March 3, 2022

Via Electronic Mail

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Re: National Institute of Standards and Technology – *Draft Report 8389 Cybersecurity Considerations for Open Banking Technology and Emerging Standards*

Ladies and Gentlemen:

The undersigned trade associations[1] (together "the associations") appreciate the opportunity to comment on the National Institute of Standards and Technology's (NIST) internal report on Cybersecurity Considerations for Open Banking Technology and Emerging Standards (hereinafter "report").[2] The associations commend NIST for identifying the importance of cybersecurity and privacy safeguards in the consumer financial data sharing ecosystem. The report, however, does not adequately address these important considerations or acknowledge the evolution in data sharing that has occurred in the United States in recent years and that continues apace.

In the United States, shifts in consumer demand for more digital and interactive financial products and services have dramatically changed the marketplace, which now includes an increasing number of fintechs and other companies not subject to the same comprehensive regulatory oversight as banks, but increasingly facilitating access to sensitive consumer data to provide such products and services.

This surge in adoption of digital products and services has accelerated banks' efforts to leverage market-developed technological solutions to help meet customer demand while ensuring consumers' sensitive financial data is kept private and secure. Unlike other jurisdictions in which consumer financial data sharing has been mandated by government action, this expansion of consumer data access in the

[1] Please see Annex A for a description of the associations.

[2] Voas, et al., "Cybersecurity Considerations for Open Banking Technology and Emerging Standards," National Institute of Standards and Technology draft report 8389 (Jan. 3, 2022) (*available at*: https://doi.org/10.6028/NIST.IR.8389-draft).

United States has developed via innovation in the marketplace. Under an industry-driven approach, participants can innovate and adapt more quickly to market changes and develop safer solutions.

The associations support innovation and welcome competition in payments and other financial products and services when this innovation is conducted responsibly and in a way that ensures customers are protected through consistent regulation and oversight. In this regard, the associations support the ability of bank customers to securely connect their bank accounts to the third-party apps of their choice, which in some cases may involve the interposition of a data aggregator to collect the customer's information from a financial institution and provide it to the app. It is critical, however, that consumers' personal and financial information remains secure when it is shared between financial institutions and third parties. Ensuring the security of customer data is, and will remain, a top priority for the banking industry.[3]

We have concerns that the report does not sufficiently address all of the complexities and risks that an open banking regime may introduce, nor does it provide recommendations for cybersecurity or privacy standards, contrary to both the title and purported purpose of the report.

In addition, the report generally endorses open banking without providing a complete discussion of the potential benefits and risks of increased data sharing and recommending appropriate privacy and cybersecurity measures to address those risks, consistent with the thoughtful approaches employed by NIST in development of the Cybersecurity and Privacy frameworks, respectively. Nor does the report reflect consultation with key stakeholders in the data sharing ecosystem such as banking organizations, fintechs, or the Financial Data Exchange (FDX), an industry standard-setting body that was established for the sole purpose of developing security protocols for Application Programming Interfaces ("APIs") to facilitate a more secure connected banking ecosystem.

Finally, section 1033 of the Dodd-Frank Act provides the CFPB with authority to promulgate rules regarding consumer access to financial records. The CFPB has taken several steps to gather information about the consumer data sharing ecosystem but has not yet issued proposed rules to implement section 1033.[4] For these and other reasons described herein, we recommend that NIST delay further action on this report until after the CFPB has proposed a rule under section 1033. Such a proposal should provide NIST with a more concrete basis on which to provide recommendations relevant to the U.S. consumer data sharing ecosystem. We also recommend that any further action on this report should proceed only after NIST engages in further information gathering and discussion on the current state of the financial data sharing ecosystem in the United States, including consulting with key market participants and stakeholders, and revise the report to address the full range of significant risks and benefits that would have to be addressed in an open banking regime to ensure the security and privacy of consumers' data. We elaborate on these recommendations below.

---

[3] SIFMA notes that the concerns expressed in this letter generally are the same for all of its members, including those that are not banks or bank affiliates.

[4] See, e.g., CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (October 18, 2017), *available at* cfpb_consumer-protection-principles_data-aggregation.pdf (consumerfinance.gov); Advance Notice of Proposed Rulemaking issued by the Consumer Financial Protection Bureau seeking input on consumers access to financial records pursuant to Section 1033 of the Dodd-Frank Act. 85 Fed. Reg. 71003 (Nov. 6, 2020).

