HOLDING COMPANY

12345 WEST COLFAX AVENUE LAKEWOOD, COLORADO 80215 303-232-3000

Statement for the Record

of

James Reuter

for the

CFPB Symposium

on

Dodd Frank Act Section 1033 and Data Aggregation

February 26, 2020

My name is Jim Reuter President and CEO of FirstBank, located in Lakewood Colorado. Founded in 1963, FirstBank has 118 locations, operating in Colorado, Arizona, and California. We have $19.5 billion in assets and employ over 3,000 people. I also serve on the board of the American Bankers Association[1]. This statement and my comments today will express both my banks views as well as those of the banking industry.

The topic of this symposium is timely. The issues surrounding the use and sharing of consumer financial data are critical. It is important that we get this right for our industry and more importantly for consumers across the country. At FirstBank, we support our customers' ability to share their financial data and remain committed to ensuring that they are in the driver's seat when it comes to their data with the appropriate protections and controls. As they access their data using services created by technology companies, it is imperative that their data be protected, they have complete control, and the providers of the services be held accountable to meeting this expectation.

As banks innovate, they do so within an established regulatory framework, backed by strong supervision and oversight, that ensures robust customer protection. Innovation is also taking place outside of the banking space. Technology-focused startups are building products that rely on access to consumer financial data. As a result, the demand for consumer financial data has increased dramatically, creating a market for this data.

We believe that if handled appropriately, access to this data can benefit consumers. This is why we fully support our customer's ability to access and share their financial data in a secure, transparent manner that gives them control. We are working alongside other banks, aggregators, and fintech companies to build the tools that facilitate access to financial data in a way that protects and empowers consumers.

However, it is important to note that sharing financial information is not the same as sharing information about where a consumer ate dinner or recently vacationed. Consumer financial data are extremely sensitive and must be protected appropriately. Accordingly, Congress has recognized the sensitivity of financial information and has provided protections for it in the Gramm-Leach Bliley Act of 1999 (GLBA)–obligations that apply to all parties that hold it throughout its lifecycle.

Banks take very seriously their responsibilities to their customers to maintain the highest level of privacy, security, and control over their financial assets and transactions. Today, consumers trust that their financial data are being protected and handled appropriately. This trust is critical to the functioning of the financial system and is the reason banks dedicate significant resources to safeguarding financial data.

Current practices in the data aggregation market, however, may leave consumers exposed and create risks that undermine this trust. Legacy processes known as "screen scraping" require users to forfeit

[1] The ABA is the voice of the nation's $17.9 trillion banking industry, which is comprised of small, midsized, regional and large financial institutions. Together, these institutions employ more than 2 million people, safeguard $14 trillion in deposits and extend more than $10 trillion in loans

their bank username and password, granting technology companies unfettered access to a customer's most sensitive data. When this happens, customers – often unknowingly – trade their privacy for technology-driven convenience in a way that exposes them to serious financial risk. Consumers often do not fully understand what data is being taken, where it is being sent, or how it is being used.

Banks, aggregators, and technology companies are all aligned on the need to move away from these legacy technologies that create risk to more secure technologies like APIs and are working together to make rapid progress toward this goal.

The Consumer Financial Protection Bureau's (CFPB) 2017 principles[2] have been key to this progress. These principles have served as a flexible bedrock for industry discussion that has facilitated real progress. Since the principles were released, Industry collaboration has led to the development of technical standards, model contracts, and other technologies that can help facilitate responsible sharing. I believe that continued industry collaboration is the best way to advance this goal. While there are several regulatory clarifications that can help facilitate progress, too much action by the CFPB risks freezing the market and would slow progress to enable responsible data sharing.

ABA Principles for Responsible Data Sharing

Through my work at ABA we have developed a set of principles – consistent with the CFPB and the rest of industry – that we believe ensure that consumers remain protected when they share their financial data. These principles reflect the principles of not only the industry, but also those of FirstBank.

1. Access

   Banks support our customer's ability to use third-parties to access their financial account data in a way that is safe and secure.

2. Security

   Consumers deserve bank-level security and protection regardless of where they choose to share their data. This means that consumer data are treated the same – and subject to GLBA protections – whether at a bank or a third party.

3. Transparency

   Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data a technology company are accessing, how long the company is holding this data, and how it is using the data.

