INDEPENDENT COMMUNITY BANKERS of AMERICA®

Noah W. Wilcox, *Chairman*
Robert M. Fisher, *Chairman-Elect*
Brad M. Bolton, *Vice Chairman*
Gregory S. Deckard, *Treasurer*
Alice P. Frazier, *Secretary*
Preston L. Kennedy, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

Via Electronic Submission

February 4, 2021

Comment Intake–Section 1033 ANPR
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20552

RE: Docket Number CFPB-2020-0034; RIN 3170-AA78

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") advanced notice of proposed rulemaking ("ANPR") soliciting public comment to assist in developing regulations to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act" or "DFA").

Section 1033 of Dodd-Frank, titled "Consumer Rights to Access Information," gives consumers the right to access their financial records in electronic form. Section 1033 enabled an explosion of non-bank entities seeking the permission of consumers 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.

The Bureau is issuing this ANPR to solicit stakeholder input on ways that the Bureau might effectively and efficiently implement the financial record access rights described in Section 1033. This ANPR

[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 trillion in assets, over $4.4 trillion in deposits, and more than $3.4 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.*

follows previous steps taken by the Bureau[2] to seek information pertaining to Section 1033 implementation.

Summary

Consumers increasingly authorize 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 policymakers to carefully consider the privacy, regulatory burden, data security, and legal implications posed by permissioned third-party access to consumer bank accounts.

ICBA has profound concerns that non-bank entities, which access customer information and store bank login credentials, do not take the same care in protecting consumer privacy and data that community banks do. The integrity of consumers' data and privacy is only as strong as the weakest link protecting that information, and as more non-regulated entities handle a consumer's data, the risk of breach and/or loss only increases. Furthermore, non-bank entities accessing customer account data must be held responsible for ensuring the security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm as a result of accessing consumer data.

As the CFPB moves forward on developing regulations to implement section 1033, ICBA urges the following:

- Consider the burden third-party access imposes on community banks;
- Ensure standard-setting supports market developments;
- Adopt the common data-sharing principles issued by the CFPB in 2017[3];
- Ensure consumer control and privacy are consistent across the entire data ecosystem;
- Bring aggregators under the direct supervision of the CFPB;
- Consider the risks associated with data accuracy from data aggregators; and,
- Apply data security requirements, consistent with the Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA), to aggregators.

ICBA's Comments

Third-Party Access Imposes Undue Burden on Community Banks

As the trusted custodian of customer financial data, community banks play a critical role in both safeguarding data and enabling customer access to their data. Community banks are impacted in a variety of ways when their customers grant permissioned access to account data held by their institution.

The practice of screen-scraping by data aggregators is of significant concern. Bank operations can be impacted by increased traffic from data aggregators accessing their servers. Unexpected surges in traffic can overload servers, creating operational issues. Additionally, because aggregators use the customer's

[2] The Bureau has engaged with stakeholders via a request for information issued in 2016, a Bureau statement of principles in 2017, and a February 2020 symposium.
[3] https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

bank log-in credentials to enable screen scraping to access a bank customer's account, this access mimics customer activity. As a result, it is challenging for banks to discern if the access is coming from their customers, aggregators or third parties. This masked use of the customer's log-in credentials raises the risk of missing suspicious activity and red flags and increases account exposure to risk and fraudulent activity.

The risk for banks is additionally heightened because banks generally do not have a direct relationship with the customer's data aggregator and the third party. This means that banks do not have a way to ensure that the permission has been legitimately authorized by their accountholder and, as noted in a Treasury Department report, "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."[4]

Further, screen-scraping allows a data aggregator to obtain significantly more data than may be needed by the permissioned third-party, including sensitive personally identifiable information. The vast amounts of bank account data being held by data aggregators create an attractive target for fraudsters, which could be subsequently stolen or sold. Critically, banks are held accountable for the safekeeping of bank funds and account data, and may become unwittingly exposed to increased compliance, reputational and financial risks if an adverse event results in losses, even if responsibility for the event resides with a third party or aggregator.

