INDEPENDENT COMMUNITY BANKERS of AMERICA®

Brad M. Bolton, *Chairman*
Derek B. Williams, *Chairman-Elect*
Lucas White, *Vice Chairman*
Tim R. Aiken, *Treasurer*
Sarah Getzlaff, *Secretary*
Robert M. Fisher, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

Via Electronic Submission to:Financial_Data_Rights_SBREFA@cfpb.gov

January 25, 2023

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

RE: CFPB's Outline of Proposals and Alternatives Under Consideration, Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights

Dear Sir or Madam:

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to respond to the Bureau of Consumer Financial Protection's ("CFPB" or "Bureau" or "Agency") Outline of Proposals and Alternatives Under Consideration ("Outline")[2] to implement Section 1033 of the Dodd-Frank Act ("Section 1033").

Section 1033 gives consumers the right to access their financial records in electronic form. Section 1033 enabled an explosion of non-bank entities seeking the consumer's permission to access their digital financial records. These companies aggregate and use those records to offer new products and services to help consumers manage their financial affairs. While the Bureau believes that consumers' ability to access their financial data empowers them to better monitor their finances, it also acknowledges that permissioned access to financial data raises a number of concerns pertaining to data security, privacy, and unauthorized access.

---

[1] *The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. ICBA is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education, and high-quality products and services.*

With nearly 50,000 locations nationwide, community banks constitute roughly 99 percent of all banks, employ nearly 700,000 Americans and are the only physical banking presence in one in three U.S. counties. Holding more than $5.8 trillion in assets, over $4.9 trillion in deposits, and more than $3.5 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities throughout America. For more information, visit ICBA's website at www.icba.org.

[2] *See* https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf; *see also* https://www.consumerfinance.gov/personal-financial-data-rights/.

Summary

Consumers are increasingly authorizing data aggregators and other third parties to access their bank accounts to provide products and services. ICBA fully supports consumers' rights to have access to their own information and supports responsible financial services innovation. However, while recognizing the value of services that enable consumers to manage their financial affairs, ICBA urges, through our responses below, the CFPB to carefully craft a rule that considers the privacy, data security, regulatory and financial burden, and legal implications posed by authorized third-party access to consumer bank accounts. Specifically, we urge the following considerations in preparation for a future proposed rule:

- Resist proposing a rule that requires banks to provide any information that fall outside of the scope of section 1033.
- Propose a rule that limits data to the extent that it can under the statute in a way that is less harmful to the consumer and to banks.
- Expand the scope of covered data providers to include all entities offering accounts that retain customer funds.
- Require authorized third parties to disclose risks and inform of their liability in the event of a loss.
- Exclude proposing that data providers make available information regarding prior transactions and deposits that have not yet settled; prior transactions not typically shown on periodic statements or portals; online banking transactions that the consumer has set up but that have not yet occurred; and account identity information.
- Create exceptions and safe harbor protections that are tailored to provide maximum legal and regulatory protection for community banks and does not impede their competitive positions.
- Bring third party providers under the supervision of the CFPB which would result in consumer protection compliance obligations and subject these entities to annual examinations.

Coverage of data providers subject to the proposals under consideration

The CFPB is considering proposing that "Covered Data Providers" are entities that meet either the definition of "financial institution" under Regulation E[3] or "card issuer" under Regulation Z[4] . The CFPB is also considering whether to allow exemptions based on asset size and activity levels, such as the number of accounts at an institution.

3 Electronic Fund Transfers (Regulation E) 12 CFR §1005.2(i)
4 Truth in Lending (Regulation Z) 12 CFR § 1026.2(a)(7)

To fully protect consumers and promote a competitive playing field, the CFPB's rule, when finalized, must expand the scope of covered data providers to include all entities offering an account that retain customer funds, for example but not limited to, Buy Now Pay Later platforms/apps, PayPal, Venmo, CashApp, and Coinbase. The scope should also be expanded to include gaming and gambling platforms and apps because these entities receive consumer's money and allow for winnings to be deposited into and exported out of the app. Many people make their living as professional video gamers and online gamblers which means their financial data is being stored on and likely shared by these entities.

