December 29, 2023

Comment Intake—Section 1033 NPR
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 2055

Re: ICBA Comments in Response to Section 1033 Notice of Proposed Rulemaking (Required Rulemaking on Personal Financial Data Rights) [Docket No. CFPB–2023–0052; RIN 3170–AA78]

Dear Director Chopra,

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to provide feedback in response to the Consumer Financial Protection Bureau's (CFPB) Notice of Proposed Rulemaking implementing Section 1033 of the Dodd-Frank Act.[2] Section 1033 of the Dodd-Frank Act requires covered financial institutions to make available certain transaction information to customers in an electronic form usable by consumers.[3] The implementation of this statute, as proposed by the CFPB, would define virtually every bank in the country as a covered "data provider," which would require them to establish and maintain a "developer portal" that third-party companies – with consumer authorization – could use to access consumer data.

Our view is that, while this proposed rule represents an improvement over some of the most onerous potential requirements considered in the Bureau's Small Business Advisory Review Panel's "Outline of Proposals and Alternatives Under Consideration,"[4] it will still impose significant technological burdens and financial costs on community banks with no mechanism to recoup those costs from the third-party companies that ultimately benefit from the access to consumer financial data. Community banks will largely be dependent on their core processors or other third-party

[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 99 percent of all banks, employ more than 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 $4.8 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] 88 Fed. Reg. 74796, available at: https://www.govinfo.gov/content/pkg/FR-2023-10-31/pdf/2023-23576.pdf.
[3] *See* 12 U.S.C. 5533.
[4] CFPB, Small Business Advisory Review Panel's for Required Rulemaking on Personal Financial Data Rights, "Outline of Proposals and Alternatives Under Consideration" (Oct. 27, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

companies to create the technologies required to allow them to build and maintain developer portals to comply with this rule, limiting their ability to control or mitigate the cost of implementation. We are further concerned that risks to consumer privacy may result from this rule because of the difficulty of ensuring that data recipients have sufficient safeguards to protect sensitive financial data.

Summary of ICBA Position

In general, the rule proposed by the Bureau is reasonable and has incorporated some feedback from the Small Business Advisory Review Panel such as tiered implementation. However, we believe that the proposed rule will still impose considerable costs on community banks that are not commensurate with any benefit provided to consumers. The financial benefits of this rule will be reaped almost entirely by third party data recipients, and we believe any final rule must be structured so that they also bear some portion of the costs. A summary of recommended improvements to the proposal is below:

1) **Exempt Small Depository Institutions from Creating a Developer Interface:** Banks with less than $850 million in assets – which are defined as small businesses by the Small Business Administration (SBA) – should be exempt from the requirement to create and maintain a third-party developer interface.

2) **Allow Banks to Charge a Reasonable Fee for Developer Interface Access:** Banks should be permitted to charge a reasonable fee for providing access to consumer information to third parties. This would permit banks to recoup some of the costs of creating a developer interface without leading to any cost to the consumer.

3) **Provide a "Whitelist" of Supervised Third Parties:** The Bureau should create a list of third-party data recipients that it examines and supervises to ensure they are in compliance with the requirements of this rule, including the data security requirements. Data providers should be exempt from conducting third-party due diligence when sharing customer data with whitelisted third-party companies. This would increase certainty in the marketplace and reduce the necessity of banks to conduct third-party due diligence on the entire universe of data recipients.

4) **Only Require 6 Months of Transaction Data:** Virtually no bank currently retains 24 months of transaction level data and requiring them to provide this information to third parties will increase the cost of compliance with this rule, as well as slow down the transmission of data.

5) **Provide More Time for Community Banks to Comply:** While we appreciate that the Bureau has created tiered compliance dates, we do not believe that 2.5 years will provide sufficient time for banks between $850 million and $10 billion in assets to comply.

Covered Data Providers

The proposed rule would create two main categories of covered institutions – "data providers" and "authorized third parties," also known as data recipients. Community banks would primarily act as data providers, that is financial institutions that are providing customer financial data to customers and third parties but could also act as authorized third parties when receiving financial data about customers of other financial institutions.