Of note, banks' operations can be adversely impacted by increased traffic from data aggregators accessing their servers. Related to this, issues with connectivity and access can erode bank customer satisfaction. If an update to technology systems inadvertently "breaks" the link that enabled the screen scraping of the customer's bank account data, discontinuation of the flow of data to the permissioned third-party could negatively impact the bank customer.

Standard-Setting Should Support Market Developments Underway

ICBA encourages the adoption of the common data-sharing principles issued by the CFPB in 2017 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 Application Programming Interface ("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

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

implementing open APIs. For example, obstacles to developing these interfaces in the United States include rearchitecting banks' complex legacy back-office infrastructure.[5]

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 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 the 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.

Consumer Control and Privacy Should be Consistent Across the Data Ecosystem

The CFPB should extend GLBA-like standards to data aggregators. Under current federal law, technology companies, and other parties that process or store consumer financial data are not subject to the same federal standards and oversight as financial institutions. To effectively protect the customer's privacy and secure customer data, all parties who access or store customer financial information, should be subject to and maintain well-recognized standards such as those created by the Gramm-Leach-Bliley Act.

Once information is shared with permissioned third-parties, consumers may no longer have control of their personal and financial information. This leaves consumers vulnerable to entities that may mislead them about what they do with the collected information. Such vulnerabilities place an extraordinary burden on consumers to be vigilant in their research and knowledge of firms to which they may provide their online account credentials.

While ICBA fully supports consumers' rights to have access to their own information, such access should be properly balanced by ensuring consumer privacy is not needlessly threatened. The relationship between community banks and their customers is built on trust and a long-standing commitment to protect customer privacy. Firms that seek to provide services and require consumers to provide their online account credentials may not have the same commitment to protecting consumer privacy. Such

[5] https://bian.org/news-room/bian-in-the-news/psd2-api-challenge-open-banking/

entities may use or resell the financial data for cross-selling and other targeted marketing purposes, without the explicit consent of the consumer.

Banks are highly regulated and have been subject to rigorous security requirements for decades. Regulators require the banking sector to protect not only their own systems but their customer data as well. Additionally, they must have policies and procedures in place to identify, prevent, and mitigate identity theft. As a result of the GLBA, banks are required to have administrative, technical, and physical safeguards and standards in place to ensure the security and confidentiality of customer information. However, protecting consumers' account data at banks is of limited value if it remains under-protected or exposed by other users.

By and large, consumers know that they have privacy rights associated with their banking relationships, but many are not aware that those rights may not transfer when they authorize access to their data. They presume their bank's protections apply. Consumers should have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

Data Minimization

ICBA strongly supports 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 their 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.

Transparent Consent Disclosures

Consumers must clearly understand to which company they are granting access to their banking data. Bank account holders may not understand that it is not the bank that is being given permission, but rather they are forfeiting their banking credentials to a third party. Use of bank logos and branding elements by data aggregators creates confusion and misleads bank customers because customers assume they are granting permission to the bank rather than a third party. Consent disclosures should identify specific data to be accessed and instructions on how to revoke permission. ICBA urges the Bureau to consider regulations that will require permissioned third parties to improve transparency and clarity in consent disclosures by specifically identifying the parties requesting permission, and clarifying who to contact with questions and concerns. Banks should not be required to provide disclosures on behalf of permissioned third parties.

Services that go beyond financial aggregation, such as money movement, should require separate and explicit consent disclosures from the permissioned third-party that include informing the customer of risks created by such services.

Data Aggregators Should be Subject to Data Security Requirements Consistent with the GLBA

ICBA believes that all entities holding consumer financial data should be subject to GLBA-like data security standards.

As data holders, community banks work vigorously to defend against security threats and take their role in securing consumer financial data very seriously. Community banks are governed by some of the strictest data security laws and regulations set forth by the GLBA and its impending regulations and Safeguards Rule. These regulations require financial institutions to disclose their information-sharing practices to their customers, safeguard sensitive data, and create robust data security. Protecting consumer financial data is central to maintaining public trust and key to long-term customer retention. Community banks are proud of the security they provide and believe existing laws and regulations appropriately mitigate risks to consumer financial data while that data is being held by community banks.