ICBA strongly supports exemptions for financial institutions so long as those exemptions are appropriately targeted. Exemptions for non-bank data holders should be predicated on whether those entities are supervised and examined by the CFPB.

Recipients of information

Consumers (direct access)

The CFPB is considering how it should address a covered data provider's obligation to make information available directly to a consumer when the account is held by multiple consumers and may propose that a covered data provider would satisfy its obligation by making the information available to the consumer who requested the information or all the consumers on a jointly held account.

ICBA believes this approach is reasonable so long as it does not require community banks to validate or make distinctions as to who should or should not receive the information, given the multiple or joint owner status of the account. An alternate approach would be to make the information available to the primary account holder to satisfy the covered data provider's obligation. Additionally, the proposal should require the third party to obtain authorization and provide notices and disclosures to all owners of an account before requesting information from a covered data provider.

Third-party access and authorization

Section 1033 generally requires data providers to make information available to a "consumer," which includes an agent, trustee, or representative acting on behalf of an individual consumer.

The CFPB is considering to propose that an authorized third must: (1) provide an "authorization disclosure" to inform the consumer of key terms of access; (2) obtain the consumer's informed, express consent to the key terms of access contained in the authorization disclosure; and (3) certify to the consumer that it will abide by certain obligations regarding collection, use, and retention of the consumer's information.

In addition to the proposals the CFPB is considering for third party authorization procedures, ICBA strongly urges against any proposed rule that would require banks to provide disclosures on behalf of permissioned third parties. We further urge against proposed rules allowing the use

of bank logos and branding elements which would create confusion and mislead bank customers and create customer support difficulties for banks.

The CFPB should also consider how these disclosures will be delivered to the consumer from the third party, and a mechanism for recording that the consumer accept and understand the terms and conditions. Finally, since community banks generally do not have a direct relationship with the third party, the risk for banks is heightened. Community banks do not have a way to ensure that the permission has been legitimately authorized by their accountholder. As noted in a Treasury Department report, this "raises issues of importance for these financial institutions, including how to verify that their customers have in fact authorized a third party to access their account or initiate a transaction."[5] As such, the proposed rule must also include a safe harbor for banks that will rely on these authorization disclosures.

Authorization disclosure content and consent

The CFPB is considering proposing that the authorization disclosure include the general categories of information to be accessed, the identity of the covered data provider and accounts to be accessed, terms related to duration and frequency of access, and how to revoke access. Key "use terms" might include the identity of intended data recipients (including any downstream parties and data aggregators to whom the information may be disclosed), and the purpose for accessing the information. The CFPB is also considering proposing that the authorization disclosure include a reference to the third party's certification to certain obligations regarding collection, use, and retention of the consumer's information. The authorization disclosure would also contain a request for consent to access the consumer's information.

ICBA supports the approach that the CFPB is considering pertaining to the content of the disclosures. We have been consistent in our belief that consumers must clearly understand to which company they are granting permission to access their banking data. That said, in addition to the scope and use terms under consideration, ICBA urges the following:

- A requirement that the third party clearly explain to the consumer that the relationship is not with the bank or data provider, nor facilitated by the bank or data provider.
- Explicitly inform the consumer of its liability to the consumer in the event of a loss or breach.
- Explicitly inform the consumer that the bank is not liable for losses sustained as a result of the third party's access.
- Explanation of the risks associated with granting permission to a third party to access customer account information.

[5] https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

- A requirement to include contact information of the third party for consumers to report issues or losses.

The CFPB's proposal should also include strict restrictions against pre-populated disclosure forms and require that they be given to the customer prior to accessing their data and annually, as long as the relationship is going, and when the third party makes material changes to practices.

The proposed rule should also require a customer's signature certifying receipt, consent, and a statement of understanding. Furthermore, a disclosure should be required for each type of service for which the consumer provides permission. Third parties should also be required to provide consumers a copy of their signed consent, either electronically or through the mail.