The proposal defines a covered data provider as a financial institution or card issuer that offers either Reg E accounts[5] (i.e., deposit and savings accounts) or Reg Z credit cards[6] unless that financial institution is a depository institution that does not offer a "consumer interface."[7] In simplified terms, **virtually all community banks that offer an online banking portal , which would meet the definition of a consumer interface, would be covered by this rule.[8]**

Once a bank is considered a covered data provider, it would be required to establish and maintain both a consumer interface and a developer interface that consumers and authorized third parties could use to access financial data. A developer interface is defined in the proposal as "an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by authorized third parties in response to the requests."[9] This could be an online portal that third party companies could use to gain permissioned access to customer data using an Application Program Interface (API).

Based on extensive feedback from community banks, we believe requiring all community banks who offer an online banking portal to create and maintain a separate developer portal to be unduly burdensome. We believe that **banks defined as small business according to the Small Business Administration's size standards – currently banks below $850 million in assets – should be exempt from the requirement to create an online developer portal.** Small community banks are dependent on core processors and other third-party providers to manage the implementation of this regulation and are not well situated to control or mitigate the cost of compliance. According to the 2023 Conference of State Bank Supervisors survey, less than one percent of respondents indicated they do not rely on external providers for digital banking products and services.[10]

We are concerned that the cost of compliance may be unduly high for small banks because small banks often purchase a bundle of services from their core processor – the creation and maintenance of a developer portal would likely be another service added to that bundle. It can be

---

[5] As defined in 12 CFR 1005.2(b).
[6] As defined in 12 CFR 1026.2(a)(15)(i).
[7] "Consumer interface" is defined as an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by consumers in response to the requests.
[8] E.g., a recent Conference of State Bank Supervisors survey ("2023 CSBS Survey") found that 98% of respondents offer mobile banking, which would likely meet the definition of consumer interface. CSBS available here: https://www.csbs.org/sites/default/files/2023-09/CSBS%202023%20Community%20Bank%20Survey%2010.04.2023.pdf, at page 11.
[9] 88 Fed. Reg. 74869.
[10] *Id*. At page 18

difficult for community banks to change which core processor they use because of the complexity of the data that cores maintain. It is unlikely that a community bank would be willing and able to undertake a costly and time-consuming core conversion simply because they prefer the developer interface offered by a competing core processor. This would lock them into purchasing the developer interface offered by their existing core, with no meaningful ability to negotiate on price.

The process of undertaking a "core conversion" can cost hundreds of thousands of dollars and take multiple years to complete. For a small community bank, this is a significant expense, and it may not be practical to go through a core conversion just to get a slightly better price on creating and maintaining the required developer portal. This could put community banks in a position where they would be at the mercy of their core processor in terms of price.

Community banks could potentially hire other third-party companies to create and maintain a developer portal on their behalf, but doing so requires extensive vendor due diligence on these third-party companies and involves increased complexity to integrate with existing bank systems. For small banks, which may not have large IT budgets or personnel, vetting third-party software providers can a significant challenge, particularly when coupled with ensuring those providers can comply with a new regulatory framework.

Exempting small community banks from this rule is consistent with the Bureau's statutory authority. First, when engaging in rulemaking, the Bureau is required to consider the potential benefits and costs to consumers and covered persons, including the potential reduction of access by consumers to consumer financial products or services resulting from such rule; and the impact of proposed rules on [banks and credit unions with less than $10 billion in assets], and the impact on consumers in rural areas."[11]

Second, the Bureau's rulemaking authority gives it the ability to "conditionally or unconditionally exempt any class of covered persons, service providers, or consumer financial products or services, from any provision of [Federal consumer financial law], or from any rule issued under [Federal consumer financial law], as the Bureau determines necessary or appropriate to carry out the purposes and objectives of [Federal consumer financial law]."[12]

Analyzing these considerations, the benefits to consumers of requiring small community banks to comply with this rule appear small while the costs are significant. The proposed rule would prohibit banks from passing on the cost of creating a developer portal to customers or third parties directly, but costs would be passed on indirectly in the form of higher interest rates, reduced lending capacity, or reduced access to free checking accounts.

