Statement for the Record

On Behalf of the

American Bankers Association

Before the

Task Force on Financial Technology

Of the

Financial Services Committee

September 21, 2021

American Bankers Association®

Statement for the Record

On Behalf of the

American Bankers Association

Before the

Task Force on Financial Technology

Of the

House Financial Services Committee

September 21, 2021

Chairman Lynch and Ranking Member Davidson, thank you for the opportunity to submit this statement for the record for the hearing titled "Preserving the Right of Consumers to Access Personal Financial Data."

The topic of today's hearing is a timely one that is getting increasing attention. As consumers access novel financial services offerings, it is critical to ensure they retain the protections they have come to expect from their bank. The American Bankers Association (ABA)[1] and our members are working hard to ensure that consumers remain protected when they choose to share their financial data.

Technology has facilitated the creation of a tremendous amount of consumer financial data. The unprecedented proliferation and availability of this data have enabled the development of new financial innovations that stand to benefit customers. However, the inherent sensitivity of this data and the discussion around the appropriate role of large technology companies in banking highlight the timeliness of this issue and the need to ensure that financial data are handled appropriately and securely.

We believe that responsible innovation in financial services will continue to benefit customers as it has throughout the history of banking. The use of data plays a critical role that can help promote competition and financial inclusion, make it possible to extend credit to many more borrowers, and give customers improved transparency into the financial products they use every day.

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

We believe that if handled appropriately, access to these data can benefit consumers**. This is why ABA and our members fully support their customers' ability to access and share their financial data in a secure, transparent manner that gives them control.** Today, banks and technology companies are collaborating to build tools that facilitate access to financial data in a way that protects and empowers consumers.

However, sharing financial information is not without risks. Consumer financial data are extremely sensitive and must be protected appropriately. Accordingly, Congress has recognized the sensitivity

[1] The American Bankers Association is the voice of the nation's $22.8 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard nearly $19 trillion in deposits and extend $11 trillion in loans. Learn more at www.aba.com.

of financial information and has provided protections for it under the Gramm-Leach Bliley Act of 1999 (GLBA), which creates a legal framework for protecting consumer data, and for sharing that data with third parties. 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.

Consumers understand the importance of protecting their financial data and are skeptical about the safety of their data when shared outside of the bank. This was highlighted by recent data from a Morning Consult survey that showed "U.S. Adults Among the Most Concerned With Data-Sharing Fraud." In the survey 63% of respondents believed that more sharing of data between financial services companies will lead to more fraud. [16% disagreed] The survey also highlighted privacy concerns, with 48% of respondents reporting that they are unwilling to "share their financial information with a provider that I do not currently use if it meant they would offer me a personalized financial management services." [34% were willing] [2]

There is significant work underway to ensure that consumers can share their financial data while maintaining these critical protections. In 2017, under then Director Richard Cordray, the Consumer Financial Protection Bureau (CFPB) released a set of guiding principles that has served as the bedrock for industry collaboration. Since then banks, data aggregators, and other technology companies have worked together to invest in technologies that move away from less secure methods of data sharing like screen scraping to more secure Application Programing Interfaces (API) based standards that give consumers transparency and control when they share their financial data.

This work has been highlighted recently by the Executive Order on Promoting Competition in the American Economy[3], and is currently on the CFPB's rule-making agenda for April 2022.[4] As the CFPB considers next steps to encourage the development of a data ecosystem that protects consumers, we believe it should focus on supporting market developments that are already well underway. Overly prescriptive standards risk undermining the progress that has been made and if not well crafted, may leave consumers exposed. While we believe that continued industry collaboration is the best way to accomplish our shared goal, there are several regulatory clarifications and other recommendations that would help facilitate the continued development of a responsible data sharing ecosystem.

Given the critical role of the CFPB in this process, the remainder of our statement will make the following recommendations for the CFPB as it looks to encourage the development of this important market consistent with the rights outlined in Section 1033 of the Dodd Frank Act.

- Banks support consumers' right to share their data as outlined by the CFPB's principles;
- The industry has made tremendous progress since the CFPB released its principles;
- Prescriptive frameworks would be counterproductive to implementing Section 1033; and

[2] https://morningconsult.com/2021/09/07/open-banking-awareness/
[3] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/
[4] https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=3170-AA78

- There are areas where the CFPB can provide clarity to allow the market to continue to develop.

Banks support consumers' right to share their data as outlined by the CFPB's principles.

Technology is changing the way consumers engage with their finances and rapidly changing what consumers expect of their bank. Banks are responding to these market changes by investing in new technologies and partnering with startups to bring their customers the latest innovations. These technologies put the branch into consumers' pockets and make it easier to manage their finances. Today, customers expect to be able to access these services across the various platforms they use and to be able to share their data to access new financial services offerings. They also expect to remain protected wherever they receive their financial services. As a result, banks see the ability to allow consumers to securely share their financial data as critical to their competitiveness.