ICBA also supports the CFPB requiring a third party to certify to the consumer that it will abide by obligations regarding use, collection, and retention of the consumer's information. The certification should also include that the third party will abide by relevant laws and regulations.

The types of information a covered data provider would be required to make available

Section 1033 authorizes the CFPB to require a data provider to make available information "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." The Outline sets forth the following categories of information the CFPB is considering requiring covered data providers to make available the following types of information:

(i) periodic statement information for settled transactions and deposits;
(ii) information regarding prior transactions and deposits that have not yet settled;
(iii) other information about prior transactions not typically shown on periodic statements or portals;
(iv) (iv) online banking transactions that the consumer has set up but that have not yet occurred; and
(v) account identity information.

Information regarding prior transactions and deposits that have not yet settled

ICBA urges the CFPB not to issue a proposed rule that would require banks to share information on transactions that have not settled. This would pose significant challenges to community banks because this information is temporary and generally not made available in monthly statements, nor online beyond the time of the hold. Other than informing a consumer of their "at the moment" balance, there is no purpose or value in sharing this information with a third party. Requiring banks to share information that changes throughout the day, and is not typically documented after settlement, would be burdensome and futile.

However, if the CFPB does if fact issue this concept as a proposed rule, clarification needs to be made "on not yet settled" because the Outlines do not state if these prior transactions that have not yet settled are in fact final transactions of final authorized amounts. Take for example automated fuel dispenser purchases ("AFD"). A consumer taps their bank issued debit or credit card at an AFD and the issuer authorizes up to $150 and holds those funds until the consumer finishes filling up their vehicle. Within a few hours the issuer is required to release the $150 hold and display the final purchase amount although the release can happen before the consumer drives away from the pump. While the issuer did approve up to $150, that was not the settled amount. The $150 AFD is not normally shown to a consumer although it was authorized. Bank issued cards work similarly at restaurants, hotels, car rental companies, and on purchases made on cruises.

Information about prior transactions not typically shown on periodic statements or online financial account management portals

Community bankers have expressed how problematic and complex this would be because of the high likelihood that this information is not stored on a core platform, as well as not knowing which data element is the focus under these circumstances. Furthermore, in the Outline, the CFPB uses the example, "with respect to many transactions displayed on a periodic statement or online financial account management portal, covered data providers receive and retain from the payment networks in which they participate certain data about the transactions that are not reflected on the periodic statement or portal. The payment networks in which a covered data provider would typically participate, and which provide transaction-specific data to the covered data provider, include card networks, ATM networks, automated clearing house (ACH) networks, check-collection networks, and real-time payment networks."[6] However, the Outline does not specify the piece of data that would be the subject of this information release. The lack of clarity of the specific data element at issue will place community banks in the position of browsing through information not maintained on their core platforms and playing the guessing game on what the third party *may* have in mind. The lack of clarity renders sharing this information impossible, and we therefore urge the CFPB to not propose this provision.

Online banking transactions that the consumer has set up but that have not yet occurred

Community banks have expressed the impracticality of obtaining and sharing information on transactions that have not yet occurred, such as multiple years of future online payments. Adding to the difficulty of providing this information is the fact that payment amounts, dates, and creditors change frequently raising the likelihood that inaccurate information will flow through the portal for third-party access. Hence, ICBA urges against proposing this requirement.

[6] Small Business Advisory Review Panel for Consumer-Permissioned Sharing of Consumer Financial Data Rulemaking Outline of Proposals and Alternatives Under Consideration (consumerfinance.gov) p.20

Account identity information
Under consideration is a requirement that covered data providers make available information related to the identity and characteristics of the accountholder, specially: name; age; gender; marital status; number of dependents; race; ethnicity; citizenship or immigration status; veteran status; residential address, residential phone number, mobile number; email address; date of birth; social security number; and driver's license number. The outlines state this type of information could be useful to an authorized third party seeking to verify a consumer's ownership of an account with a covered data provider.