These costs are not offset by any substantial benefits. Customers can already access their financial information through online banking portals and there is no evidence of significant consumer demand for sharing this information with third parties among community bank customers. In fact, evidence that exists from other countries indicates a lack of consumer demand. In the five years

[11] 12 U.S.C. 5512(b)(2).
[12] 12 U.S.C. 5512(b)(3).

since the United Kingdom mandated open banking, only 7 million consumers and businesses use open banking enabled products and services.[13]

Exempting small banks from the requirement to create a developer portal would be a reasonable accommodation that would allow for a free market-based solution. Some critics of a small institution exemption claim that not requiring all depository institutions to create a developer portal would put small banks at a competitive disadvantage to their large bank peers. If that proves to be true, small banks would still have the option to voluntarily create a developer portal to eliminate this competitive disadvantage. However, if there is not significant consumer demand among community bank customers for sharing data with third parties, they should not be required to incur this unnecessary expense.

Compliance Dates

The Bureau has proposed the following series of staggered compliance dates for depository institutions based on asset size:

- Depository institution data providers that hold at least $500 billion in total assets – 6 months after publication of a final rule.
- Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets – 1 year after publication of a final rule.
- Depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets – 2.5 years after publication of a final rule.
- Depository institutions that hold less than $850 million in total assets – 4 years after publication of a final rule.

In general, we support tiered implementation of regulations that gives smaller institutions more time to adapt to new technical requirements. As stated above, however, we believe that the smallest depository institutions should be exempt from creating a developer interface. Therefore, we propose the following, alternative staggered implementation timeline framework:

Maintain the following timelines:

- Depository institution data providers that hold at least $500 billion in total assets – 6 months after publication of a final rule.
- Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets – 1 year after publication of a final rule.

Adjust the following timelines:

- Depository institutions that hold at least $10 billion in total assets but less than $50 billion in total assets – 2.5 years after publication of a final rule.

[13] Financial Conduct Authority, "Recommendations for the next phase of open banking in the UK," April 17, 2023, page 3, *available at* https://assets.publishing.service.gov.uk/media/643e608e22ef3b000c66f3bf/JROC_report_recommendations_and_actions_paper_April_2023.pdf.

- Depository institutions that hold at least $850 million but less than $10 billion in total assets – 5 years after publication of a final rule.
- Depository institutions that hold less than $850 million in total assets – Exempt.

First, we believe that the addition of a $850 million - $10 billion category is appropriate because there are significant differences in the resources and technological sophistication of banks of $850 million and $50 billion in assets. To group all banks between $850 million and $50 billion into a single category for purposes of compliance with this rule would place a significant burden on banks at the lower end of the size spectrum. $10 billion is a more appropriate threshold because that is the level which CFPB supervision begins.

Furthermore, we believe that five years is more appropriate than four years for the smallest banks to be required to comply with this rule. In our letter responding to the Bureau's "Outline of Proposals and Alternatives Under Consideration," we argued that five to eight years would be the minimally practical time required for community banks to develop, test, and implement compliant third-party access portal, particularly considering the dependence of community banks on external software providers.

Fees Prohibited

The notice of proposed rulemaking states: "A data provider that does not already have a developer interface would incur some upfront and ongoing costs to establish and maintain one, and data providers in general will incur some cost to maintain the interfaces as well as a marginal cost of providing covered data through the interfaces. The CFPB has therefore considered whether its proposed rule should permit a reasonable, cost-based fee to recover the upfront or fixed costs associated with establishing and maintaining the interfaces. There also may be some costs associated with providing covered data through the interfaces. The CFPB has preliminarily determined, however, that the marginal cost of providing covered data in response to a request is negligible."[14]

As such, the proposed rule states that "A data provider must not impose any fees or charges on a consumer or an authorized third party in connection with: (1) Interfaces. Establishing or maintaining the interfaces required … or (2) Requests. Receiving requests or making available covered data in response to requests as required."[15]

We vehemently disagree with the Bureau's characterization of the costs associated with the creation and maintenance of a developer portal as negligible. We believe the recurring annual costs will be substantial and may result in decreased availability of free checking products as data providers impose account maintenance fees to offset the rising costs of regulatory compliance.

The Bureau's permission that the consumer should not pay to access or share their data through the developer portal is a reasonable one. However, by prohibiting data providers from passing on

[14] 88 Fed. Reg. 74814.
[15] 88 Fed. Reg. 74870.

some of the cost of creating and maintaining a developer portal, the Bureau is essentially forcing banks to recoup the cost of creating a developer portal indirectly – either through annual account fees, higher interest rates on loan, or greater fees for other bank services. The direct monetary beneficiary of access to customer data is the authorized third party who is now able to offer a financial product or service to that customer.