This is why banks have long supported[5] their customers' ability to share their financial data. However, making this data available is not as easy as flipping a switch. Banks are trusted custodians of their customers' most sensitive data and consumers expect the application of appropriate protections designed to maintain the safety and security of that information wherever they engage with their finances. We believe access to data is only part of the equation that must be supported by robust consumer protections to ensure it benefits, not harms, consumers.

The complexity of this issue and the importance of ensuring that consumers remain protected is why Congress gave the CFPB authority to prescribe standards to implement the rights outlined in Section 1033.

In 2017, the CFPB released a set of principles[6] to support responsible sharing of consumer data. According to then Director Richard Cordray, "these principles express our vision for realizing an innovative market that gives consumers protection and value." Importantly, these principles recognized the critical balance of ensuring consumers have the ability to share their data, while ensuring they remain protected when they do so.

These principles have served as a flexible bedrock for meaningful industry discussions that has facilitated real progress. Since the principles were released, industry collaboration has led to the development of technical standards, industry utilities, and other technologies and practices that can help enable responsible sharing.

ABA supports these principles which are consistent with our own long-held principles outlining what consumers should expect when they share their financial data.

1. Access

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

[5] https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2017/02/ABA-Comment-CFPB-Data-Aggregators.pdf
[6] https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

2.Security

Consumers deserve the same level of data security and protection afforded by regulated financial institutions ("bank-level") regardless of where and with whom they choose to share their data. This means that consumer data are treated the same – and subject to GLBA or substantively similar protections – whether at a bank or a third party.

3.Transparency

Consumers must have transparency about how companies use their financial data, including companies that they permit to access their data. It should be clear to consumers what data a technology company is accessing, which downstream parties are getting access to the data, how long the company is holding this data, and how the data is or may be used. This should be accomplished by affirmative consent and clear, accessible, and understandable legal disclaimers.

4.Control

When consumers share their financial data they should have control over what information is shared, how it is used, and for how long it may be 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.

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 to provide the service. Limiting sharing to necessary data helps minimize privacy risks and allows consumers to clearly 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. Where possible, aggregators should obtain sensitive personally identifiable data directly from the consumer.

The industry has made tremendous progress since the CFPB released its principles.

ABA believes that collaboration among banks, technology companies, and data aggregators is the best way promote an ecosystem that facilitates responsible data sharing. Since the CFPB released its principles in 2017, industry collaboration has led to tremendous progress that highlights the efficacy of this approach.

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.

Because of the strong progress that has been made in each of these areas, consumers are better protected when they share their financial data today.

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. 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. For more information on how APIs work, please refer to ABA's "Understanding APIs" report[7].

This is an area where industry has made significant progress. In the fall of 2018 banks, aggregators, and technology companies came together to establish 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 of these parties. ABA is a member of FDX alongside many of our member banks, technology companies, and aggregators.

The nature of innovation means that things are constantly changing, and no single technology will always be the right tool to facilitate secure data transmission. Moreover, flexibility is needed to accommodate the wide range of technologies banks currently employ. Prescriptive standards may prevent the most innovative companies from finding new, more secure methods of facilitating data sharing. There are also many different APIs for different solutions and while APIs are the best technology today, banks 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.

Contracts

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

With legacy practices like "screen scraping" the bank has no direct relationship with an aggregator. This is because from a bank's perspective, an aggregator looks like its customer. Aggregators effectively show up on a bank's website and enter login credentials and access an account.

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.

This is another area where the industry has made significant progress. Akoya is a network utility that makes it easier for banks and fintech apps to integrate API solutions. Akoya facilitates API connections by providing technical, legal, and security standards among financial institutions, data aggregators, and fintechs. This means that rather than having to create individual relationships with every aggregator or fintech, banks and fintechs can simply join the network and agree to a common set of rules designed to protect consumers. ABA recently hosted a podcast with Akoya and Jack

[7] https://www.aba.com/news-research/research-analysis/understanding-apis

Henry to discuss efforts developments that ensure community banks can offer their customers these products.[8]

Regulation also plays an important role here. Consistent regulation and proactive supervision of data recipients would make it easier for data holders to enter into contracts. Absent this supervision, banks feel the need to secure appropriate protections for their customers through these contracts. If there were a more consistent regulation, data holders would have a degree of confidence that recipients were being examined for compliance with key consumer protection laws, simplifying the contracting process.

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 consumers have consented to share their financial data and provide a transparent portal that allows them to understand what data are shared, limit the data that are shared, and revoke access altogether. These systems can also help trace where data travels and provide visibility on the downstream parties that can access it.