ICBA would not support a proposed rule requiring banks to share this information given the potential for fraudsters to infiltrate third party platforms and use these identifying factors to facilitate identify theft, or other financial abuses. Additionally, customers do not always keep their account information, such as addresses, telephone numbers, name changes, etc., up to date which will result in inaccurate information being shared. Since both scenarios are problematic and may result in liability to banks, ICBA strongly discourages the CFPB from proposing that data providers provide this information.

Other information
The CFPB is considering proposing that covered data providers make available consumer reports; fees that the covered data assessed on consumer accounts; bonuses, rewards, discounts, or other incentives; and information about security breaches that exposed a consumer's identity or financial information.

ICBA would strongly urge against a proposed rule with requirements for banks to provide any of this information because they fall outside of the scope of section 1033.

Overall, our members question why the CFPB would consider these data elements which are fraught with data security and privacy concerns and highly susceptible to fraud, identify theft, or other financial abuses against the consumers they are discharged to protect. The CFPB should understand that the data elements proposed would require banks to pull data from multiple systems and place an extraordinary financial and operational burden on their ability to share this information. The costs associated with sharing this data will have a disproportionate effect on community banks as they do not have large staffs and systems to collect and share this data. The CFPB should be careful to consider the implications of exceeding the statutory mandates of Section 1033 by creating new and unnecessary data to be shared.

Statutory exceptions to making information available
Section 1033(b) sets for the following exceptions to a data provider from making available: any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors; any information collected by the data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct; any information required to be kept confidential by any other provision of law; and any information that the data provider cannot retrieve in the

ordinary course of its business with respect to that information. ICBA urges the CFPB to ensure these exceptions are included in its proposal and tailored to provide maximum legal (including contractual) and regulatory protection for community banks. The exceptions also should not impede or hamper their competitive positions and should provide clear parameters on the data to be shared.

Current and historical information

The CFPB is considering proposing that a covered data provider would need to make available the most current information that the covered data provider has in its control or possession at the time of a request for current information. Since Dodd-Frank Act ("DFA") Section 1033(c) states that section 1033 does not impose a duty on a data provider to maintain or keep any information about a consumer, the CFPB is considering proposing that a covered data provider would only need to make available information going as far back in time as that covered data provider makes transaction history available directly to consumers.

ICBA recommends proposing time limits on historical information to be shared to up to 12 months. Although record retention rules dictate how long a bank is to maintain specific records and transactions (many with varying times), some banks maintain records beyond those timeframes. Limiting the information to as far back as the consumer is able to obtain directly may not be as seamless, nor efficient as the CFPB may believe it is. The more data shared over a longer period of time could have serious system issues for a financial institution, such as slowing or shutting down systems and weakening data security. One year's worth of data is more than enough information for a third party to use for purposes for which the consumer gave their permission.

How and when information would need to be made available

The CFPB is considering proposals to define the methods and the circumstances in which a covered data provider would need to make information available directly to a consumer (direct access), and to a third party (where a consumer authorizes a third party to access data on their behalf).

Direct access

The CFPB is considering proposing to require a covered data provider to make information available if it has enough information from the consumer to reasonably authenticate the consumer's identity and reasonably identify the information requested.

"Reasonably authenticate" is a term that that is vague and may provide inconsistency from the prudential regulators.. Any proposed rule must include a safe harbor and indemnification for banks that reasonably authenticate a consumer's identity and reasonably identify the information requested.

To avoid disjunction across the regulatory ecosystem, a proposed rule should include language pertaining to the CFPB working closely with all prudential regulators to establish a universal

standard for reasonably authenticating the consumer's identity and reasonably identifying the information requested.

The CFPB is also considering proposing that covered data providers be required to make available through online financial account management portals all the information that would be covered by the proposals, and to allow consumers to export the information in both human and machine-readable formats. The Outline uses the example that many data providers allow consumers to export a history of their transactions in file formats that present the information in a consumer-friendly display and file formats such that the file could be imported or read into a computer system for further processing, e.g., a Comma Separated Values ("CSV") file format.