I. The Report Presents a Positive View of Open Banking without Discussing the Full Range of Risks and Benefits

As an initial matter, the report states that it is "not intended to be a promotion of OB within the U.S.," yet presents a number of supposed benefits of open banking while providing limited discussion of the risks that arise when data sharing is expanded without accompanying data protection and privacy controls. For example, the report defines open banking as follows:

> Open banking (OB) describes a new financial ecosystem that is governed by a set of security profiles, application interfaces, and guidelines for customer experiences and operations. OB ecosystems are intended to provide new choices and more information to consumers, which should allow for easier interaction with and movement of money between financial institutions and any other entity that participates in the financial ecosystem. OB also aims to make it easier for new actors to gain access to the financial sector (e.g., smaller banks and credit unions), has the potential to reduce customers fees on transactions, and is already in use in various countries.

This definition itself only describes potential positive outcomes from open banking, such as providing "new choices and more information to consumers, which should allow for easier interaction with and movements of money between financial institutions" and "has the potential to reduce customers fees on transactions . . ." It also says it would make it "easier for new actors to gain access to the financial sector (e.g., smaller banks and credit unions)." But NIST cites no empirical evidence or research to support these statements.

In addition, Section 5 purports to describe "Positive Outcomes and Risks" but essentially only lists positive outcomes that could result from open banking, such as enhancing fraud detection and prevention methods, improving consumer experience, reducing screen-scraping and other less secure methods of data sharing.[5]

While so-called "open banking" has the potential to help facilitate increased consumer choice among financial services providers, absent appropriate data protection controls and oversight, an open banking regime also has the potential to raise significant cybersecurity, privacy and fraud challenges that the draft report does not discuss in any meaningful way. For example, while the report acknowledges that screen scraping continues in the United States, it inaccurately states that "Although there is a general appreciation within the U.S. financial services industry of the benefits – even the necessity – of adopting an open banking model, the lack of clear consensus regarding how to implement such a model (whether mandated by laws and regulations or reached independently by the industry itself) has arguably been a significant obstacle to the realization of a U.S. open banking ecosystem."[6] On the contrary, there is a general consensus that there are benefits to increased data sharing, but that such data sharing also presents risks – such as those from screen scraping – that must be addressed and that the industry must move to more secure means of data sharing.

[5] Report at 23.

[6] Report at 19-20.

In addition, the report also states that "Having an open platform should stimulate the means of securing financial systems, such as by enabling better methods for detecting and preventing fraud. At a much larger scale, OB could serve as a foundation upon which measures of risk and stability can be built, thereby preventing or predicting potential weaknesses before they occur."[7] It is unclear what methods for detecting and preventing fraud NIST means to suggest exist or could be implemented in open banking. Rather, an expansion of open banking, which involves more data sharing across multiple entities, including the ability to move money, could in fact *expand* opportunities for fraud, particularly as the ecosystem is opened to more and more nonbanks not subject to the same comprehensive regulatory oversight as banks.

Banks use a variety of measures and technologies to identify and defend against fraud, some of which would be lost or degraded if data aggregators or other third parties are allowed to initiate an increasing number of transactions on behalf of the consumer without being legally mandated to implement fraud prevention and consumer protection measures similar to those required of banks.[8] It is important to note that banks are required by law and regulation to protect consumer data and establish and maintain robust programs for this purpose. Further, banks are regularly examined for compliance with these requirements. Unless all entities in the ecosystem are subject to the same legal requirements and oversight for security and fraud detection, fraud could expand dramatically while the ability to combat it could diminish.

The report also does not discuss at any length the complexities presented regarding the assignment of liability for unauthorized transactions and security breaches, including under Regulation E, in an open banking ecosystem, although it does reference that this is a concern among relevant parties in the United States.[9]

II. The Report Does Not Provide a Full View of the Current State of the Data Sharing Ecosystem

The report lacks a comprehensive discussion of the current state of the financial data sharing ecosystem in the United States, crucial to lay the foundation for discussion of the future state if open banking is implemented. The report acknowledges the risk of "data leakage" that could result from "mandating, or at least fostering, adoption of OB" if institutions are not prepared to implement "proper security guidelines, designs, policies, [or] APIs" or were to create "improperly secured endpoints."[10] In other words, the risks to consumer data security could increase unless ***all*** institutions in the data sharing ecosystem adopt appropriate security controls. Yet, the report states that "While market competition of services ensures that customers can get more than just a bundle deal, it also opens the possibility of inferior third-party options appearing as alternatives. Given that a fraction of today's third-party services

[7] Report at 23.