We have seen many large banks unveil permissioning platforms. Wells Fargo's "Control Tower" and JPMorgan Chase's "Security Center" are just a few examples. Core integrations with Akoya offer community banks the ability to offer similar features.

Prescriptive frameworks would be counterproductive to implementing Section 1033.

Today, millions of consumers already have the ability to share their financial information via secure API. This progress has been driven by industry collaboration that is supported by the principles-based approach that the CFPB has taken to date. A more prescriptive approach is not only unnecessary but may undermine the progress that has already taken place and risks leaving consumers exposed if undertaken too narrowly.

In the advanced notice of proposed rulemaking issued in 2020, the CFPB considered whether it should prescribe criteria that identify the specific data fields that should be subject to the access rights described in Section 1033. This would represent a major shift away from the CFPB's current principles-based approach developed under Director Cordray that would likely have serious unintended consequences.

Implementation of prescriptive standards would quickly undermine the progress that has taken place since the CFPB published its principles in 2017. If the CFPB were to announce a new approach to data aggregation, industry participants would pause and quickly step away from existing initiatives that already give consumers more secure methods to share their data.

Prescriptive standards also rarely facilitate innovation. By their very nature, standards are relatively static. In a market that is evolving as quickly as financial services, the data fields that are identified as

[8] https://www.aba.com/news-research/podcasts/empowering-community-banks-with-open-finance

important for today's use cases of aggregated data are unlikely to be appropriate for the innovations of tomorrow.

Prescriptive action cannot focus solely on access but must also address the risks to consumers.

In addition to being unnecessary, prescriptive rulemaking may also put consumers at risk. Any prescriptive rule cannot only focus on defining the data fields, but must also build a robust framework for consumer protection that includes supervision, liability, and data security.

Access cannot be divorced from the other important principles already outlined by the CFPB and must be paired with security, transparency, control, and minimization. Consumers only benefit from access when the financial data retains bank-level legal protections, regardless of the entity that holds the data, and consumer trust in the financial system is maintained. Any effort to prescribe access without also prescribing the protections that must apply to that data would inevitably leave consumers exposed. For example, open banking laws enacted in Europe were only possible because strong general privacy laws already applied to all firms.

Moreover, any action to define the specific data fields subject to Section 1033 would undermine the CFPB's core principle of minimization. All fields included in this definition would inevitably be shared in every instance, rather than only shared if needed for the service a consumer authorized.

Today, many of these protections are implemented through the contracts that govern access. These contracts are either negotiated on a bilateral basis or via industry utilities like Akoya. These negotiations ensure that the right data fields are made available while minimizing the unnecessary data shared and securing protections for consumers.

Any prescriptive action by the CFPB to define the terms of access would also need to address the following critical issues:

- **Supervision**: The CFPB would need to establish a framework for direct supervision of all data recipients including downstream users of financial data to ensure that data are being afforded the appropriate protections.
- **Liability:** The CFPB would need to establish a liability framework that ensures that consumers are made whole in the event of a loss. It is critical that liability sits with the party best able to control for the risk and flows with the data to the entity that the consumer has permissioned to access the data. Any such framework should provide a practical, efficient, and fair means to assign and enforce the liability.
- **Data Protection and Privacy:** The CFPB would need ensure that data privacy requirements are consistent across banks and nonbanks. The FTC Safeguards Rule[9] (which applies to nonbanks) only sets out the standards and stops short of the important requirements adopted by the federal banking agencies for institutions to (a) establish and maintain appropriate safeguards to ensure the security of the data to which they have access and (b) notify customers as quickly as appropriate after a breach or data loss to allow customers to take steps to protect themselves in the event their information may have been compromised. [10]

[9] 16 C.F.R. 314

[10] For more analysis on the importance of GLBA please see pages 4-5 of ABA's 2017 comments. https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2017/02/ABA-Comment-CFPB-Data-Aggregators.pdf

Congress should urge the CFPB to provide clarity to allow the market to continue to develop.

While we believe a market-driven approach is the best way to empower consumers to control their financial data, there are several regulatory and legal clarifications that can help give certainty to the market that will allow the private sector to more quickly make progress. Many of these topics are likely to be covered by the upcoming CFPB rulemaking. We believe that Congress should urge the CFPB to consider the following recommendations to ensure that customers of all banks – regardless of their asset size – can control their financial data and fully benefit from financial innovation.

Congress should urge the CFPB to clarify that GLBA applies to financial data throughout its lifecycle.

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, 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."

Consumers expect that their financial data are adequately protected whether 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." ABA believes that data aggregation should be treated as a data processing activity that is financial in nature such that data aggregators fall under the GLBA's definition of "financial institution" and be subject to all the rules that apply to all other financial institutions. This ensures that data protections apply consistently and continually regardless of where the data originated, where they are transferred, or the type of company 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).]" This definition includes not only banks, but as interpreted by the Board of Governors of the Federal Reserve, 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 we 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, we believe that 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.

