March 3, 2022

Submitted to: nistir-8389-comments@nist.gov

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 Clearing House Association L.L.C. ("The Clearing House")[1] appreciates this opportunity to comment on the National Institute of Standards and Technology's ("NIST") draft report 8389 on "Cybersecurity Considerations for Open Banking Technology and Emerging Standards" ("Report").[2] The Clearing House and its members fully support the ability of consumers to safely and securely share their data with permissioned third parties and appreciate NIST's interest in improving stakeholder understanding of cybersecurity considerations for open banking technology and emerging standards relating to such considerations. The Clearing House has endorsed and fully supports the Consumer Financial Protection Bureau's *Principles for Consumer-Authorized Financial Data Sharing* ("CFPB Principles"),[3] a vital standard for open banking in the U.S., and believes that any standards adopted in the U.S. for open banking technology must comport with the framework outlined in the CFPB Principles. The Clearing House also notes that the Consumer Financial Protection Bureau ("CFPB") is actively engaged in pre-rulemaking activity related to the implementation of § 1033 of the Dodd Frank Act and

[1] The Clearing House Association, L.L.C., the country's oldest banking trade association, is a nonpartisan organization that provides informed advocacy and thought leadership on critical payments-related issues. Its sister company, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the U.S., clearing and settling more than $2 trillion each day. *See* The Clearing House's web page at www.theclearinghouse.org.

[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://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8389-draft.pdf).

[3] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf). *See also* Consumer Financial Protection Bureau, "Consumer-authorized financial data sharing and aggregation[,] Stakeholder insights that inform the Consumer Protection Principles" (Oct. 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf).

consumer permissioned data access, which is likely to establish material new standards relating open banking. Given such anticipated developments, the Report is premature and should be withdrawn and tabled until such rulemaking is complete.

The Clearing House appreciates the ability to comment on the Report and notes that NIST has historically done significant and valuable work in developing standards that advance cybersecurity and privacy risk management in the U.S., and that are broadly used by depository financial institutions.[4] The present Report, however, is premature and should be withdrawn. If NIST nevertheless decides to proceed with issuing the Report, then significant refinement must be undertaken for the Report to be comparable in caliber to, and provide the same valuable contributions as, the work that NIST has previously done. We hope our comments are helpful to NIST in addressing some of the Report's deficiencies and that NIST will withdraw, or, in the alternative, will substantially revise the Report if NIST decides to proceed.

I. Executive Summary and Recommendations

Although ostensibly focused on cybersecurity concerns, the Report contains minimal actual information relating to the cybersecurity risks associated with open banking. Further, the Report fails to accurately represent the current state of open banking in the U.S. today. Both deficiencies are critical to the Report actually being able to serve as a valuable contribution to a discussion of cybersecurity considerations related to open banking. Further, while the Report notes some of the regulatory developments in the U.S. relating to open banking, it leaves out others, which serve as important standards for financial institutions in their facilitation of open banking. Finally, the Report fails to give due consideration to the impact of anticipated rulemaking activity by the CFPB relating to the implementation of § 1033 of the Dodd Frank Act and consumer access to data, and the material new standards that the rulemaking is likely to create, thereby rendering the Report premature. Accordingly, NIST should either withdraw the Report pending the finalization of the CFPB's rulemaking activity, or, in the alternative, NIST should substantially revise the Report to ensure that it is comprehensive and accurate if NIST decides to proceed.

* * * * * *

[4] *See, e.g.*, National Institute of Standards and Technology, "Privacy Framework" (Jan. 2020) (available at: https://www.nist.gov/privacy-framework/privacy-framework); National Institute of Standards and Technology, "Cybersecurity Framework" (available at: https://www.nist.gov/cyberframework), and Version 1.1 (available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf); National Institute of Standards and Technology, "NIST Cyber Security Framework Comment Letter" (Jan. 22, 2018) (available at: https://fsscc.org/wp-content/uploads/2021/02/FSSCC_Submission_to_12-2017_NIST_CSF_Request_for_Comment_FINAL.pdf); National Institute of Standards and Technology, "Financial Services Sector Specific Cybersecurity 'Profile'," Cybersecurity Workshop (May 17, 2017) (available at: https://www.nist.gov/system/files/documents/2017/05/18/financial_services_csf.pdf); and work of the National Institute of Standards and Technology in connection with the Financial Services Sector Coordinating Council, generally (information available at: https://fsscc.org/).