[8] For example, transaction transparency may be reduced when a third party initiates a transaction on behalf of the customer, limiting a bank's ability to view the details of a transaction, including the digital footprint of the consumer. Further, some of the aggregators actively thwart multi-factor authentication, which banks use to safeguard customer accounts, which could allow more fraud to occur undetected.

[9] 12 CFR Part 1005 et. seq.

[10] Report at 23.

use less accurate, less standardized, and less secure methods (such as screen scraping to gather data), having an open standard should be a net positive."[11]

In addition, the report states that "OB can improve the security of the current e-banking ecosystem by offering a set of common standards, both in software and in operational guidelines, so that large and small institutions could be held to the same level of data security."[12] Thus, to the extent that risks of data sharing are acknowledged, the report in some respects appears to assume that any movement to open banking would necessarily be accompanied by improved risk management controls. That conclusion is not adequately explained, but it appears to assume that if open banking were mandated, appropriate safety and security controls would similarly be mandated. At a minimum, the report should engage in a more robust discussion of how and on what basis these conclusions were drawn. Furthermore, this discussion largely ignores the evolution in the consumer data ecosystem that has taken place in the United States absent any mandated open banking regime, as well as the possible solutions to address the challenges that remain in the United States.

Consumer-permissioned access to authorized data has increased competition in the provision of financial services to consumers. Banks are highly incentivized to facilitate consumer-authorized data access as a means of increasing consumer satisfaction and enhancing their digital experience. The banking industry has been working for years to develop technical solutions that enable consumer-permissioned access to financial data while providing adequate data protections, including through collaborations between banks, fintechs, and data aggregators that demonstrate how the industry has progressed the data sharing marketplace to better serve consumers.

First, the industry continues to move away from screen scraping and credential-based data access towards data sharing through APIs, which facilitate the transfer of consumer financial data through tokenized access, thus removing credential sharing and allowing users to be securely authenticated at their own financial institution. Data sharing through APIs is more accurate and secure than screen scraping and credential-based data access, and continued adoption of APIs will benefit consumers and all market participants.[13]

The financial services industry collectively has advanced the marketplace towards common technical standards for the secure access of consumer-permissioned data. Several industry efforts have advanced the adoption of APIs in the United States. For example, FDX developed a common API technical standard for data sharing through an industry consortium of banks, data aggregators, fintechs and consumer groups. Over 28 million consumers are now using FDX's API for data sharing in North America.[14]

---

[11] *Id*.

[12] Report at 24.

[13] U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation* (July 2018), *available at*: https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

[14] *See* Press Release, "Financial Data Exchange (FDX) Reports 28 Million Consumer Accounts Use FDX API for Open Finance and Open Banking", *available at*: https://financialdataexchange.org/FDX/News/Press-Releases/Financial%20Data%20Exchange%20(FDX)%20Reports%2028%20Million%20Consumer%20Accounts%20Use%20FDX%20API%20for%20Open%20Finance.aspx.

Additionally, banks and data aggregators have begun entering into data access agreements to facilitate the data sharing process through APIs and to specify how data is protected and how and when data is accessed. The industry also is moving towards utilizing networks to facilitate access. For example, Akoya's Data Access Network facilitates direct connections utilizing FDX's API by providing a single point of integration for data providers and recipients and reducing the need for creating specific bilateral data access agreements.[15] Despite the industry's progress, screen scraping remains a widely used method for accessing payment account data, enabling the unsecure data harvesting of credentials to continue.

While the report mentions that screen scraping remains a threat in the United States, the report does not explicitly discuss the dangers this poses to consumers and the possible role the government could play to outlaw screen scraping, either through an act of Congress or coordination between the CFPB and the federal banking agencies in implementing section 1033 of the Dodd-Frank Act. Section 1033 provides the CFPB with authority to promulgate rules around consumer financial data sharing. The importance of this report in making robust recommendations regarding data security and privacy is all the more critical in light of the backdrop of potential government actions that could help to enhance the security of increased data sharing.