Under the Bureau's proposed framework, **data recipients are receiving all of the financial benefit of this rule while data providers are bearing all the cost** – as well as all of the risk of losing customers to competitors. Furthermore, it appears as though the proposal, as written, is deliberately favoring fintech data recipients to the detriment of incumbent banks and credit unions. Given the light supervisory framework to which these fintechs are subject relative to regulated depository institutions, this seems highly likely to result in consumer harm.

Data providers must be permitted to negotiate and charge reasonable fees for accessing the financial data of their customers. They have invested considerable time and financial resources to store and protect that data. Charging a flat fee for API access plus a fee per API call is currently industry standard practice and we do not see a reason this should change. **We propose banks be permitted to charge a reasonable fee each time a third-party company accesses information about a bank customer.** A reasonable fee would not be large enough to impact the pricing of loans or services offered to customers by third parties but would significantly help data providers offset the cost of maintaining a developer portal. It would also place the cost of this rule with the parties that ultimately reap the largest financial benefits – the data recipients.

Covered Data

The Bureau is proposing to require banks to make available the following categories of data:

a) Transaction information, including historical transaction information in the control or possession of the data provider.
    - A data provider is deemed to make available sufficient historical transaction information if it makes available at least 24 months of such information.
b) Account balance.
c) Information to initiate payment to or from a Regulation E account.
    - This category includes a tokenized account and routing number that can be used to initiate an Automated Clearing House transaction.
d) Terms and conditions.
    - This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.
e) Upcoming bill information.
f) Basic account verification information, which is limited to the name, address, email address, and phone number associated with the covered consumer financial product or service.

Community banks strongly object to being required to provide 24 months of transaction information. Very few community banks retain 24 months of data on individual transactions – most will retain twelve or six months of such data, and some retain as little as 90 days' worth. Records of

older transactions exist, but they are stored as .pdf files of customer bank statements. The Dodd Frank Act specifically exempts covered data providers from providing "any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information."[16] **In our view, 24 months of transaction data is more than community banks can retrieve in the ordinary course of business and a lower safe harbor of 6 months of transaction data would be more appropriate.**

Retaining additional transaction data may seem like a relatively simple undertaking, but it is not. Consider that each account may have hundreds or thousands of transactions per year and each community bank may have tens or hundreds of thousands of customer accounts. The data burden quickly becomes immense, as do the increased costs to store and safeguard the data.

Additional data retention also leads to slower speeds and decreased performance of computer systems – including both the customer and developer interfaces. This is particularly relevant with regard to developer interfaces which are required by this regulation to submit a response in 3,500 milliseconds in order for that response to be considered "proper." Requiring banks to send up to 2 years' worth of transaction data in response to every request from a third party will lead to much larger information packages and slower system response times. This will increase the likelihood of "improper" responses, making it much more difficult for data providers to remain in compliance with the rule.

In a similar vein, we are concerned with the requirement to provide third parties terms and conditions through the developer portal. Terms and conditions can be large files and are not generally attached to an individual customer's account. First, we believe that the regulation should provide more explicit requirements regarding the exact terms and conditions banks must provide third parties to satisfy this requirement. Second, rather than requiring banks to make terms and conditions available through the developer portal, which we believe will increase the latency and cost of the portal, banks should have the option to satisfy the requirement to provide access to terms and conditions by making them publicly available on the bank's website.

Requirements for Developer Interfaces

The proposed regulation establishes the following requirements for developer interfaces maintained by covered data providers:

1) Standardized format: The developer interface must make available covered data in a standardized format. A qualified industry standard created by CFPB-approved industry standards-setting bodies would count as a standardized format. In the absence of a qualified industry standard, the interface would be required to make available covered data in a format that is widely used by the developer interfaces of other similarly situated data providers.

[16] 12 U.S.C. 5533(b)(4).

The standardized format provision is appropriate as proposed. Allowing industry standard setting bodies to establish technical standards for APIs that enable data sharing is preferable to have standards set by regulation. Technical standards and industry best practices may change more quickly than the federal rulemaking process is able to adapt to them. Allowing industry standard setting bodies to react to these changes in real time will result in a more dynamic and secure framework for sharing customer data.