If NIST decides to proceed with the Report, then in order to ensure that the Report provides a more balanced and accurate assessment of open banking in the U.S., and an appropriate contribution to the understanding of cybersecurity considerations for open banking technology and emerging standards, the Report should be revised to take into consideration the following:

- NIST should revise the Report to more accurately characterize open banking developments and approaches in the U.S. and other jurisdictions.
    - The U.S. has developed a robust open banking ecosystem through regulatory guidance and a market driven approach, connecting more consumers in the U.S. to open banking platforms than are connected in the United Kingdom ("U.K.") and Europe combined, and
    - The U.S. has a vastly more complicated and diverse financial ecosystem than many other jurisdictions, making the experience in other jurisdictions of questionable value.
- While open banking offers many potential benefits, it also presents substantial risks. The paper as written touches only briefly on cybersecurity risks and should be revised to reflect a more balanced and comprehensive view. Specifically, NIST should more fully set forth the risks associated with open banking, including cybersecurity risk, privacy risk, fraud, liability limitations, risks to bank IT systems, risk associated with credential-based access, risks associated with screen scraping, and concentration risk.
- Given the that report is directed to the U.S., the definition of open banking used in the Report and much of the discussion of open banking should be revised to take into account that a substantial amount of open banking activity in the U.S. is not accomplished through APIs and that, while the private sector has made great strides in the creation of an API standard and other standards, there is no established, uniform "security profile" or other "guidelines for customer experiences and operations" currently in the U.S.
- The NIST report recommendations should be revised to acknowledge that, while NIST frameworks may be beneficial tools to assist in managing the risks associated with open banking, the frameworks are voluntary and there is no regulatory and supervisory structure in the U.S. to ensure compliance. This is an essential risk of open banking, in that information (and through credential-based access consumer bank account passwords and IDs) is flowing from the highly-regulated and supervised depository financial institution environment to a much less regulated and in many instances not supervised data aggregator and fintech environment.
- The NIST report recommendations should be revised to acknowledge existing regulatory standards in the U.S., such as the CFPB Principles, and OCC and other federal financial regulatory guidance on third-party risk management. The NIST frameworks are broad, meant to be universally applied, and in many instances may not be sufficiently specific or sufficiently aligned with existing regulatory standards. Before releasing the paper and making recommendations, NIST should undertake a gap analysis between the NIST frameworks and existing regulatory standards to ensure the frameworks are fully aligned with U.S. regulatory guidance applicable to open banking.

II. Discussion

A. NIST Should Withdraw the Report

The Report fails to take into account the pre-rulemaking activity in which the CFPB is engaged to implement § 1033 of the Dodd Frank Act and consumer permissioned access to data. This rulemaking is almost certain to create material new standards relating to open banking. For the Report to be a relevant and lasting contribution to open banking, those material new standards would need to be taken into account in any discussion of cybersecurity risks and emerging standards. Therefore, it is The Clearing House's recommendation that the Report be withdrawn and tabled until the CFPB rulemaking is complete. Failure to do so risks the Report becoming rapidly outdated.

B. NIST Should Revise the Report to More Accurately Characterize Open Banking Developments and Approaches in the U.S. and Other Jurisdictions

1. Open Banking in the U.S. has Seen Explosive Growth through a Market-Driven Approach Coupled with Regulatory Guidance

Through a market-driven approach coupled with regulatory guidance, open banking in the U.S. has grown steadily over the last two decades. According to Akoya, a provider of data access and sharing technology, over 350 million accounts in the U.S., "including 57 percent of demand deposit accounts, a third of retail brokerage accounts, [ ] a quarter of defined contribution accounts," and "nearly half of credit cards issued," are accessible via consumer-permissioned, application-programming-interface-based data access.[5] And according to the non-profit, standard-setting organization Financial Data Exchange ("FDX"), 28 million consumer accounts in the U.S. and Canada use FDX's application programming interface, or API, for open finance and open banking data sharing.[6] This growth has been fueled not only by innovation in financial services, including from technological advances made by banks and nonbanks that make open banking connectivity possible, but also by robust consumer demand for online banking and payments services. Further, the market growth of open banking in the U.S. has been facilitated by the many private sector activities noted below.

The rise of fintechs and proliferation of fintech-provided financial solutions mean that financial services are frequently provided by companies not affiliated with the consumer's financial institution. These companies are not regulated to the same standards as depository financial institutions and, unlike in Europe and the U.K., there is no uniform supervisory

[5] *See* Akoyoa, "Akoya rings in 2022 with Huntington National Bank, M&T Bank, and Truist," Press Release (Jan. 24, 2022) (available at: https://www.akoya.com/news/Akoya-rings-in-2022-with-Huntington-National-Bank,-M&T-Bank,-and-Truist).