4. Control

   When consumers share their financial data, they should have control over what information is shared and how it is used. Intuitive control would allow consumers to see easily who is authorized to receive their data, modify what access they have, and revoke that access when a service is no longer used. If consumers can easily control the data being accessed, they can better understand what is being used and protect themselves accordingly.

[2] https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

5. Minimization

Consumers should expect that data-sharing is limited to the data that are needed to provide the service they have authorized and only maintain these data as long as necessary. Limiting sharing to necessary data helps minimize privacy risks and allows consumers to better understand what kind of data is being accessed and used. Services that go beyond financial account aggregation, such as money movement, present different risks and should be subject to separate agreements and require separate informed consent.

Industry Driven Progress

I believe that collaboration between banks, technology companies, and data aggregators is the best way promote an ecosystem that facilitates responsible data sharing. The significant industry progress in recent years demonstrates this to be true. There are several separate, but related pieces needed to build an ecosystem that supports responsible sharing that include 1) technical standards to securely move the data from point A to point B, 2) contracts that make it easy for banks to work with aggregators, and 3) permissioning systems that track and manage consumer consents.

Technical Standards (APIs):

It is critical that we move away from legacy processes like "screen scraping" that leave consumers exposed to risk and adopt technical standards that can securely move data from banks to aggregators and beyond. Application Programing Interfaces (APIs) serve as universal adaptors for data, allowing for more secure transmission of data between systems in a standardized format. This empowers customers to share financial data without forfeiting their bank-user credentials.

This is an area where industry has made significant progress. In the fall of 2018 banks, aggregators, and technology companies came together to found the Financial Data Exchange (FDX) out of a recognition that progress was only possible with the participation of a diverse group of stakeholders. FDX is a nonprofit formed to develop a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data. FDX has developed an API that can facilitate secure data sharing among all these parties. FirstBank is a member of FDX alongside many other banks, technology companies and aggregators.

The nature of innovation means that things are constantly changing, and it is important to note that no one technology will always be the right tool to facilitate secure data transmission. There are also many different APIs for different solutions and while APIs are the best technology today, we need the flexibility to adopt new technologies as the business of banking evolves. Technology mandates would lock us into legacy technologies and risk undermining both safety and innovation.

Legal Contracts

In order to move to API standards, banks and data aggregators must enter into legal contracts that dictate how data is accessed and protected. These contracts are critical to ensuring that customers remain protected and that their data is afforded bank-level protections when it is shared.

This area is a particular challenge for banks of my size, and one that only gets worse for smaller institutions. Data aggregators devote significant resources to establishing relationships with larger institutions that represent a significant portion of the deposit base. These negotiations allow banks to ensure that the appropriate protections are in place when their customers' data is accessed. However, many data aggregators simply don't have the resources to engage with a bank of my size.

With legacy practices like "screen scraping" the aggregator has no direct relationship with the bank. This is because from a bank's perspective, the aggregator looks like our customer. They effectively show up on a banks website and enter login credentials and access an account. In our systems, we can see logins that are clearly are driven by computers, not our customers. In these cases, it can be hard to discern a consumer-authorized data aggregator from a malicious actor trying to gain access to our customer's account. Our bank is somewhat unique in our ability to monitor these logins, because we own our entire technology stack. Many community banks rely on core providers to power their IT systems and lack the tools to get this kind of insight.

Implementing an API requires a contract that governs the use of that API and ensures the bank's data security and privacy requirements are being honored. However, negotiating these contracts is an expensive and time-consuming process, often taking as long as 12 months. While larger institutions have the resources and scale to engage in these negotiations, community banks typically lack the resources to negotiate directly with aggregators.

The Clearing House (TCH) recently released a template agreement known as the Model Data Access Agreement designed to improve the process of contract negotiations. The model agreement was designed in consultation with banks and technology companies. This model contract is voluntary and is intended to be modified as individual circumstances may warrant. Additionally, it avoids taking positions on commercial terms that would be negotiated between parties. The contract does, however, provide for a common ground from which banks can engage with aggregators.[3]

Permissions

The third key component of empowering consumers to securely share their financial data is a permissioning system. Unlike the first two efforts, these are not industry-wide efforts, but typically done at the bank level as it is part of a bank's digital experience. These systems are key to facilitating transparency and consumer control over their data. Permissioning systems track where a consumer has consented to share their financial data and provide a transparent portal to that allows them to understand what data are shared, limit the data that are shared, and revoke access altogether.

