Title X of Dodd-Frank includes not only an individual, but "an agent, trustee, or representative acting on behalf of an individual." This definition is best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies. Otherwise, narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications.

Treasury Report at 31 (citations omitted).

Both the business and technological arrangements underlying customer-directed financial data sharing are evolving. In general, a portion of the market is moving toward bilateral agreements between financial institutions and data aggregators for handling customer-directed data sharing. Aggregators in turn assist their own customers, data-driven financial services providers, with obtaining the financial data—at their customers' request—necessary for services to function. However, market participants generally recognize that individually negotiated bilateral agreements are an inefficient means of dealing with permissioned data access. In particular, such agreements lack uniformity and provide the potential for specific institutions to exert restrictions on data access, including by seeking to block particular data fields that the customer requested to be shared, such as data that could be used by potential competitors. Additionally, the technology used for data sharing is shifting throughout the market. Many market participants are moving from credential-based access based on consumers providing their login credentials to an intermediary to obtain their financial information[27] to access enabled through an application programming interface (API) provided by a financial institution to a data aggregator. This too enables certain data fields to be unilaterally blocked from being accessed via the API, as the bilateral agreements generally prohibit a data aggregator from accessing data through any means other than the API.

One result of these developments is a potentially increased concentration of market power in data-holding financial institutions. For example, on the business side, The Clearing House released a model agreement for data sharing between financial institutions and data aggregators.[28] On the technical side, major financial institutions, fintechs, and others are part of the Financial Data Exchange (FDX), which is seeking to implement technical solutions for APIs to enable data sharing.[29]

FDATA members have number of competition concerns within this market:

---

[27] This is often referred to in shorthand as "screen-scraping." However, that terminology conflates the means of providing authentication for data access (providing a credential such as a password), with the means of collecting the data (retrieving it from a screen that is normally designed to be viewed by a consumer). APIs can enable consumers to provide authentication without disclosing credentials to a third party, and also enable more efficient retrieval using data feeds.

[28] *See Model Agreement*, The Clearing House, https://www.theclearinghouse.org/connected-banking/model-agreement (last visited June 1, 2020).

[29] Additionally, a number of financial institutions recently obtained an ownership interest in their own data-sharing network. *See* Penny Crosman, *Fidelity's data sharing unit Akoya to be jointly owned with the Clearing House, 11 banks* (Feb. 20, 2020, 9:51 AM), https://www.americanbanker.com/news/fidelitys-data-sharing-unit-akoya-to-be-jointly-owned-with-the-clearing-house-11-banks.

- Broad attempts to override customer-directed access to financial data, by directly restricting third parties' access to that data despite customer authorization, outside of individual instances of suspected fraud or unauthorized access.

- Relatedly, constructive restriction of customer-directed access to financial data, due to intentional degradation of data sharing, under similar circumstances.

- Targeting and blocking sharing of specific data fields, contrary to customers' authorization, used by directly competing services. Blocking specific data fields can effectively render competing services useless and coerce customers into using services offered by the financial institution that may not be best suited for their needs.

Constructive restriction of customer-directed access is a particular concern. For example, a financial institution may use a token to facilitate permissioned access to financial data via an API. That token can be set to expire after a period of time. Frequent token expiration, causing the customer to need to constantly re-authorize permission for data access, may deter a customer from relying on the financial service, in some cases by adding extensive friction, and in others by undermining services that rely on continual data access. Additionally, some services like SMB lending based on cash-flow data, or real-time financial management applications, rely on continuous updating of information and may be rendered unusable by token expiration requirements imposed by a financial institution.

Restrictions on specific data fields also can enable suppression of competition for competing services, even if all data is not blocked. For example, selectively blocking the sharing of some portion of data that a fintech lender uses for underwriting can undermine the lenders' ability to perform effective analysis of creditworthiness, and therefore its ability to compete to provide a competitive loan to the customer. This is true even if the lender has access to some portion of the data—but not all of the data that the customer permissions in order to allow the service to function effectively.

II. Restrictions on Customer-Directed Access to Financial Data Raise Serious Competition Concerns in the Market for Data-Driven Financial Services.

Overriding customer-directed data access for competing financial services in these ways raises issues under antitrust laws. There are fraud-related reasons for restricting data in certain limited circumstances, and market participants are currently working together to address them. However, restrictions on customer-directed data sharing to competitors, and/or targeted suppression of certain data that consumers and SMBs choose to share with competitors, directly thwarts competition and must be closely scrutinized under antitrust laws.

http://www.fdata.global/north-america

A. Restrictions on Consumer-Permissioned Data Sharing Inhibit Competition.

1. Data-Driven Financial Service Providers and Consumers Would Be Substantially Harmed by Overriding Customer-Directed Access to Financial Data.