[6] *See* Financial Data Exchange, "Financial Data Exchange (FDX) Reports 28 Million Consumer Accounts Use FDX API for Open Finance and Open Banking" (Jan. 24, 2022) (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).

oversight or, sometimes, no oversight whatsoever over fintechs using and holding consumer financial data.[7] As is more fully discussed in section II(B) of this letter, this can raise a host of cybersecurity and privacy risks for consumers and banks that should be fully explored in the NIST report.

2. The Clearing House's Connected Banking Initiative

The Clearing House's Connected Banking initiative seeks to enable "innovation and customer control through a more secure exchange of financial data."[8] The initiative recognizes the need to move beyond a system of credential-based data access and screen scraping and to a safer, more secure, more transparent and consumer-centric API environment. The initiative is guided by input from The Clearing House's owner banks, which are some of the largest and most sophisticated banks in the world, and which have been on the forefront of creating a safe and secure environment for consumer data sharing.

The terms "credential-based data access" and "screen scraping" may sound innocuous, but they are not. Credential-based data access involves consumers sharing their internet banking platform login credentials (user ID and password) with a third party. These are the same login credentials that consumers use to authenticate into their internet banking platform in order to move money and initiate other financial transactions and services. When a consumer shares their login credentials, financial institution ("FI") data holders may not be able to distinguish whether the login credentials are being used by the consumer, an authorized third-party, or a criminal actor. Indeed, it is interesting to note that some data aggregator and data user agreements reviewed by The Clearing House *prohibit* the data aggregator's or data user's customers from sharing the data aggregator or data user's internet platform login credentials (provided by the data aggregator or data user) with any third parties, such practice apparently being viewed by those data aggregators and data users as a significant risk to their own data security and integrity.[9]

---

[7] Critical to the establishment of open banking in Europe and the U.K. was the establishment of robust, rules-based, supervisory frameworks that created information security and other standards for all parties involved in the open banking ecosystem. The absence in the U.S. of a supervisory framework applicable to data aggregators and many of their fintech clients is a distinguishing factor between Europe, the U.K. and the U.S. and a critical distinction that should be noted in any discussion of cybersecurity risks. . (*See, e.g.*, European Central Bank, "The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security" (Mar. 2018) (available at: https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html); *and* Competition & Markets Authority, "Retail Banking Market Investigation: Final Report" (Aug. 9, 2016) (available at: https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf), pp. 441-461 (proposing requirements for the largest banks in the U.K. to adopt API standards).)

[8] Detailed information regarding The Clearing House's Connected Banking initiative is available at: https://www.theclearinghouse.org/connected-banking.

[9] *See, for example,* Plaid, "End User Privacy Policy," at "Registration" (Dec. 30, 2019) (providing that users "may never share [their] Account information, including [their] Plaid Dashboard password, as well as [their] API authentication credentials, including [their] Client identification Number ('Client ID') and secret, with a third party of allow any other application or service to act as you"); *and* Robinhood Financial LLC & Robinhood Securities, LLC, "Customer Agreement," at "K. Electronic Access" (Dec. 30, 2020) (prohibiting Robinhood users from sharing their usernames and passwords with any third parties).

Similarly, the process of screen scraping also carries certain risks. Screen scraping refers to the practice by which a data aggregator or data user employs automated processes to "scrape" data from the FI data holder website. In most circumstances, such data includes far more data than is actually needed to power the product or service being provided, including personally identifiable information or other details that the consumer may not have authorized if the process were more transparent to, and capable of being controlled by, the consumer. In addition, screen scraping is more prone to inaccuracies and has the potential to create operational challenges for FI data holders.