2) Commercially Reasonable Performance: A developer interface must provide commercially reasonable performance. To be commercially reasonable, it must have a proper response rate equal to or greater than 99.5 percent. A proper response is a response either fulfills the query or explains why the query was not fulfilled, is consistent with the reasonable written policies and procedures that the data provider establishes and maintains, and is provided in no more than 3,500 milliseconds.

The rigid criteria specified by the proposed commercially reasonable performance criteria are onerous and will increase the cost of creating and testing a compliant developer interface. Standards of commercial reasonableness should not be mandated, but should instead be negotiated contractually or established as part of a qualified industry standard.

However, addressing the criteria proposed by the Bureau, we believe mandating a response in less than 3.5 seconds for the interface to submit is unreasonable. Because some requests will require the submission of large quantities of transaction data or other customer data, they will take longer for the developer portal to transmit. Conversely, requests to transmit more limited data may be completed by the system more quickly. A better approach would be to require an average transmission time no greater than a fixed amount, rather than consider all responses submitted in more than 3.5 seconds as per se improper.

Furthermore, we believe that additional clarification is needed to specify when the 3.5 second clock begins to run. Under the proposed rule, upon receiving a request from a third party, data providers are permitted to ask the consumer to confirm the account(s) to which the third party is seeking access and the categories of covered data the third party is requesting to access. We believe that clarification is necessary to confirm that the clock to respond to a request for data only begins to run once customer confirmation has been received.

Community banks have also expressed significant concern with the requirement that systems provide a proper response rate of equal to or greater than 99.5%. This high of a proper response rate would require significant auditing and testing, increasing the cost of compliance. In addition, a high volume of requests could delay system responses beyond the 3.5 second response time, leading to a greater percentage of technically “improper” responses. We recommend not setting a specific proper response rate, and instead requiring a proper response rate that is reasonable.

3) Access Cap Prohibition: The proposal states that a data provider must not unreasonably restrict the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface and that any frequency restrictions must be applied in a manner that is nondiscriminatory and consistent with the reasonable

written policies and procedures that the data provider establishes and that comply with a qualified industry standard.

This requirement – which permits reasonable, non-discriminatory access caps – appears appropriate as proposed. API access caps can be reasonable and necessary to ensure that they are not abused by bad actors and continue to function normally. A blanket prohibition on any access caps could considerably drive up the cost of creating and maintaining a functioning developer portal. The Bureau strikes an appropriate balance between providing access to data and not creating unreasonable costs by allowing for the imposition of reasonable access caps.

4) Access Credentials (Prohibition on Screen Scraping): The proposal states that a data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface. This would prohibit the practice of screen scraping, where a third-party accesses information about a consumer using their username and password and logging in to an online banking portal.

For years, the trend in the industry has been to move away from screen scraping. Compared to accessing consumer information using an API, screen scraping may present greater concerns to customer privacy and data security because there are fewer limitations on the data that can be accessed by third parties once they obtain a consumer's login credentials. On the other hand, screen scraping can allow customers to consensually share their personal financial information with third parties using existing online banking portals, thus avoiding the expense and technical difficulty of creating a developer interface.

The text of Section 1033 of the Dodd-Frank Act requires "to the extent appropriate" that any implementing rules "do not require or promote the use of any particular technology in order to develop systems for compliance."[17] By requiring the creation of a developer interface and prohibiting screen scraping, there is a colorable argument that the CFPB is exceeding its statutory authority by promoting the use of APIs as the particular technology required to comply with the rule.

Therefore, while APIs do offer improvements to privacy compared to screen scraping, we cannot endorse an outright prohibition of screen scraping. We urge the Bureau to be technology neutral, particularly with respect to small depository institutions, and allow individual banks the choice to weigh the pros and cons of building a developer interface, permitting screen scraping, or prohibiting all third-party access to customer data.

5) Security Program: Developer portals would be required to comply with either Section 501 of the Gramm-Leach-Bliley Act (GLBA) or the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

This requirement is appropriate as proposed. The Gramm-Leach-Bliley Act's Safeguards framework would apply to all or nearly all companies that are required to act as data providers under the rule.

[17] 12 U.S.C. 5533(e)(3).

This framework is already well understood by the financial services industry and is a robust standard for protecting consumer data. Additional data security requirements that exceed or add to the Safeguards framework for developer portals are not necessary.