Overriding customer-directed access to financial data, under the circumstances discussed above, would have serious repercussions for financial service providers and the consumers and SMBs they serve. In 2019, FDATA examined the impact of restricting access to a portion of the market that currently relies on credentialed access rather than APIs. Its findings were based on a survey of its members that were shared with the CFPB. FDATA's conclusion is that overriding consumer-permissioned access to data would be devastating to the market. In particular, cutting off customers' credentialed access would result in the following becoming inoperable:

- More than 530 million loan accounts;
- More than 310 million financial management accounts, which help customers manage their account balances, provide overdraft protection, and make payments on time;
- More than 330 million advisory accounts;
- More than 210 million accounts that help customers move and save their money;
- Nearly 200 million payments accounts;
- Nearly 140 million accounts that provide fraud monitoring or identity verification and authentication; and
- More than 100 million accounts providing underwriting data for potential lenders.

Overall, FDATA estimates that as many as ***1.8 billion consumer and SMB accounts in the United States would lose functionality*** if customer-directed credentialed data access was completely cut off and only data provided through financial institutions' APIs was permitted. This number is a conservative estimate since it is based only on data concerning the largest financial institutions. The number would be significantly larger if it took into account consumers and SMBs that have financial services accounts that access data from the thousands of smaller financial institutions across North America. Overall, FDATA estimated that up to 100 million consumers use digital financial services that may be affected by restricting existing data access arrangements.[30]

[30] John Pitts, *BankThink: OCC did its part to secure customer data. Now it's CFPB's turn*, American Banker (Mar. 16, 2020, 9:40 AM), https://www.americanbanker.com/opinion/occ-did-its-part-to-secure-customer-data-now-its-cfpbs-turn.

2. Restrictions on Customer-Directed Data Sharing Can Be Anticompetitive.

Restrictions on customer-directed data sharing that directly inhibit competition in this way must be scrutinized under well-established antitrust laws.[31] Potentially anticompetitive conduct is generally subject to a "rule of reason" analysis that considers the restraint, the industry at issue, and the relevant market, to "assess the restraint's actual effect on competition," and identify those "restraints with anticompetitive effect that are harmful to the consumer."[32] Antitrust regulators evaluate the level of competition with, as compared to without, the relevant conduct, and analyze whether conduct likely harms competition by increasing the ability or incentive profitably to raise price above, or reduce output, quality, service, or innovation below, what likely would prevail in the absence of the conduct.[33] In general, if a company can show that conduct harms competition, the party restricting competition must show cognizable procompetitive justifications for the challenged conduct, such as enhanced efficiency or increased product output. However, these justifications will be insufficient if the restraint is not necessary to achieve the procompetitive goal or the goal may be achieved in a manner that is less restrictive of competition.[34] Ultimately, a violation will be found if the anticompetitive conduct outweighs the procompetitive justifications.[35]

Concerted refusals to deal with competitors are actionable when they unreasonably restrain trade.[36] Indeed, in providing its most recent guidance to banks on dealing with data

---

[31] The Sherman Act outlaws any unreasonable "contract, combination . . . or conspiracy in restraint of trade," and any monopolization, attempted monopolization, or conspiracy or combination to monopolize. 15 U.S.C. §§ 1, 2. The FTC Act covers similar conduct. 15 U.S.C. § 45(a). *See* Federal Trade Commission, The Antitrust Laws, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws.

[32] *See, e.g., Ohio v. Am. Express Co.*, 138 S.Ct. 2274, 2283-84 (2018) (internal quotations and citations omitted).

[33] FTC & U.S. Dep't of Justice, Antitrust Guidelines for Collaborations Between Competitors, at 4 (April 2000), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/joint-venture-hearings-antitrust-guidelines-collaboration-among-competitors/ftcdojguidelines-2.pdf. [hereinafter "FTC/DOJ Guidelines"].

[34] *Am. Express*, 138 S. Ct. at 2284.

[35] *See, e.g., Capital Imaging Assoc., P.C. v. Mohawk Valley Medical Associates, Inc.,* 996 F.2d 537, 543 (2d Cir. 1993).