However, not all entities are governed by such strict security regulations or place the same importance on protecting customer data. As evident in the recent breach at SolarWinds, bad actors will look to weaker points in the financial services ecosystem to illegally access consumer data. These entities are not required to have strict data security practices, though they hold the same data. No matter how securely community banks hold consumer data, if others in the supply chain are not required to have similar practices, consumer data will be needlessly exposed to preventable threats.

Community banks are too often left to mitigate the damage done to consumers, while the breached entities are not required to fully address the damage they have caused. The following examples, while not directly related to consumer access, illustrate the issue of inconsistent data security regulation in the financial ecosystem.

- In 2014, when Home Depot was breached, community banks were responsible for replacing payment cards, notifying customers, implementing enhanced monitoring, and reimbursing customers for fraudulent transactions.
- In 2017, when Equifax was breached and sensitive personal information of millions of consumers was stolen, community banks faced untold damages due to the unique circumstances of the massive data breach. Community banks instituted at their own cost additional protective measures to deter customer identity theft and fraudulent transactions. Additionally, community banks bear the responsibility for costs associated with payment card cancellation and replacement, fraudulent charges, customer notification, and closing affected accounts, all while monitoring the risk of exchanging information with Equifax.
- In 2020, two significant breaches at American Banking Systems and SolarWinds have produced yet to be defined costs for community banks.

While these incidents vary considerably in type of attack and complexity, one constant remains true throughout – non-bank entities should (or must) have the same stringent protections in place as community banks to protect consumer data.

The integrity of consumer data is only as strong as the weakest link protecting that information. As more parties handle a consumer's data, the risk of breach and/or loss only increases. While the Dodd-Frank Act requires financial institutions to allow consumers access to their financial records, there is no explicit statutory provision requiring these same rights to be carried over to third parties with whom consumers have shared their online credentials. For this reason, ICBA urges the Bureau to hold all entities who handle consumer financial data to similar data security standards that community banks are held to under

GLBA. Securing financial data at the data holder level is of limited value if it remains exposed at other points due to varying security standards and requirements.

Regulatory and Legal Considerations

Regulatory Oversight of Data Aggregators

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, and compliance systems, or procedures; and (3) detecting and assessing risks to consumers and consumer financial markets.[6] 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.[7] 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 of harm to consumers continues to increase. Just as it has for other non-banks,[8] 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 ("EFTA") 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, including disclosures, error resolution, and rules related to unauthorized electronic fund transfers. The regulation also outlines the procedures consumers must follow in reporting errors with electronic funds transfers, 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.

---

[6] 12 U.S.C. 5514(b)(1)
[7] 12 U.S.C. 5514(b)
[8] The Bureau has exercised this authority for student loan servicing, debt collection auto-financing, and consumer reporting.

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 electronic fund transfer service provider. The regulation makes clear that a "person that provides an electronic fund transfer 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."[9] Clarifying data aggregators' roles as service providers will also trigger responsibilities related to disclosures, documentation, and error resolution.[10]

The purpose of the CFPB's non-bank supervision 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.

Risks to Data Accuracy from Data Aggregators

The transfer of data from the financial institution to a third-party presents risks with regard to data accuracy. Data aggregators often collect data by screen scraping based on where information appears on a website. When a financial institution updates its website or launches a new customer portal, the third-party must remap how to pull that content. This process can be challenging to maintain and can potentially introduce errors and inaccuracies in collected data.

Today, data holders, such as consumer reporting agencies and banks, are required by the Fair Credit Reporting Act ("FCRA") to maintain accurate consumer data. Yet, data aggregators may or 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 credit 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

[9] 12 C.F.R. § 1005.14(a)(1-2) Electronic fund transfer service provider not holding consumer's account.
[10] Ibid §1005.14 (b)(1) – (b)(2)

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.

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.

ICBA appreciates the opportunity to provide comments in response to this request. If you have any questions, please do not hesitate to contact me at Rhonda.Thomas-Whitley@icba.org or (202) 659-8111.

Sincerely,

/s/

Rhonda Thomas-Whitley
Vice President and Regulatory Counsel