The CFPB should consider the unintended consequences when proposing the delivery and exportation of data to the consumer. Consumer-friendly displays could be impeded (or rendered useless) based on the data requested and where that data is stored. Data from a core service provider is more likely to be machine readable and result in consumer-friendly displays. But if that data is not stored with the core service provider, such as data on a hard copy document filed in the bank, it will not be machine readable.

Additionally, there are limitations on various file formats. For example, CSV file formats are antiquated and rely on specific coding that has to be set in the application which handles the file for data to display in a consumer-friendly way. CSV is also not conducive to large and complex data transportation. XML file formats have different limitations. While the file formats may work better with transporting data and with Application Programming Interfaces ("APIs"), the type of data requested determines how readable the information will be.

The CFPB asks responders for input on whether they should consider data that is typically retained in records that are not easily made available in electronic form, such as paper or audio recordings. ICBA strongly urges the CFPB to issue a rule within the parameters of the DFA and not issue any rule requiring data holders to make any information available that is not in electronic form, such as paper or audio recordings.

The CFPB is interested in input on whether to require covered data providers to make available information it knows is inaccurate. Community banks may not be aware that the information it provides is inaccurate. At times, data is rendered inaccurate because transactions may be pending, have not posted, or have not been reversed (e.g., hotel or car rental holds). If this proposed rule does take these factors into consideration, the CFPB could unwittingly place burdens on banks for factors beyond their control. The CFPB should consider a safe harbor protecting data holders from any liability associated with information that may be inaccurate when transported upon a third party's request. The proposed rule should also require third parties to issue a notice to consumers informing them that factors may render some data inaccurate at the time the data was accessed.

Third-party access

General obligation to make information available through a data portal

The CFPB is considering proposing that covered data providers must establish and maintain a third-party access portal that does not require the authorized third party to possess or retain consumer credentials. The CFPB is also considering what role screen scraping should play in the context of a covered data provider's compliance with the rule.

The CFPB states that it is aware that a number of large data providers, data aggregators, and large data recipients have been developing and implementing voluntary standards and guidelines related to third-party access portals. While the CFPB positively views these industry-led standard-setting endeavors the agency asks whether it should define standards and whether certain aspects of the regulation of third-party access portals are better suited to be regulated by industry participants**.**

ICBA encourages the adoption of the data sharing principles issued by the CFPB in 2017[7] to share and use permissioned customer financial account information. These principles include user-authorized access and the ability to revoke consent and reflect applicable laws and industry best practices regarding data privacy and security. To this end, the industry should move beyond screen scraping which can lead to suboptimal outcomes for the financial data ecosystem and put customer accounts at unnecessary risk. ICBA advocates leveraging secure API technology to enable the principles discussed below. Access should be transparent, enhance customer control, and require storing only the minimum amount of data needed for application functionality. Additionally, the data should be stored for only the length of time needed. ICBA advocates the use of more secure APIs so long as standards are not mandated, which would threaten to disadvantage community banks. More broadly, there is a lack of widespread adoption of external-facing application APIs among financial institutions in the United States. Considerable investment and effort are needed to make this change. Developments in Europe with Payment Services Directive 2 ("PSD2"), a directive requiring financial institutions and others to grant licensed third party providers access to bank customer account information, have illustrated the operational challenges of implementing open APIs. For example, obstacles to developing these interfaces in the United States include rearchitecting banks' complex legacy back-office infrastructure.[8]

Importantly, there is limited adoption of APIs among community banks as they are highly dependent on their core banking platforms and other solution providers for API integration capabilities. APIs and API integration from core and solution providers may come at a cost to

[7] cfpb_consumer-protection-principles_data-aggregation.pdf (consumerfinance.gov)
[8] https://bian.org/news-room/bian-in-the-news/psd2-api-challenge-open-banking/

community banks. For this reason, standards implementation by different market participants should reflect industry progression at a reasonable cost or no cost, so as not to leave community banks at a disadvantage from any asymmetry of capabilities and resources.