Application programming interfaces ("APIs") offer significant advantages to credential-based data access and screen scraping. As the CFPB has noted:

> An API is a structured data feed that connects the account holder, such as the consumer's bank, to the data aggregator [note omitted]. Because an API requires an agreement between the account holder and the data aggregator, parties to an API have the opportunity to agree on terms regarding the scope of data that the account holder will provide to the data aggregator, how often the account holder will provide or update that information, limits on the data aggregator's use or resale of data, and other terms, such as the parties' respective liabilities to each other and the consumer.
>
> APIs do not require consumers to provider their security credentials to the data aggregator; instead, the consumer can authenticate the aggregator with the financial institution, and the institution will provide an access token to the aggregator. As a result, an API may limit a data aggregator's access to certain account information or account services, such as making electronic fund transfers.[10]

To facilitate the shift from credential-based access and screen scraping to APIs, The Clearing House is actively engaged in the development of new technology standards, infrastructure, innovative solutions to address risk management requirements, consumer research, legal agreements, and in ongoing industry collaboration.[11] The initiative is guided by the goal of acting "in the best interest of consumers [to] enhance safety and foster efficiency in financial services."[12]

The Clearing House's Connected Banking initiative has resulted in a number of important deliverables, including the Model Agreement that is mentioned in the NIST Report:

- Model Agreement: In order to enhance consumer control over the data they share with data aggregators and data users and to provide for a safer and more secure method to facilitate such sharing, the Connected Banking initiative has focused on

[10] Consumer Financial Protection Bureau, "Taskforce on Federal Consumer Financial Law Report[,] Volume I" (available at: https://files.consumerfinance.gov/f/documents/cfpb_taskforce-federal-consumer-financial-law_report-volume-1_2022-01_amended.pdf), pp. 489-490.

[11] *See* The Clearing House's Connected Banking initiative, *supra* note 8. The work being done by The Clearing House is specifically acknowledged in the CFPB Taskforce Report. *See* "Taskforce on Federal Consumer Financial Law Report[,] Volume I," *supra* note 10, at p. 495, note 139.

[12] The Clearing House's Connected Banking initiative, *supra* note 8.

accelerating the ability of data holders, data aggregators[13] and data users to establish safe and secure direct connections through APIs. Recognizing that legal agreements between data holders and authorized entities[14] can take considerable time and resources to develop, The Clearing House, in collaboration with its member banks and in consultation with data aggregators and data users, developed a Model Agreement that can be used as a reference to facilitate the development of API-related data sharing agreements. The Model Agreement was based on a number of already existing bilateral agreements in the market and was specifically developed to be consistent with the CFPB's Principles and focus on consumer control and transparency, safety and security of the data, and appropriate accountability for any risks introduced into the system.[15] Bilateral agreements play a vital role in today's data sharing market. In the absence of a further legal framework being developed through regulatory action or otherwise, bilateral agreements are the only way that FI data holders can allocate liability, ensure transparency and consumer control, and address many other fundamental issues.[16]

- API Technical & Security Standards: The Clearing House and many of its member banks are founding members of the Financial Data Exchange ("FDX"), which was created to provide an organization through which cross-industry participants could develop, maintain, and facilitate the adoption of common API

[13] The Bureau has defined "data aggregator" as "an entity that supports data users and/or data holders in enabling authorized data access." ("Taskforce on Federal Consumer Financial Law Report[,] Volume I," *supra* note 10, at p. 494.) According to the Bureau's Taskforce on Federal Consumer Financial Law ("Taskforce"), which released a two-volume report on January 5th ("CFPB Taskforce Report") containing recommendations on how to improve consumer protections in the financial marketplace, "there may be at least 120 or as few as a handful of firms that engage in this activity." The CFPB Taskforce Report notes a Vermont law that requires parties that buy or sell third-party data to register with the secretary of state and that as of March 2019, 121 firms had registered. The CFPB Taskforce Report further notes that some of these entities – such as the National Student Clearinghouse and the nationwide consumer reporting agencies – are not typically thought of as data aggregators in the consumer finance market, even though they gather and provide consumer data. "Focusing more narrowly on financial data aggregators," the CFPB Taskforce Report posits that "there are as few as six significant firms in the market." (*Id.* at pp. 494-495.)

[14] The Bureau has defined "authorized entities" as "entities or persons with authorized data access to particular consumer financial data." (*See* Consumer Financial Protection Bureau, "Consumer Access to Financial Records[,] Advance notice of proposed rulemaking" (Oct. 2020) (available at: https://files.consumerfinance.gov/f/documents/cfpb_section-1033-dodd-frank_advance-notice-proposed-rulemaking_2020-10.pdf), p. 6.)

[15] More information on the Model Agreement is available at: https://www.theclearinghouse.org/connected-banking/model-agreement.

[16] While bilateral agreements may be needed for some time in the future, it is anticipated that small banks will ultimately be able to leverage bilateral agreements between their third-party service providers and data aggregators and data users. There is also the potential for entities that play a central utility role, like Akoya, to develop common rule sets or agreements that may ultimately take the place of some or all of the content that is covered in bilateral agreements today.

standards for sharing consumer financial data.[17] More detailed information on the work of FDX is provided below.