[36] *See* FTC/DOJ Antitrust Guidelines at 4; *see also FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447 (1986) (concerted refusal to share information with insurance companies; "[a] refusal to compete with respect to the package of services offered to customers, no less than a refusal to compete with respect to the price term of an agreement, impairs the ability of the market to advance social welfare by ensuring the provision of desired goods and services to consumers at a price approximating the marginal cost of providing them").

aggregation services, the OCC emphasized "[a]ny collaborative activities among banks must comply with antitrust laws."[37] Moreover, use of market power in one market—for example, depository services—to "tie" consumers to another service in a competitive as a de facto matter (here, services in the data-driven financial services market) have been held to unreasonably restrain competition in violation of the antitrust laws.[38]

Financial institutions that control consumer and SMB financial data have substantial market power, both in terms of market share and ability to impose barriers to entry on competitors.[39] When working in some combination, and potentially in some instances unilaterally, they can dramatically affect competition in data-driven financial services. As noted above, the potential impact on fintech accounts of restricting a range of data fields would be enormous—it would essentially disable the ability of certain competitors to operate entirely.[40] Additionally, a customer could be effectively coerced into using a particular data-based financial product offered by the customer's primary depository institution if the customer is denied the ability to authorize access to account information by a third party. In fact, that denial could effectively inhibit the customer's ability to obtain a data-driven financial service *from other competitor banks*, many of which use data aggregation services to obtain customer financial information for their product offerings.[41]

Regulators have taken action against attempts to block pre-existing data sharing that have the effect of unreasonably restricting competition. These actions often arise in situations where, as here, the status quo is a level of data sharing that facilitates competition. Indeed, the status quo

---

[37] Office of the Comptroller of the Currency, OCC Bull. 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29 (2020), *available at* https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html. [hereinafter "OCC 2020 Guidance"].

[38] *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 463 (1992); *Virtual Maint., Inc. v. Prime Comput., Inc.*, 11 F.3d 660, 667 (6th Cir. 1993).

[39] *See Ind. Fed'n of Dentists*, 476 U.S. at 460-61.

[40] *See* FTC/DOJ Guidelines at 15 ("An exercise of market power may injure consumers by reducing innovation below the level that otherwise would prevail, leading to fewer or no products for consumers to choose from, lower quality products, or products that reach consumers more slowly than they otherwise would."). Under these circumstances, it is not necessary to perform a detailed market analysis. *See Ind. Fed'n of Dentists*, 476 U.S. at 460-61 ("Since the purpose of the inquiries into market definition and market power is to determine whether an arrangement has the potential for genuine adverse effects on competition, 'proof of actual detrimental effects, such as a reduction of output,' can obviate the need for an inquiry into market power, which is but a 'surrogate for detrimental effects.'") (quoting 7 Phillip E. Areeda, Antitrust Law ¶ 1511, at 424 (1986)). *See also* FTC/DOJ Guidelines at 10-11, 26.

[41] *See Eastman Kodak*, 504 U.S. at 463; *see also Virtual Maint.*, 957 F.2d at 1318 (finding that company had market power over separate software support market for those companies doing business with an auto manufacturer with which company had an exclusive license);.

here is consumers and SMBs *affirmatively deciding* to provide access to account data in order to obtain competitive financial services. In the case of collaborative efforts, as the Department of Justice (DOJ) and Federal Trade Commission (FTC) have noted, "[a]nticompetitive harm may be observed, for example, if a competitor collaboration . . . successfully eliminates procompetitive pre-collaboration conduct, such as withholding services that were desired by consumers when offered in a competitive market."[42]

For example, the FTC and a number of states recently filed a complaint against a pharmaceutical company, alleging that the company engaged in anticompetitive practices by signing "data-blocking" agreements with distributors to stop critical sales data from being transferred to third parties.[43] In particular, the government alleged that the company, which had a monopoly over a certain drug for treating for a particular medical condition, entered into these agreements in order to "prevent[] the [downstream] companies from obtaining accurate information about [product] sales," and that "[b]y obscuring these sales, Defendants sought to prevent [potential competitors] for accurately assessing the market opportunity for a [competitive] product and thereby deter them from even pursuing development of a [competitive] product."[44] By allegedly thwarting competition, defendants protected their revenues and were able to charge higher prices.[45]

Moreover, the government specifically noted in that case that the restricted "sales data is not [the defendant's] to control."[46] Similarly, here, the consumer or SMB has the ability to access his or her financial information and provide it to another party, including a third-party competitor. Restrictions on sharing financial data *override* this customer choice to provide that information to third parties.

Another example is the FTC's policing of the market for transactional data involving real property. In 2014, the FTC challenged the acquisition of one data company by another based on a concern that the acquiring company would be able to take anticompetitive actions in the market for certain real property data—specifically, national assessor and bulk recorder data, which includes information about both the physical characteristics and transactions information of real property such as mortgage and lien records. The agency specifically noted the barrier to entry for new competitors in the market, including that "to compete effectively" in that market, "a firm must have several years of national historical data and an ability to provide go-forward national

---

[42] FTC/DOJ Guidelines at 12.

[43] Amended Complaint, *FTC v. Vyera Pharm. LLC*, No. 20-cv-00706 (S.D.N.Y. Apr. 14, 2020), *available at* https://www.ftc.gov/system/files/documents/cases/161_0001_vyera_amended_complaint.pdf.