III. The Report's Recommendations Should be Enhanced to Ensure that All Entities Are Held Accountable and Liable for Protecting Consumer Data Privacy and Cybersecurity

The report acknowledges that "because banking deals with customer data, privacy is also a concern, and states that "OB initiatives should be proactive in adopting privacy frameworks, such as the NIST Privacy Framework . . . In particular, the five primary functions of the NIST Privacy Framework should be observed: Identify, Govern, Control, Communicate, and Protect."[16] It also acknowledges the importance of "the OB ecosystem's ability to ensure that the data remains protected" and that cybersecurity principles should be incorporated into the standard, such as the NIST Cybersecurity Framework" that provides "tenets to adhere to."[17]

The associations appreciate NIST's recognition that privacy and cybersecurity risks must be addressed in any open banking framework. Consistent with the report, we agree that participants in a connected banking ecosystem should also adopt industry best practices focused on protecting consumers. For example, the associations member companies regularly participate in joint public-private initiatives to reduce fraud and disrupt cyber-crime such as the National Cyber-Forensics and Training Alliance (NCFTA) that shares real-time information and serves as an early warning system to

---

[15] *See*, e.g., Press Release, "U.S. Bank and Akoya team up to accelerate safe, secure, and transparent consumer-permissioned financial data access", *available at*: Akoya and U.S. Bank team up to accelerate safe, secure, and transparent consumer-permissioned financial data access | Company blog | U.S. Bank (usbank.com) (Nov. 16, 2020); *see also* Akoya website at https://www.akoya.com/.

[16] The report also states that "Other privacy frameworks have been adopted as well. For example, the Open ID Financial API encourages stakeholders to adhere to the ISO/IEC 29100 privacy framework [72]. The FAPI explicitly calls out 11 categories of interest: consent and choice; purpose legitimacy and specification; collection limitation; data (access) limitation; use, retention, and data disclosure limitation; accuracy and quality; openness, transparency, and notice; individual participation and access; accountability; information security; and privacy compliance." Report at 27.

[17] Report at 27.

firms, enabling better protections and providing law enforcement with valuable information to disrupt criminal activities. Firms also participate in forums like the Financial Services Information Sharing and Analysis Center (FS-ISAC) which shares cyber threat intelligence information among firms and with government partners to protect against cyber threats that could harm financial institutions and their customers.[18] Additionally, firms adopt a number of frameworks and best practices, including the NIST Cybersecurity and Privacy Frameworks, International Standards Organization (ISO) standards, and adhere to Payment Card Industry (PCI) compliance standards, among others.

However, these suggested tools and practices are not themselves sufficient to address the risks to consumer data as it increasingly is transferred to less supervised entities. Curiously, the report does not address the numerous other requirements to which federal banking organizations are subject that are critical for helping to ensure consumer data remains secure and cyber-attacks are detected and deterred.

For example, while both the NIST Cybersecurity and Privacy Frameworks are useful tools to help organizations think about and manage risks, there is no oversight from an independent body or regulator to enforce the adoption of or adherence to those principles and practices. In contrast, banks that are subject to federal bank supervision and regulation are subject to numerous laws and regulations that govern how consumer data can be collected, used, and retained and how it must be secured. Indeed, over many years, banks have developed sophisticated systems to protect consumer data and to detect, prevent, and respond to cyber threats. These activities are subject to extensive regulatory oversight to ensure such protections are in place and can include financial penalties or restrictions on activities for failure to comply. In particular, banks are subject to the Gramm-Leach-Bliley Act and its implementing regulations that require maintaining consumer data privacy, extensive guidelines from the Federal Financial Institutions Examination Council (FFIEC) Information Technology handbooks,[19] and the federal banking agencies' third-party risk management guidelines.[20]

The report does not discuss these significant differences in oversight between banks and nonbanks in the United States in contrast to other jurisdictions that have implemented open banking. While the report includes a survey of different open banking frameworks, it fails to note that in contrast

---

[18] For more information on these initiatives, please see https://bpi.com/information-sharing-collaboration-issue-summary/

[19] FFIEC IT handbooks are used in the supervision of financial institutions and cover topics such as information security, management, technology architecture and operations, and retail payment systems.