Congress should urge the CFPB to 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 log-in 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 and shared. In most cases consumers do not have a direct relationship with these companies and must trust that their data are being handled appropriately.

As discussed in above, ABA believes that data aggregators are subject to GLBA, but their compliance with its privacy and security obligations is not clear and, more importantly, 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 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. ABA believes that establishing accountability across all providers of comparable financial products and services is a fundamental mission of the CFPB. 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 expeditiously 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 CFPB has imposed supervisory authority over the larger data aggregators, it will be better able to monitor – and react to – risks to consumers in this rapidly evolving marketplace.

<u>Congress should urge the CFPB to clarify that data aggregators are subject to Regulation E as service providers.</u>

Under Section 1005.14 of Regulation E, a person that provides an electronic fund transfer service to a consumer but does not hold the consumer's account is generally subject to Regulation E, (with certain modifications) as a service provider, 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 should be treated as "service providers" under Regulation E, as they enable the use of "access devices" that initiate electronic fund transfers to and from the account. As service providers, they are liable for unauthorized transactions under Regulation E and are subject to 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 commercial or other relationship with the data aggregator, no knowledge of, and no power over the data aggregator's security system, or any relationship with the aggregator's end clients. 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 service provider responsibilities of Regulation E support classifying data aggregators as service providers. These include requirements related to error resolution, disclosures, the prohibition against the issuance of unsolicited access devices, and changes in terms notices.

To avoid any ambiguity, the CFPB should confirm in Regulation E or the Official Commentary that data aggregators providing electronic fund transfer services are service providers under Regulation E. Equally important is that data aggregators be examined for their compliance with these consumer protection rules.

Congress should urge the CFPB to require that data aggregators periodically reconfirm consumer authorization to access their accounts.

When consumers authorize a third party to access their financial data, they expect that data sharing is limited to the data needed to provide the service they have authorized. This applies not only to the scope of data being shared, but to the period of time over which that access is granted. Some use-cases of data aggregation are ongoing. However many are one-time events like account ownership verification. Yet, data holders have the ability to store login credentials indefinitely, sometimes continuing to access data years after the consumer has stopped using the service.

Federal Reserve Board Governor Lael Brainard explains this in a 2017 speech:

> In examining the terms and conditions for a number of fintech apps, it appears that consumers are rarely provided information explaining how they can terminate the collection and storage of their data. For instance, when a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information. If a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don't have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best.[11]

We believe that the CFPB should require data aggregators to re-obtain a consumer's consent on a periodic basis to ensure that consumer data are not shared indefinitely.

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

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 the data 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. The bank customers have directed their bank to share their data; a bank's contract simply lays out the terms for how that data are shared and provides a more secure portal for doing so. Such a

[11] https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm

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.

Banks should not be considered furnishers for purposes of FCRA

Congress should urge the CFPB to make clear that when a bank or other data holder is compelled to share information with a third party at the direction of a customer, the bank and other data holders are not considered to be furnishers for purposes of the Fair Credit Reporting Act (FCRA), regardless of how the third party uses the information. In these cases, banks are merely accommodating the customer and acting as the customer's agent. They are providing information just as they do, for example, when they send bank statements (by paper or electronically) directly to a lender processing their customer's loan application. The only difference is that the information is shared more efficiently using a process that is more convenient for the customer.

In these cases, the customer's agreement to share data is with the data aggregator, not the bank or other data holder. The banks and other data holders have no choice but to share the information and derive no direct or indirect benefit in sharing it. Its agreement with the third party is simply to provide a means for mitigating risk when sharing sensitive information at the customer's direction. In many cases, they may not and often do not know the purposes for pulling the data or how it will be used. Moreover, the data holders never collected the data with the intent of the data being used for these purposes.

Section 1033 of the Dodd-Frank Act recognizes this challenge and provides limitations that make clear banks do not have these responsibilities in regard to aggregated data. The law requires banks to make available only data that are in the "control or possession" of the bank and explicitly exempts "any information that the covered person cannot retrieve in the ordinary course of its business." Section 1033 requires banks only to disclose the data that they already have. FCRA imposes further requirements on furnishers to curate data in a way that makes it specifically usable for credit reporting purposes.

Congress should urge the CFPB to coordinate with banking regulators in any rulemaking

Implementation of Section 1033 has wide-reaching implications for banks. Because of the sensitive nature of financial data, there are serious safety and soundness concerns that must be addressed. This is why Section 1033 requires the CFPB to "consult with the Federal banking agencies and the Federal Trade Commission," when prescribing any rules.

Conclusion

Today, technology is fundamentally changing the way financial services are being delivered. Consumer financial data are more available and more widely shared than ever before. ABA believes that innovations in financial services present tremendous value. This value is only realized when innovations are 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.