[44] *Id.* ¶ 7.

[45] *Id.* ¶ 8.

[46] *Id.* ¶ 190.

data."[47] Similarly, many providers in the market for data-driven financial services rely on volumes of data that can only be gathered over time, such as transaction records used for cash-flow lending or personal financial management. Further, market participants need ongoing access to that data to provide valuable services to consumers.

In that same case, following a settlement requiring the licensing of the relevant data to a competitor, the FTC later found that degradation in data transfer to the potential competitor posed a competitive risk. In particular, the FTC found that the defendant "slowed [the competitor's] acquisition of the full scope of . . . bulk data," and "soon after [the defendant] began delivering bulk data to [the competitor, it] discovered that the deliveries were missing certain required data."[48] The FTC therefore modified the order to ensure sufficient transfer of data to ensure competition was protected. Similarly, here, the degradation of certain data, including the omission of certain data fields, can pose serious competitive risk.

In other markets as well, the FTC and DOJ have challenged mergers of parties controlling highly specialized data out of a concern that potential restrictions on that data would result in anticompetitive effects. For example, the DOJ blocked a transaction involving the two leading providers of inventory management solutions (IMS) for automotive dealerships out of concern that the new company would control substantially more vehicle information data, which is difficult to assemble, than anyone in the market.[49] The DOJ was particularly concerned that the acquisition would allow the new company to "deny or restrict access to [the covered] data and thereby unilaterally undermine the competitive viability" of competitors in the market for inventory management solutions.[50] To allow the deal to proceed, the DOJ required the acquiring company to divest its interest in part of the business, and to "enable the continuing exchange of data and content between the divested IMS business and other data sources, internet sites and automotive solutions that [it] will control."[51]

---

[47] *CoreLogic, Inc.*, F.T.C. No. 1310199, at 3 (May 21, 2014), https://www.ftc.gov/system/files/documents/cases/140324corelogiccmpt.pdf (complaint).

[48] *CoreLogic, Inc.*, F.T.C. No. 1310199, Docket No. C-4458, at 2 (June 15, 2018), https://www.ftc.gov/system/files/documents/cases/c4458_corelogic_order_to_show_cause_and_order_modifying_order_06142018.pdf. (show cause order and order modifying order).

[49] Complaint, *United States v. Cox Enters., Inc.*, No. 1:15-cv-01583 (D.C. Cir. Sept. 29, 2015), https://www.justice.gov/atr/case-document/file/779371/download.

[50] *Id.* at 8.

[51] Press Release, U.S. Dep't of Justice, Justice Department Requires Cox Automotive to Divest Inventory Management Solution in Order to Complete Acquisition of Dealertrack (Sept. 29, 2015), https://www.justice.gov/opa/pr/justice-department-requires-cox-automotive-divest-inventory-management-solution-order.

Similarly, the FTC challenged the merger of two companies with access to national syndicated cross-platform audience measurement,[52] finding that without access to the data, new entrants would not be able to join the market.[53] Ultimately, the acquiring company agreed to divest individual-level data per agreement with the FTC.[54] In another case, the FTC required a data processing company to sell copies of its title plant databases to other competitors in Oregon following an acquisition of a competitor,[55] noting that title plant databases need to be used by entities seeking to ascertain the title status of property.[56] The FTC also challenged an acquisition that would have left one entity with more than 90% of the relevant market for educational marketing data,[57] out of concern that such control over educational marketing data would create a barrier to entry for potential new entrants. It concluded, "A new entrant or expanded fringe firm would need an up-to-date database with the size, breadth and scope of market coverage comparable, at a minimum, to that held by [one company] prior to the [a]cquisition."[58] And the agency challenged a transaction that would have combined the two leading providers of electronic public record services,[59] requiring the divestiture of certain electronic public data assets to a competitor.[60]

B. Overriding Consumer-Permissioned Access for Data-Driven Financial Services Generally Do Not Have Procompetitive Benefits.

The anticompetitive effects of restricting customer-directed data sharing to competitors are not generally outweighed by any procompetitive benefits. To be sure, certain restrictions may be necessary to stop fraudulent or similar conduct. In the current marketplace, stakeholders are

---

[52] *Nielsen Holdings NV*, F.T.C. No. 1310058 (Sept. 20, 2013), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130920nielsenarbitroncmpt.pdf (complaint).

[53] *Id.* at 3.

[54] Press Release, FTC, FTC Approves Nielsen Holdings N.V. and Nielsen Audio, Inc.'s Application to Sell its LinkMeter Technology and Related Assets to comScore, Inc., FTC (April 2, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-nielsen-holdings-nv-nielsen-audio-incs-application.