Similarly, policymakers should not prescribe how permissioned customer data is structured and exchanged. Establishing prescriptive technical guidelines (e.g., specific data fields, formats, etc.) would undermine progress already underway. Today the industry is moving towards adopting standardized APIs to address technical inconsistencies and enable compliance with the common CFPB principles. Coordination among all stakeholders - financial institutions, data aggregators, fintech providers, regulators, and consumers themselves - is needed to move towards a common set of industry technical standards. In recent years, the financial services ecosystem, through industry bodies such as Financial Data Exchange (FDX) and Afinis, has collaborated to move towards API interoperability. ICBA encourages continued work through these industry standardization efforts to ensure that customers can control their financial data sharing preferences in a secure and transparent manner, while minimizing unnecessary data stored.

With respect to covered data providers that have not yet established a third-party access portal at the time the rule is final and effective, the CFPB asks if it should require that they make information available to authorized third parties before they establish a third-party access portal. ICBA urges against requiring community banks to make information available before they establish a portal. Requiring banks to build and maintain a portal for third-party access is already a significant burden. The burden is amplified for smaller banks, as well as the risks of transporting such data outside of a secure mechanism. Furthermore, a sufficient timeframe to develop, test and implement such portal needs to be addressed in the proposed rule. Our members have expressed that sufficient time would range from five to eight years, and that implementation time be staggered based on asset size.

Third party obligations - collection, use, and retention limits

The CFPB is considering proposals under which authorized third parties would have to limit their collection, use, and retention of consumer information to what is reasonably necessary to provide the product or service the consumer has requested.

We recommend the CFPB ensure that data is limited to minimize the risk to consumers and to banks. Data holders are not in the position, nor should they be placed in the position, to ascertain or determine whether the data aggregator is getting enough or too much access to information. Nor does it have control over how long the third party retains that information.

ICBA strongly supports regulations limiting the use and sharing of data to that which is authorized by the consumer. Any future rulemaking should include "data minimization." Data that is accessed with authorization by the consumer should have limited application functionality. This enables minimal amount of third-party data access, collection, and storage for a restricted period of time, and mitigates consumer risks in the event of a breach or misuse of

data. These restrictions should also apply to limiting data to the original entity receiving permission, thereby prohibiting the sale of data to unpermissioned third parties.

Data accuracy and dispute resolution requirements

The CFPB is considering a proposal to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the data that they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes submitted by consumers.

Today, data holders, such as consumer reporting agencies and banks, are required by the Fair Credit Reporting Act ("FCRA") to maintain accurate consumer data. Third-parties may not comply with these requirements. Exacerbating matters, consumers have limited visibility into and ability to correct the data transmitted by an aggregator. Accurate consumer financial and credit reporting data is crucial for both consumers and community banks and other financial institutions. Consumers have rights from entities subject to the FCRA to see what data is being held, ensure accurate information, and dispute incomplete or inaccurate information. Consumers lose these rights when non-regulated entities are holding the data. Similarly, community banks and other financial institutions need accurate financial and credit reporting data to offer appropriate services to consumers.

Data aggregators and other third parties must provide better transparency on data access. As data aggregators are not currently regulated, they are not required to provide the same level of transparency or accuracy to consumers as other stakeholders in the financial services ecosystem. In addition to weaker, if any, security requirements, the lack of transparency with how data aggregators treat consumer data is cause for concern. When data aggregators seek permission from consumers to access their data, consumers should be provided with clear disclosures on specific data being collected and how it will be used, along with any downstream usage of that data. Unfortunately, there is a lack of incentives for data aggregators in the current market environment to provide this level of transparency.

ICBA believes that the Bureau should exercise their formal and explicit supervision and enforcement authority over data aggregators. Given their prolific access to and storage of consumer data, the CFPB should regularly supervise and examine data aggregators and brokers under its "larger participants" authority under Section 1024 of the Dodd-Frank Act. Ideally, supervision would give the Bureau information about data aggregators' activities and compliance with consumer protection laws as well as allow the Bureau to detect and assess risks to consumers and the consumer financial markets. Just as the Bureau has done in other markets, it should exercise its Section 1024 authority over larger participants in the data aggregation market.