[20] The federal banking agencies also have issued "Third Party Risk Management Guidelines" that outline the expectations for banks to manage the risks of counterparties with whom they have business relationships. The agencies recently proposed amendments to this guidance and requested comment on the extent to which banking organization may have "business arrangements" and third-party relationships with data aggregators, and therefore should manage these relationships consistent with the third-party risk management guidance." BPI submitted a comment on the proposed amendments to the TPRM Guidance and stated that data aggregators — including both those that engage in unilateral "screen-scraping" and those with which a banking organization may have a contract or other data sharing relationship — can pose meaningful risks to banking organizations and their customers but that the TPRM practices and expectations described in the Proposed Guidance would not be appropriate for either type of activity for several reasons. However, the ultimate expectations of the regulators in this regard remain unclear at this point. *See* BPI's comment letter in response to the "Proposed Interagency Guidance on Third-Party Relationships," available at: Microsoft Word - BPI Comment Letter - Interagency Guidance on Third Party Relationships (Docket ID(7661407.20).docx.

with the UK and other jurisdictions, nonbanks in the U.S. data sharing ecosystem are not subject to regular, direct regulation or supervision for privacy, security, prudential, or consumer protections, in contrast to federally regulated banks.[21]

To protect consumers and ensure that privacy and cyber risks are managed appropriately, all participants in the consumer data sharing ecosystem with access to consumer data should be subject to the same requirements and oversight for their privacy and security practices. Without these protections, U.S. consumers' information and financial health could be put at risk.

Finally, it should be noted that Congress or the CFPB also could take further action to bring data aggregators and other third-party data users under federal supervision. The CFPB has initiated consultations with industry around these matters and could promulgate new rules in the coming years.[22]

IV. The NIST Report Does Not Appear to Have Been Subject to the Procedural Rigor and Due Diligence Typical of NIST Publications

As described previously, the report does not reflect consultation with key parties in the financial data sharing ecosystem. Among the report's authors is the CEO of Stealth Software, a cloud data security company, that could stand to benefit if the United States were to move to an "open banking" ecosystem. There is no discussion or explanation of why the CEO participated in drafting the report or the extent or content of his contribution or participation, while other parties such as banking organizations, fintechs, and various entities that are working to improve security in the financial data sharing ecosystem were not consulted. One such key organization is FDX, which is composed of a cross-section of banks, third-party fintechs, data aggregators, consumer groups, and other financial industry groups that have aligned around a common API to standardize the security and authentication methods

---

[21] For example, as noted in the NIST report:

> "PSD2 limits but does not impose an outright ban on screen scraping by TPPs . . . Although [it] does effectively prohibit screen scraping as it was most frequently practiced prior to PSD2, some form of permissible screen scraping survives in the form of contingency mechanisms . . . as a compromise between the security risks of screen scraping and the potential competitive disadvantage to TPPs if an ASPSP's "dedicated interface" (i.e., API) fails or is unavailable . . . However, the RTS requires TPPs utilizing such contingency measures to identify themselves to the relevant ASPSP prior to 535 scraping, which theoretically mitigates some of the security risk for the ASPSP [33] . . . in the E.U., the GDPR ([37]) plays a crucial role alongside and beyond PSD2 in the legal and regulatory framework of the European open banking ecosystem.
>
> Further, Article 25 creates a "legal mandate for "data controllers" (i.e., entities that determine the purpose and means of processing individuals' personal data) to adopt both technical and organizational measures that implement the principles of "privacy by design" [39]. In the context of the PSD2 open banking framework, GDPR "data controllers" include both ASPSPs (such as FIs) and TPPs." Article 25 also requires organizations to only process personal data that are necessary for the specific purpose to be accomplished by the processing. Article 32 also requires organizations to implement technical and organizational measures "to ensure a level of security appropriate to the risk" presented by data processing, in particular from destruction, loss, alteration, unauthorized access, or disclosure of personal data that are transmitted, stored, or otherwise processed [37].