[55] *Fidelity National Financial, Inc.*, F.T.C. No. 131-0159 (Dec. 23, 2013), https://www.ftc.gov/sites/default/files/documents/cases/131224fidelitystatement.pdf (agency statement).

[56] *Fidelity National Financial, Inc.*, F.T.C. No. 131-0159, Docket No. C-4425, at 3-4 (Dec. 24, 2013), https://www.ftc.gov/sites/default/files/documents/cases/131224fidelityc/mpt.pdf. (complaint).

[57] *Dun & Bradstreet Corporation*, F.T.C. No. 9342 (May 7, 2010), https://www.ftc.gov/sites/default/files/documents/cases/2010/05/100507dunbradstreetcmpt.pdf (complaint).

[58] *Id.* at 4.

[59] *Reed Elsevier NV*, F.T.C. No. 0810133, Docket No. C-4257 (June 5, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2008/09/080916reedelseviercpdo.pdf (decision and order).

[60] *Id*. at 10.

working together to address fraud and consumer protection concerns while competition continues. A broad restriction on customer-directed data sharing, or targeted restrictions on certain data that is useful for competitors, would not advance these goals.

Moreover, a rule of reason analysis under antitrust laws requires looking at whether conduct will result in "cognizable efficiencies," which are those not arising from anticompetitive reductions in output or service, and that cannot be achieved through practical, significantly less restrictive means.[61] These may include efficiency improvements, higher output, increased quality, or product innovation, and must provide some cognizable economic benefit.[62]

Restricting customer-directed data sharing to third-party competitors would not advance any of these goals, as a general matter. There are two broad concerns that stakeholders must manage in dealing with financial data sharing: regulatory requirements and consumer protection concerns such as fraud and data security. However, no law or regulation requires financial institutions to broadly restrict customer-directed access to competitors or to selectively restrict sharing of certain data to competitors. And stakeholders have been working collaboratively to deal with consumer protection concerns for years without resorting to broad data blocking or targeted restrictions on certain data, which in fact would undermine those efforts. Indeed, all financial services competitors are subject to consumer protection oversight and accountable to the very customers who direct them to access their financial data.

1. No Law or Regulation Compels Broad Data Access Restrictions.

a. Gramm-Leach-Bliley Act.

The primary law governing sharing of consumer financial information, the Gramm-Leach-Bliley Act (GLBA), has not been an impediment to consumers choosing to share their financial information with aggregators and third parties. In general, GLBA requires financial institutions to provide consumers with a notice and an opportunity to opt out prior to a provider sharing their nonpublic personal information with non-affiliated companies.[63] Financial institutions may also share nonpublic personal information with consent or at the direction of the consumer necessary to effect a transaction requested or authorized by a consumer.[64] GLBA also contains information security provisions, but these also do not block customer-directed transfer. In particular, the federal banking regulators have provided guidance that "access to or use of

---

[61] FTC/DOJ Guidelines at 23.

[62] *See, e.g., Broad. Music, Inc. v. Columbia Broad. Sys., Inc.*, 441 U.S. 1, 19-20 (1979); *Nat'l Coll. Athletic Ass'n v. Bd. of Regents*, 468 U.S. 85, 117 (1984); *Paladin Assocs. v. Mont. Power Co.*, 328 F.3d 1145, 1157 (9th Cir. 2003); *Toys "R" Us, Inc. v. FTC*, 221 F.3d 928, 938 (7th Cir. 2000).

[63] 15 U.S.C. § 6802(a).

[64] *Id.* § 6802(e).

customer information is not 'unauthorized' access if it is done with the customer's consent," and that "[w]hen a customer gives consent to a third party to access or use that customer's information, such as by providing the third party with an account number, PIN, or password, the Guidelines do not require the financial institution to prevent such access or monitor the use or redisclosure of the customer's information by the third party."[65]

In short, if a consumer has directed access to an account, GLBA does not pose an impediment to sharing data with a third party. In particular, it does not require a financial institution to re-confirm permission for data sharing from a consumer—which, if done repeatedly, can sharply and unnecessarily degrade the quality of the service a consumer receives from a competitive service.

b. EFTA and Regulation E

While the full applicability of the Electronic Fund Transfer Act (EFTA) and its implementing Regulation E remains somewhat unsettled in different kinds of data transfer arrangements, it is not a legitimate basis for restricting customer-directed data access. In general, EFTA and Regulation E limit consumers' liability for unauthorized electronic fund transfers from their accounts under certain conditions. Unauthorized transfers generally are those that are "initiated by a person other than the consumer without actual authority to initiate the transfer."[66] However, where consumers furnish "access devices" to another party, financial institutions can treat transactions as authorized until they are informed otherwise by a consumer. Financial institutions have therefore argued that providing authentication credentials, or an authorization to use an API, would constitute provision of an "access device" for purposes of allocating legal liability.