ICBA supports rules requiring third parties to ensure the accuracy of data they collect because the knowledge of what the consumer consents to and what the third-party requests rest between them. Banks will be required to release information based on what is requested by the third party.

The CFPB is also considering proposals for covered data providers to implement reasonable policies and procedures to ensure data accuracy, establish performance standards, and prohibit covered data provider conduct that would adversely affect the accurate transmission of consumer information, or some combination of the above.

While ICBA agrees that data providers should not actively take steps that would adversely affect the accuracy of transmitted consumer information, we are concerned that requiring data providers, such as community banks, to adhere to FCRA dispute investigations would exceed the scope and purpose of FCRA, as ICBA does not believe that data providers would be considered "data furnishers" here.

Under FCRA, furnishers are required to investigate disputes made directly by the consumer, or indirectly via the consumer reporting agency. Data providers are considered "furnishers" when they provide data to a consumer reporting agency for inclusion in a consumer report. Here, however, data providers are providing information to a third-party request, as if the individual consumer requested the information themselves. Further, the data provider is NOT conveying the information for inclusion in a consumer report, which is the second prong in the defined term of "furnisher" under FCRA. Instead, data providers, such as community banks, are providing the information as a requirement under section 1033 and not for the purposes of creating a consumer report.

Separately, the CFPB is also considering a proposal to require authorized third parties to maintain reasonable policies and procedures to ensure the accuracy of the data that they collect and use to provide the product or service the consumer has requested, including procedures related to addressing disputes submitted by consumers. While ICBA believes that such a proposal may be prudent, we caution the Bureau against using FCRA authority in mandating such investigations. As mentioned above, data providers do not meet the definition of "furnisher," and as such, are not covered by FCRA when providing data to permissioned third parties.

Data security requirements

The CFPB seeks input on a proposal to authorize third parties to develop, implement, and maintain a comprehensive written data security program appropriate to the third party's size and complexity, and the volume and sensitivity of the consumer information at issue. ICBA fully supports a proposed rule requiring authorized third parties to implement Gramm-Leach-Bliley Act ("GLBA") like data security standards, as well as the CFPB's authority to impose such standards onto these third parties. GLBA's information security safeguards and data privacy provisions provide a secure framework which community bank customers have come to expect from their financial products.

Specifically, ICBA recommends the creation of a safeguards rule that incorporates the "*Interagency Guidelines Establishing Information Security Standards"*[9] as an option for complying with any data security requirement under the CFPB's rule. Any safeguards rule the CFPB incorporates should be based on risk and complexity if the minimum standards for such a rule are equal to or stronger than what is required at the institution where the information originated. Further, the interagency guidelines referenced above should serve as a minimum baseline for such standards. The CFPB should also consider the examination standards set forth for information security in the "*FFIEC Information Technology Examination Handbook: Information Security."*[10]

Enforcement and supervision of authorized third parties

ICBA has been vocal in our opinion that the CFPB exercises it statutory right to supervise recipients of consumer information including authorized third parties. Unless this happens, consumers who place their financial lives in the hands of authorized third parties will not be protected. Title X of the DFA authorizes the CFPB to establish a supervisory program for non-banks that offer consumer financial products or services. Pursuant to statute, the Bureau is authorized to supervise non-banks for purposes of: (1) assessing compliance with federal consumer financial law; (2) obtaining information about activities, compliance systems, or procedures; and (3) detecting and assessing risks to consumers and consumer financial markets.[11] The Bureau conducts examinations, of various scopes, of supervised entities. In addition, the Bureau may, as appropriate, request information from supervised entities without conducting examinations.[12] Such authority ensures consistent consumer safeguards and levels the playing field among all industry participants. Pursuant to this authority, data aggregators should be supervised by the CFPB.