Many large banks have unveiled permissioning platforms, Wells Fargo's "Control Tower" is just one example. However, this technology is largely unavailable to community banks today as it is not offered by their core banking platforms. These core providers play a critical role in ensuring that community banks have the tools to meet market demand and remain competitive in a digital economy.

Recommendations

I believe a market-driven approach is the best way to empower consumers to control their financial data. There are, however, several regulatory and legal clarifications the CFPB can make to give banks like mine the confidence we need to adopt industry solutions.

I believe the following recommendations are necessary to ensure that customers of all banks – regardless of their asset size – can control their financial data and fully benefit from financial innovation.

[3] https://www.theclearinghouse.org/connected-banking/model-agreement

The CFPB should clarify that GLBA applies to data aggregators

U.S. law has long accorded special status to consumer financial information given the sensitivity of the information. To ensure consumer financial information is properly secured, it is subject to laws related to privacy, data protection, and restrictions on data use and accessibility. For example, the Gramm-Leach-Bliley Act of 1999 (GLBA) imposes on financial institutions obligations to respect customer privacy and to safeguard financial information. Specifically, Section 501 of that law imposes on financial institutions an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[4]

Consumers should expect that their financial data is protected whether it is held by a bank or a data aggregator. As discussed above, GLBA provides a robust framework to protect "nonpublic personal information" of a consumer that is held by a "financial institution." Data aggregators fall under the GLBA's definition of "financial institution" and therefore should be subject to all the rules that apply to all other financial institutions. This assures that data protections apply consistently regardless of where the data originated, where it is transferred, and the type of company is using or storing the data.

Congress used an intentionally robust and expansive definition of "financial institution" in GLBA, which encompasses "any institution the business of which is engaging in financial activities as described in [the Bank Holding Company Act of 1956, section 4(k).]"[5] This definition includes not only banks, but as interpreted by the Board of Governors of the Federal Reserve, the definition encompasses any entity that provides data processing, data storage and data transmission services for financial data. In other words, GLBA clearly applies to data aggregators.

While I believe it is clear that GLBA applies to data aggregators, any confusion in the market could stifle the progress toward moving to more secure methods of data sharing. Therefore, the CFPB should articulate clearly that data aggregators fall within GLBA's definition of "financial institution" subject to the requirements of GLBA as they apply to other financial institutions. This would ensure that consumers receive the GLBA security protections as implemented by the Bureau's Regulation P and the FTC's Safeguards Rule.

The CFPB should bring data aggregators under direct supervision

By the nature of their business, data aggregators hold a tremendous amount of consumer financial data. It is estimated that data aggregators hold the consumer login credentials for tens of millions of customers. Despite this, many consumers don't know that these intermediaries exist or how much of their information is being collected. In most cases consumers do not have a direct relationship with these companies and must trust that their data is being handled appropriately.

As discussed above data aggregators are subject to GLBA, but their compliance with its privacy and security obligations is not clear and, more important, is not subject to supervision or regular examination. Proactive supervision is critical to identifying risks before any harm is done to consumers.

A cornerstone of Title X of the Dodd-Frank Act was the authority given to the CFPB to establish a supervisory program for nonbanks to ensure that federal consumer financial law is "enforced

[4] 15 U.S.C. § 6801(a)

[5] 15 U.S.C. § 6809(3).

consistently, without regard to the status of a person as a depository institution, in order to promote fair competition." Experience demonstrates that consumer protection laws and regulations must be enforced in a fair and comparable way if there is to be any hope that the legal and regulatory obligations are observed. Establishing accountability across all providers of comparable financial products and services is a fundamental mission of the Bureau. This is especially important for data aggregators, given the sensitive consumer financial information they store and process.

The bulk of the data processing in this area is managed by a select group of large companies. Accordingly, the CFPB should initiate the rulemaking process under Dodd-Frank Act 1024 to define those "larger participants" in the market for consumer financial data that will be subject to regular reporting to and examination by the CFPB. Once the Bureau has imposed supervisory authority over the larger data aggregators, the CFPB can better monitor – and react to – risks to consumers in this rapidly evolving marketplace.