The marketplace would benefit from additional regulatory clarity in this area, but regardless, Regulation E does not provide a justification for overriding consumer preferences for data sharing. When consumers direct third parties to access data, liability can be allocated among the parties in way that ensures that consumers have recourse in case of a data breach or other compromise that results in unauthorized access. As one recent report notes, "[f]irms are beginning to negotiate contractual indemnification clauses to address such situations, so that liability can be decided through negotiated settlement, arbitration, or litigation, depending on the individual contracts at issue."[67] Moreover, FDATA endorses the position that the party

---

[65] Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness, 66 Fed. Reg. 8616, 8620 (Feb. 1, 2001).

[66] 12 C.F.R. § 1005.2(m)

[67] FinRegLab Policy Report at 52.

responsible for consumer or SMB loss of funds must also be responsible for making the consumer or SMB whole, given sufficient evidence of that third party's responsibility, consistent with Regulation E. And in any event, contractual disputes on this issue would not be a justification for anticompetitive conduct.[68]

Nor is the analysis any different in the case of restricting consumer-permissioned data transfers to additional parties—for example, an aggregator providing cash-flow data to a SMB lending platform at the consumer's direction. The parties should be able to reasonably negotiate liability limitations without the need for a veto over downstream users. Moreover, in case of a data breach or other fraudulent conduct involving consumer data, the data aggregator already bears a risk of potential liability under, at a minimum, the FTC Act, state consumer protection laws, and, potentially, other state tort laws.[69] In short, consumers will have some recourse under the parties' contractual arrangements. It is certainly not *procompetitive* to override consumer choice based on potential differences in interpretation of Regulation E that can be resolved by good faith negotiations.

c. Fair Credit Reporting Act.

Some financial institutions argue that customer-directed data sharing should be restricted, at least for data used for lending decisions, due to obligations under the Fair Credit Reporting Act (FCRA). The FCRA generally imposes obligations on "consumer reporting agencies" (CRAs) that provide defined "consumer reports" for certain purposes. It also imposes obligations on recipients of those consumer reports and furnishers of information to CRAs. One "permissible purpose" covered by the FCRA is for use in connection with a credit transaction.[70]

However, restrictions on customer-directed data sharing are not required to meet FCRA obligations. First, data aggregators themselves are not functioning as "consumer reporting agencies." Section 603(f) of the FCRA provides, in part, that a "consumer reporting agency" is "any person which . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties…."[71] The FTC has released informal guidance that entities that perform "conduit functions" do not fall within this definition. In particular, the

---

[68] *See SD3, LLC v. Black & Decker (U.S.), Inc.*, 801 F.3d 412, 430 (4th Cir. 2015) (finding that plaintiff demonstrated a cognizable group boycott claim through, among other things, showing that defendants "offer[ed] only bad faith terms that were intended to be rejected").

[69] *See* discussion *infra* Section Part II.B.2.

[70] 15 U.S.C. § 1681 *et seq*.

[71] *Id.* § 1681a(f).

guidance notes that "[a]n entity that performs only mechanical tasks in connection with transmitting consumer information is not a CRA because it does not assemble or evaluate information," and "a business that delivers records, without knowing their content or retaining any information from them is not acting as a CRA" even if the recipient uses the information for a permissible purpose under the statute.[72] The FTC also states that "[a]n entity acting as an intermediary on behalf of the consumer who has initiated a transaction does not become a CRA when it furnishes information to a prospective creditor to further the consumer's application."[73]

Second, financial institutions are not "furnishers" of information under the FCRA, even if aggregators were deemed to be CRAs. The FCRA Furnisher Rule provides that a furnisher does not include "a consumer to whom the furnished information pertains."[74] In the case of permissioned consumer data access, the consumer is effectively providing the information, by authorizing its release directly from the financial institution. Instead, the statute requires some affirmative act by an entity to "furnish" information to qualify as a furnisher. As one recent comprehensive report notes, "We are not aware of any stakeholders that are actively pressing to treat banks and prepaid issuers as furnishers under the Fair Credit Reporting Act where cash-flow data is collected by an aggregator for use in credit underwriting."[75]

d. Third-party service provider oversight obligations.

Supervised financial institutions, such as banks, must comply with specific third-party service provider oversight obligations. The OCC, for example, has released guidance on third-party oversight that specifically addresses data aggregators and requires a level of due diligence.[76] However, in the case of arrangements with data aggregators, financial institutions can perform appropriate due diligence without broadly blocking customer-directed data access or selectively restricting data to competitors in an anticompetitive fashion. Indeed, the OCC's most

---

[72] FTC, 40 Years of Experience with the Fair Credit Reporting Act, at 29 (July 2011) *available at* https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

[73] *See id*. at 30; *see also id*. at 30-31. ("an entity does not become a CRA solely because it conveys, with the consumer's consent, information about the consumer to a third party in order to provide a specific product or service that the consumer has requested").