To date, aggregators benefit from unregulated access to sensitive consumer financial data without the oversight of examinations. Banks, on the other hand, are vigorously examined by various federal regulators for consumer protection compliance. As aggregators continue to collect consumer data without commensurate supervision, the risk to consumers continues to increase. Just as it has for other non-banks,[13] the CFPB should define data aggregators as "larger participants" and subject them to regular supervision.

Additionally, the CFPB should address regulatory uncertainty pertaining to the Electronic Fund Transfer Act and its implementing regulation, Regulation E. Regulation E establishes the framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems. Regulation E lays out requirements applicable to electronic fund transfers ("EFTs"), including disclosures, error resolution, and rules related to unauthorized

[9] 12 CFR part 30, App. B (OCC Safeguards Guidelines); 12CFR part 208, App. D-2 (Federal Reserve Board Safeguards Guidelines); 12CFR part 364, App. B (FDIC Safeguards Guidelines)
[10] https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf
[11] 12 U.S.C. 5514(b)(1)
[12] 12 U.S.C. 5514(b)
[13] The Bureau has exercised this authority for student loan servicing, debt collection auto-financing, and consumer reporting.

EFTs. The regulation also outlines the procedures consumers must follow in reporting errors with EFTs, and the steps a bank must take to provide recourse.

A community bank's success is largely dependent on its reputation of fostering customer trust. Maintaining the integrity of customer financial relationships is of utmost importance to community banks, not only because it is required by law but also because it is the right thing to do. If a customer experiences a financial loss with a permissioned third party, the customer is likely to seek redress from their bank. Regardless of where a breach occurs, banks take a variety of steps at their own expense to protect the integrity of customer accounts and should have access to various cost recovery options. Too often, the breached entity evades accountability while financial institutions are left to mitigate the customers' damages. Future rulemaking should clarify that data aggregators are solely liable for unauthorized transfers under Regulation E.

The CFPB should also clarify that banks are exempt from Regulation E liability for unauthorized transactions initiated by or through data aggregators acting as an EFT service provider. The regulation makes clear that a "person that provides an EFT service to a consumer but that does not hold the consumer's account is subject to all [disclosure and error resolution] requirements of this part if the person: (1) issues a debit card (or other 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."[14] Clarifying data aggregators' roles as service providers will also trigger responsibilities related to disclosures, documentation, and error resolution.[15]

The purpose of the CFPB's non-bank supervision authority is to prevent harm to consumers and promote a system that is fair and competitive. Promoting fairness and competitiveness requires data aggregators to be held liable for unauthorized transactions occurring within the scope of their authorization. The aggregator acts on behalf of the customer. The aggregator is not an agent, nor a third-party service provider, acting on behalf of the bank. Absent the customer connection, there is no relationship that would require a bank to execute its Regulation E protocol to address unauthorized transactions initiated by or through aggregators. This uncertainty must be resolved through rulemaking in a manner that is fair to community banks, as data holders.

The CFPB must be careful not to interpret customer-permissioned aggregator access to a bank's data as a direct vendor relationship. Banks and aggregators are brought together at the direction of a consumer authorizing access to their data. The aggregator is not an agent, nor a third-party service provider, acting on behalf of the bank. Absent the consumer connection, there is no

[14] 12 C.F.R. § 1005.14(a)(1-2) Electronic fund transfer service provider not holding consumer's account.
[15] Ibid §1005.14 (b)(1) – (b)(2)

contractual or other business relationship between the bank and the data aggregator that would trigger vendor due diligence requirements. As such, banks should not be required to conduct vendor-like due diligence on aggregators, and a requirement to do so would be an unfair and misplaced regulatory burden.

Conclusion

ICBA asks the CFPB to carefully consider these comments and address our concerns as the Bureau considers rules which would impact how community banks provide permissioned third parties account access to their customers' account data.

If you have any questions, please do not hesitate to contact me at Rhonda.Thomas-Whitley@icba.org or (202) 821-4451.

Sincerely,

/s/

Rhonda Thomas-Whitley
Vice President and Regulatory Counsel