Denying Access/Third-Party Vetting

Under the proposal, a data provider may deny access to a consumer or third-party access to a developer interface based on risk management concerns. To be considered a reasonable denial, the denial must be "directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner."[18] While we are supportive of the requirement for third parties to be subject to either Section 501 of the Gramm-Leach-Bliley Act or the Federal Trade Commission's Standards for Safeguarding Customer Information, we are concerned that it will be extremely difficult for any data provider to adequately vet all possible third party data recipients or to accurately monitor their compliance with the safeguarding standards.

This is deeply concerning for community banks because if there is a breach at a third-party company and a customer's data is stolen and/or misused, customers will likely blame the bank. Furthermore, we are concerned that banks will ultimately bear the financial liability of making customers whole – even though the failure to provide adequate data security was the fault of the third-party. We see this pattern now in the realm of check fraud and virtual payments fraud – even though the customer's loss is caused by fraud and negligence of third-parties, it is the payor bank that ultimately reimburses their customers for losses.

The Bureau could mitigate these concerns by clearly specifying that **financial liability for breaches lies with the party where the breach occurs** – and requiring third party data recipients to indemnify data providers when breaches at the third party occur. Furthermore, we believe the Bureau should create a list of third-party data recipients that are examined by the Bureau and that the Bureau certifies to comply with either Section 501 of the Gramm-Leach-Bliley Act or the Federal Trade Commission's Standards for Safeguarding Customer Information. Banks should be permitted to reasonably deny access to third parties that do not appear on this Bureau maintained "Whitelist."

Being able to rely on a list of Bureau approved counterparties would save data providers the cost and time required to vet all potential third parties. It would also be an important benefit to consumers because they could be sure that their data was being shared only with companies that are supervised for compliance with industry standard data security protections.

Responding to Requests by Third Parties

A data provider is required to respond to a request by an authorized third party when it receives information sufficient to:

(i) Authenticate the consumer's identity;

[18] 88 Fed. Reg. 74871.

(ii) Authenticate the third party's identity;
(iii) Confirm the third party has followed the authorization procedures; and
(iv) Identify the scope of the data requested.

The data provider is permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm:
(i) The account(s) to which the third party is seeking access; and
(ii) The categories of covered data the third party is requesting to access.

We support the proposed provision allowing data providers to confirm the scope of the third party's authorization. We believe the provision should be clarified further to permit a data provider to confirm with a consumer that they have provided authorization in the first place.

Furthermore, we believe that data providers should receive a copy of the authorization document required by proposed 12 CFR § 1033.401(c).

Standard Setting

We support the Bureau's proposed approach of allowing qualified industry standards for APIs to be established by Bureau recognized standard-setting bodies that meet the agency's criteria as being fair, open, and inclusive. We have consistently argued that technical standards are best set by industry standard setting groups than prescriptive regulations because both technology and industry best practices can change more quickly than federal regulation. As long as these standards are created by industry bodies that are trusted and allow the participation of a wide variety of stakeholders, we believe they are a superior alternative to standards prescribed by regulation.

The Independent Community Bankers of America is a member of the Financial Data Exchange (FDX), which is an industry standard setting body that intends to seek recognition as a qualified standard setting organization. We believe that FDX meets the Bureau's proposed standards for openness, balance, due process, appeals, consensus, and transparency. Therefore, we encourage the Bureau to grant FDX recognition pursuant to proposed 12 CFR 1033.141(b) once the rule is finalized.

Third Party Obligations

Under the proposal, third party data recipients are subject to the following obligations:

1) <u>General Limitation on Collection, Use, and Retention of Consumer Data:</u> A third party is to limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. Targeted advertising, cross-selling of other products or services, or the sale of covered data are not reasonably necessary to provide any other product or service.

We are supportive of this proposed limitation on the use of consumer data by third parties, particularly its prohibition of selling data to additional third parties. Community banks consistently expressed concerns that once customer data leaves the bank and goes to a third party, they have no control over how that data is used or whether it is sold to other third parties without the banks'

knowledge. This could be harmful to consumers because if third parties were permitted to sell data, they may not sell the most complete or current form of the data, leading to decisions being made about a consumer based on incomplete data.

In the market today it is common, when a bank pulls a credit report about a customer who is seeking a loan, for the credit rating agency to sell what are known as "trigger leads" to other lenders. This can result in the customer receiving dozens of unsolicited loan offers and often leaves them with the false perception that it is the community bank where they inquired about a loan that sold their information. The selling of leads by third parties for the purpose of targeted marketing can lead to predatory lending behavior, damage customers trust in the banking system, and cause customer annoyance.