[74] 16 C.F.R. § 660.2(c)(3).

[75] FinRegLab Policy Report at 86.

[76] *See* Office of the Comptroller of the Currency, OCC Bull. 2013-29, Third-Party Relationships: Risk Management Guidance (2013), *available at* https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html; OCC 2020 Guidance, *supra* note 28.

recent guidance, in March 2020, makes clear that banks must follow antitrust laws in their dealings with third parties.[77]

While arrangements between aggregators and financial institutions can vary in certain circumstances, in the case of customer-directed access to financial information, the relationship is generally at the low end of third-party risk for the institution. The OCC's March 2020 guidance, for example, recognizes a sliding scale when banks deal with aggregators accessing consumer-permissioned data. It notes that, "In many cases, banks may not receive a direct service or benefit from these arrangements. In these cases, the level of risk for banks is typically lower than with more traditional business arrangements."[78] In contrast, obligations are higher when the bank engages a third party in a contract to perform some bank function—for example to use data aggregators to obtain data from other sources to help offer services to their existing customers.[79]

To be sure, OCC guidance suggests that banks must still manage aggregator relationships in a "safe and sound manner with consumer protections," that "banks still have risk from sharing customer-permissioned data with a data aggregator" even absent a business arrangement, and that "[b]ank management should perform due diligence to evaluate the business experience and reputation of the data aggregator to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data." For agreements enabling customer-permissioned data sharing, "banks should gain a level of assurance that the data aggregator is managing sensitive bank customer information appropriately given the potential risk." For situations involving credentialed access without a third-party agreement, which the OCC acknowledges does not constitute a business relationship, "banks should take appropriate steps to identify the source of these activities and conduct appropriate due diligence to gain reasonable assurance of controls for managing this process."[80]

---

[77] OCC Guidance, *supra* note 28. The OCC guidance points to other situations where information sharing about legitimate due diligence and monitoring can be efficiently shared. But those guidelines apply to third-party relationships generally, which in most instances will not involve relationship with potential competitors. In contrast, in this case, the third parties subject to diligence *are* the potential competitors.

[78] *Id*.

[79] For example, from the 2020 Guidance: "A business arrangement exists when a bank contracts or partners with a data aggregator to use the data aggregator's services to offer or enhance a bank product or service. Due diligence, contract negotiation, and ongoing monitoring should be commensurate with the risk, similar to the bank's risk management of other third-party relationships." *Id.*

[80] *Id*. Additionally, it notes that "[t]hese efforts may include research to confirm ownership and understand business practices of the firms; direct communication to learn security and governance practices; review of independent audit reports and assessments; and ongoing monitoring of data-sharing activities."

Particularly for established firms in the financial services marketplace, banks can conduct this due diligence without broadly restricting the flow of data or targeting certain data fields when the data sharing is directed by the consumer. FDATA members, for example, have years of established history providing consumer-permissioned access to data and safeguarding that data. They regularly communicate about their security practices—by proactively flagging potential fraudulent conduct to banks, for example. They also conduct independent third-party security audits and have a track record of demonstrating controls over sensitive information. Moreover, unlike many other service providers, data aggregators and other data-driven financial service providers are directly accountable to *their own customers*.

Further, while FDATA supports the move to APIs, third-party guidance would not justify restricting customer-directed data sharing via permissioned credentialed access, which has been going on for years, in the absence of an existing, workable API solution. Third-party oversight certainly does not justify second-guessing a consumer's decision to direct access to *certain data fields* to a potential competitor, since the level of security and controls that a company has will not differ by the kind of data. While third-party oversight obligations are important, as the OCC has emphasized, they must respect antitrust laws when competitors are involved.[81]

2. Consumer Protection Concerns are Better Addressed by Collaborative Efforts than Unilateral Restrictions on Customer-Directed Data Sharing.

All members of the financial services ecosystem are concerned about preventing fraudulent activity and securing consumer financial data. Indeed, all entities that deal with financial information are subject to legal obligations to implement reasonable data security measures. However, broadly overriding customer-directed data sharing, or selectively suppressing the sharing of certain data fields, does not effectively advance consumer protection goals. Certainly, from a competition standpoint, such restraints do not advance any procompetitive goal or do so in a manner that could not be achieved in a less restrictive way.[82]

---

[81] OCC guidance also discusses diligence over third parties' subcontractors, including oversight and risk control. Aggregators' relationships with financial services companies that are its own customers do not fit neatly into this framework. Moreover, these companies have additional incentives to safeguard consumer data, not only as a legal matter but because they answer directly to their customers who grant them permission to access their data. Regardless of the degree of downstream "fourth-party" oversight that may be appropriate in any particular case, restricting data to only certain downstream competitors, or restricting data fields of use primarily to certain downstream competitors, directly raises the kinds of competition concerns outlined in Section II.A, above.