The CFPB should clarify liability for unauthorized transactions under Regulation E

Under §1005.14 of Regulation E, a person that provides an electronic fund transfer service to a consumer is generally subject to Regulation E, with certain modifications, if it (1) issues an access device that the consumer can use to access the consumer's account held by a financial institution and (2) has no agreement with the account-holding institution regarding such access.

Data aggregators that permit consumers to initiate electronic fund transfers from accounts held at financial institutions that do not have an agreement with the financial institution are "service providers" under Regulation E, as they issue "access devices"[6] that may be used to permit electronic fund transfers to and from the account. As service providers, they are liable for unauthorized transactions under Regulation E as well as certain other provisions.

Imposing liability for unauthorized transactions under these circumstances is appropriate and fair. The data aggregator is in the best position to control the risk of unauthorized transactions conducted through its system. In contrast, the financial institution holding the account has no relationship with the data aggregator, no knowledge of, and no power over the data aggregator's security system. This approach is consistent with payment system laws which generally assign liability to the party that is in the best position to avoid a loss and manage the risk of a loss. Indeed, it is for these reasons that Regulation E assigns liability to service providers.

Moreover, other provisions related to service provider responsibilities support classifying data aggregators as service providers under Regulation E. These include requirements related to error resolution, disclosures, the prohibition against the issuance of unsolicited access devices, and change in terms notices.

To avoid any ambiguity, the CFPB should confirm this in the regulation or official commentary.

[6] Under Section 1005.2(a) of Regulation E, "Access device means a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers."

Banking regulators should clarify that bank agreements with data aggregators do not constitute third-party vendor relationships

Notably, data aggregators are authorized by and act on behalf of bank customers, not the bank. When banks enter into agreements with data aggregators, they do so to reduce risk and to apply additional protections to their consumers' data as it leaves the secure banking environment.

Section 7 of the Bank Service Company Act (BSCA) requires banks to notify their regulators of contracts or relationships with certain third-party service providers and undertake due diligence on these partners. This is intended to capture relationships where banks partner with third parties to deliver experiences to their customer. In the case of data aggregators, there is no such partnership. A consumer has directed his or her bank to share their data; a bank's contract simply lays out the terms for how that data is shared and provides a more secure portal for doing so. Such a contract should not result in the data aggregator becoming a third-party service provider to the bank. Rather, the relationship should be regarded as a customer-aggregator relationship.

A lack of clarity about the applicability of the BSCA to contracts with data aggregators could stifle adoption of more secure technologies that provide additional protections for customers. Moreover, banks have little ability to perform due diligence or supervise these data aggregators because the aggregators have no incentive to respond to bank due diligence requests since there is no business relationship between the bank and the aggregator. The CFPB should coordinate with the prudential banking regulators to ensure that relationships between banks and aggregators are not considered third-party vendor relationships.

Core providers should offer community banks the tools to facilitate secure data sharing

My bank is unique for my size in that we own our entire technology stack. Most community banks rely on technology infrastructure from companies that provide software systems known as core banking platforms. Core technology supports everything from accepting deposits to originating loans, all of which tie into operating the core ledger that keeps track of customers' accounts. For many banks, their core provider is the heart of their IT infrastructure. Without the support of these core providers, it would be impossible for community banks to offer the API access or permissioning systems that the market demands today.

ABA has engaged with the core providers through its banker driven Core Platforms Committee, made up of community and mid-sized banks, in an effort to strengthen relationships between banks and cores. One of the key priorities that this committee has identified is data access. Community banks often struggle to quickly and easily access the data held in their core platforms, much less facilitate access for third parties. For community banks to remain competitive, it is critical that the core providers engage in industry efforts and adopt technologies that facilitate the secure data sharing that customers demand.

Conclusion

Today, technology is fundamentally changing the way financial services are being delivered. Consumer financial data is more available and widely shared than ever before. I believe that innovation in financial services present tremendous value. This value is only realized when innovation is delivered in a responsible manner that maintains the trust that is critical to the functioning of our financial system. The focus on the consumer financial data market is important.

By fairly addressing both the opportunities and risks, we have the ability to give consumers innovative services that they can trust. Customers need security, transparency and control to unlock the true potential of fintech and take charge of their financial future.