Therefore, we believe the proposed prohibition on selling customer data or using customer data for cross-selling and targeted advertising without explicit customer consent is appropriate. We are still concerned that some third parties may seek to get around this provision by requiring consumers to sign long or confusing consent documents that permit these otherwise prohibited uses.

2) Duration: Third parties will be required to limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization. After one year, third parties will be required to receive reauthorization from the consumer.

We agree with the Bureau that there should be a limitation on the duration that third parties can collect consumer data. However, we do not believe that a one-year period should be considered per se reasonable for possible authorized use. For example, if a company is collecting customer data to underwrite a loan, it is only reasonable for them to collect that data for as long as it takes them to make a credit decision. This could be hours or days rather than a full 12 months.

Our understanding is that the 12 months functions as a ceiling rather than a floor – that is that no third party could collect data for more than 12 months without reauthorization but that a shorter period may apply depending on the permitted use. We believe that the Bureau should further clarify this in the regulation.

3) Accuracy: Third parties are required to establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party.

While we agree generally with the notion of requiring data recipients to maintain policies and procedures to ensure the accuracy of consumer data, we do not believe there is a practical way for community banks to determine whether such policies and procedures are effective or whether third parties are actively adhering to them. In other words, requiring policies is a good first step, but if third party data recipients do not adhere to the policies, it will be ineffective. In our view, the Bureau should act in a supervisory capacity to ensure that larger third-party data recipients are effectively implementing their policies to ensure data accuracy.

4) Data Security: Third-party companies will be subject either to Section 501 of the Gramm-Leach-Bliley Act (otherwise known as the Safeguards Rule) or the FTC's Standards for Safeguarding Customer Information.

Because the GLBA standards apply to any company engaging in activities that are financial in nature, it is our understanding that virtually all third-party companies that receive consumer financial data will be covered by this standard. In our view, this is appropriate. Banks rigorously comply with the GLBA standards and have a good record of protecting consumer data.

As with the previous provision, the key to this provision's effectiveness will depend on the conduct of third-party data recipients. Banks are not well-positioned to vet the data security programs that every third-party data recipient uses, nor are they well-positioned to ensure that third parties comply with their own written policies, maintained up to date software, or adequately train their employees with respect to data security and data privacy. Here again we think the Bureau should exercise its supervisory power to ensure that third party data recipients are complying with the relevant safeguarding standards and to take action against companies that do not. Furthermore, data providers would feel more comfortable sharing customer data with third parties that have been vetted and examined by the CFPB.

5) Provision of Covered Data to Other Third Parties: Before providing covered data to another third party, the third party will require the other third party by contract to comply with the third-party obligations described in the regulation.

We support this provision as proposed. As customer data moves farther from the data provider, the risk of the data being misused, compromised, or not up to date increases, so it is important for third parties that are further attenuated from the data provider to maintain adequate security and data integrity standards.

6) Revocation of Third-Party Authorization: The third party will provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's covered data that is as easy to access and operate as the initial authorization.

This provision is appropriate as proposed. We believe it should be easy for consumers to revoke third party access to their data.

Data Aggregators

The proposed rule permits a data aggregator to perform the authorization procedures on behalf of the third-party seeking authorization to access covered data. The third-party seeking authorization remains responsible for obtaining the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing. We are supportive of permitting the use of data aggregators. From a third-party risk management perspective, it is more feasible for banks to vet the practices of a few data aggregators than the entire possible universe of third-party data recipients.

Conclusion

ICBA appreciates the opportunity to provide feedback on the Bureau's proposed implementation of Section 1033 of the Dodd-Frank Act. As we stated initially, while this proposed rule includes some positive changes from the framework provided for the SBREFA Panel, it will still impose significant technological burdens and financial costs on community banks with no mechanism to allow them to recoup those costs from the third-party companies that ultimately benefit from the access to consumer financial data. The Bureau could reduce or mitigate this harm by exempting small banks from the requirement to create a developer portal or by allowing data providers to charge a reasonable fee for access to data to third parties.

Please feel free to contact me at Mickey.Marshall@icba.org if you have any questions about the positions stated in this letter.

Sincerely,

Mickey Marshall
AVP and Regulatory Counsel