[22] For example, under section 1024 of the Dodd-Frank Act, the CFPB can engage in a larger participant rulemaking in order to supervise the activities of data aggregators and other similar firms.

for data transfer.[23] The broad adoption of FDX's API technical standard will improve security for the customer and create predictability for the industry. FDX continues to enhance its API specification by including new features and use cases for consumer-permissioned scenarios and has enhanced the data sharing ecosystem by developing user experience guidelines for the permissioning process and common data sharing terminology to align industry stakeholders.[24] With representation from market participants, FDX is uniquely situated to continue the development of technical standards for the industry and should have been a key party with whom NIST consulted in developing the draft report. Further, the report should include a more robust discussion of FDX's ongoing significant contribution to improving security in the connected banking ecosystem.[25]

In addition to common technical standards, the industry is moving towards utilizing networks to facilitate access. For example, Akoya's Data Access Network facilitates direct connections utilizing FDX's API by providing a single point of integration for data providers and recipients and reducing the need for creating specific bilateral data access agreements.[26] In this regard, Akoya could help provide scale to current consumer financial data sharing efforts that can be complex, time consuming, and costly for smaller banks or credit unions to implement. However, Akoya is not mentioned in the report and does not appear to have been consulted.

V. The Report Should Address Consumer Consent and Control

Finally, the report does not directly address the important principles of consumer control and consent over the use, sharing, and storing of their data. The fact that it is consumers' financial health and security that is at risk when their data is shared is not discussed to any significant degree. In this regard, the following two guiding principles should govern consumer data sharing:

- Informed consumer consent should be a precondition to any sharing of consumer financial information; and
- The consumer should have effective control over the type and amount of information that is shared, including potential re-use of the information.

Indeed, the report should discuss how consumers can be empowered to effectively control the sharing and use of their financial data. At a minimum, the report should discuss that consumers need sufficient information and clear mechanisms of control in order to make informed decisions about:

- the parties they are sharing their data with,
- the duration and frequency of permissioned access they are granting,
- the specific data elements they are sharing,

---

[23] *See* Financial Data Exchange website at https://financialdataexchange.org/.

[24] Press Release, *"Financial Data Exchange Releases FDX API Version 5"* (October 21, 2021), *available at* https://financialdataexchange.org/FDX/News/Press-Releases/Financial_Data_Exchange_Releases_FDX_API_5.0.aspx#:~:text=Financial%20Data%20Exchange%20(FDX)%20Releases%20FDX%20API%205.0.

[25] For example, *see* https://financialdataexchange.org/FDX/News/Announcements/FDX_Security_Specification_Boosted_with_FAPI.aspx.

[26] Press Release, "U.S. Bank and Akoya team up to accelerate safe, secure, and transparent consumer-permissioned financial data access", (Nov. 16, 2020); *see also* Akoya website at https://www.akoya.com/.

- the ability to revoke the access,
- the ability to require third and fourth parties to delete their data, and
- the purposes for which third parties may use their data.

Congress or the CFPB could take action to provide consumers with this control over their data, which could be explored in the report.

VI. Conclusion

The rapid expansion of the digital financial services marketplace in the United States has helped to facilitate increased consumer choice among financial services providers. While the benefits of an increasingly digital and competitive marketplace are many, ensuring the security of customer data remains of critical importance.

The NIST report does not adequately address all of these risks or reflect consultation with key market participants and stakeholders. Any future work NIST pursues on this topic should discuss the many serious risks – primarily to consumer data privacy and cybersecurity - that an increasingly open banking ecosystem presents and identify ways in which those risks can be addressed.

* * * * *

If you have any questions, please contact Paige Paridon by phone at 703-887-5229 or by email at paige.paridon@bpi.com.

Sincerely,

Paige Pidano Paridon
Senior Vice President, Associate General Counsel
Bank Policy Institute

Melissa MacGregor
Managing Director & Associate General Counsel
SIFMA

Rob Morgan
SVP Innovation and Strategy
American Bankers Association

Annex

The Associations

American Bankers Association: The American Bankers Association is the voice of the nation's $23.7 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $19.7 trillion in deposits and extend $11.2 trillion in loans.

Bank Policy Institute: The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

Securities Industry and Financial Markets Association: The Securities Industry and Financial Markets Association is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of its industry's nearly one million employees, SIFMA advocates on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. SIFMA serves as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance and efficient market operations and resiliency. SIFMA also provides a forum for industry policy and professional development.