[82] *Am. Express*, 138 S. Ct. at 2284.

First, in addition to the established history of consumer financial data sharing with appropriate safeguards, the risks of data sharing are constrained by the fact that data aggregators and competing data-driven financial services companies are themselves subject to legal obligations to secure financial information. As a baseline, all for-profit entities are subject to Section 5 of the FTC Act, which the FTC has interpreted as requiring "reasonable" data security measures.[83] This requirement includes taking measures to appropriately secure consumer financial information from fraud.[84] Entities that fail to implement reasonable measures are subject to enforcement by the FTC, state enforcement officials, and potentially others. Similarly, the FTC actively polices companies' privacy representations and brings enforcement actions when consumers are misled about the scope of data sharing, including consumer financial information.[85]

Additionally, all "financial institutions" as defined in Gramm-Leach-Bliley Act are subject to the GLBA Safeguards Rule. This rule requires establishment of a "comprehensive information security program" that is "appropriate to [a company's] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."[86] It also requires that a company identify "reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks," including "[d]etecting, preventing and responding to attacks, intrusions, or other systems failures."[87]

Second, unilateral restrictions on customer-directed data access make it *more difficult* to implement effective data security. A financial institution may be concerned, on a case-by-case basis, that a request for financial data is fraudulent and customer financial information may be compromised. However, having two or more points of fraud detection—one at the aggregator level and one at the financial institution—would potentially increase the security on the account.

---

[83] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015); FTC, *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[84] *E.g.*, Complaint, *FTC v. Equifax Inc.*, No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), *available at* https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf; *LightYear Dealer Technologies*, F.TC. No. 1723051, Docket No. C-4687 (FTC 2019), https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_final_complaint.pdf (complaint).

[85] *E.g.,* Complaint*, FTC v. Blue Global, LLC*, 2:17-cv-2117-ESW (D. Ariz. July 3, 2017), https://www.ftc.gov/system/files/documents/cases/ftc_v_blue_global_de01.pdf; *Goal Financial, LLC*, F.T.C. No. 0723013 Docket No. C-4216 (Apr. 9, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/04/080415complaint_0.pdf (complaint).

[86] 16 C.F.R. § 314.3(a).

[87] *Id.* § 314.4(b).

Additionally, blanket restrictions will not stop all consumers from providing financial information directly to competing financial services. For example, a customer facing a blanket restriction on sharing account numbers via a secure third-party aggregation service may provide account numbers directly to competing financial services. That is *less* secure than sharing such information via an aggregator coordinating the data exchange directly with the financial institution. Overriding customer-directed access would lead to consumer workarounds that would be inherently less secure. In this area, cooperative approaches to data security are more effective than unilateral approaches.

Third, outside of normal fraud prevention practices, the procompetitive benefits of overriding consumer decisions to share data, either broadly or on a use case level, are dubious. In *Indiana Federation of Dentists*, for example, the Supreme Court rejected the defendants' argument that an anticompetitive agreement to broadly withhold x-rays from insurers was justified to prevent inadequate treatment. Describing this argument as "in essence, that an unrestrained market in which consumers are given access to the information they believe to be relevant to their choices will lead them to make unwise, and even dangerous, choices," the court held that the defendants' position was "nothing less than a frontal assault on the basic policy of the Sherman Act."[88] The court further noted that the potential competitors had an incentive to compete on quality for their own customers[89]—just as here, data-driven financial service providers have an incentive to provide valuable services to their customers.

Conclusion

Third-party financial services providers are today fueling tens of millions of American consumers' and SMBs' financial wellbeing through the provision of products and services that compete directly with those offered by traditional financial institutions. Competition issues in the marketplace are therefore critically important to ensuring that Americans maintain access to critical technology-powered financial tools as consumers and SMBs alike deal with a challenging economic landscape. Robust competition in data-driven financial services will deliver lower costs, better services, and better outcomes for consumers' and SMBs' financial outlook. Overriding consumers' and SMBs' direction to share data to obtain the benefit of these financial services would pose a significant harm to competition and to consumers and SMBs nationwide.

[88] *See* 476 U.S at 463; *see also Nat'l Soc'y of Prof'l Eng'rs v. United States*, 435 U.S. 679, 695 (1978) ("[i] n our complex economy the number of items that may cause serious harm is almost endless . . . [t]he judiciary cannot indirectly protect the public against this harm by conferring monopoly privileges on the manufacturers").
[89] 476 U.S at 463.