- Uniform Assessment Instrument: Meeting regulatory expectations for due diligence on parties with whom an FI data holder is sharing data (either through an API or otherwise) can be significantly burdensome in terms of time and resources committed for both the FI performing the due diligence and the data aggregator or data user on whom due diligence is being performed, with each FI historically performing one-off due diligence inquiries.[18] In order to create efficiencies and encourage the development of API relationships, The Clearing House developed a uniform assessment instrument that has been implemented in the market and that streamlines due diligence, allowing due diligence information to be collected once by assessment vendors and then shared by assessment vendors with multiple FIs through their secure portal. The shared assessment tool alleviates largely redundant processes across the financial ecosystem.
- Central Utility Option: The Clearing House and a number of its member banks played a pivotal role in the spinout of Akoya L.L.C. ("Akoya") from Fidelity Investments, Inc. and the positioning of Akoya to provide an option that solves for connectivity issues in an API-reliant ecosystem. The role Akoya is playing in the market is discussed in more detail below.
- Consumer Research: The Clearing House's Connected Banking initiative has been further guided by in-depth consumer research detailing consumer preferences and awareness regarding the data practices of the financial applications they use. Key findings include:
    - Consumers want more education and control over access to their information;
    - While consumers tend to feel secure about using financial applications, most are unclear about the terms and conditions of the services they have signed up for;
    - When consumers learn more about the actual practices of the data users that provide them with the financial applications they use, their trust in data privacy and security is eroded; and

[17] Additional information on The Clearing House's support for FDX is contained in: The Clearing House, "The Clearing House Supports Financial Data Exchange Work on API Technical Standards" (Oct. 18, 2018) (available at: https://www.theclearinghouse.org/payment-systems/articles/2018/10/data-privacy-10-18-2018).

[18] *See, for example*, OCC, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29 (Oct. 30, 2013) (available at: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html (accessed Jan. 7, 2021)), *and* OCC, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," OCC Bulletin 2020-10 (March 5, 2020) (available at: https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html) (FAQ #4, in particular, relates to the application of OCC guidance to data aggregation relationships).

- Most consumers are not aware of what personal and financial information financial applications have access to, for how long, and what actions the application service provider can take with their information.[19]

While The Clearing House appreciates NIST's mention of its work on the Model Agreement, The Clearing House believes that a more comprehensive discussion in the Report of all of the above developments would result in a more accurate picture of the state of open banking in the U.S. market.

3. FDX

FDX is an international, nonprofit organization operating in the U.S. and Canada that is dedicated to unifying the financial industry around the FDX Application Programming Interface ("FDX API"), which is a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data. FDX has broad stakeholder representation and is currently comprised of over 200 data holders (*i.e.*, financial institutions), data users (*i.e.*, third-party financial technology companies or fintechs and financial institutions[20]), data access platforms (*i.e.*, data aggregators and other ecosystem utilities), consumer groups, financial industry groups, and other permissioned parties in the user-permissioned financial data ecosystem.

FDX exists chiefly to promote, enhance and seek broad adoption of the FDX API technical standard, which allows for consumers within the financial data ecosystem to be securely authenticated without the sharing or storing of their login credentials with third parties. Broad adoption of the FDX API standard helps to transition the industry away from screen scraping (the retrieval of financial account information with a user's provided login credentials) and enhances the security and reliability of the flow of user-permissioned data between data holders, data aggregators, and data users. Moving the industry to API based access is important for a number of reasons. Most importantly, the use of credential-based access and screen scraping requires the sharing of sensitive consumer login credentials and provides limited consumer control over the amount of data consumers share with data aggregators and data users. Credential based access and screen scraping are also inefficient and can place stress on financial institutions due to the sheer number of automated logins. Consumers and financial institutions also bear significant risks associated with potential data breaches at data aggregators and data users and the potential for losses attendant to login credentials and other sensitive consumer information coming into the possession of criminal actors.

The FDX API technical standard seeks to replace the practice of credential-based data access and screen scraping with tokenized access in concert with API-based data collection, which allows a consumer to be securely authenticated at their own financial institution and permission only the data that the consumer would like to share. APIs provide the ability for the

[19] *See* The Clearing House, "Consumer Survey: Financial Apps and Data Privacy," p. 3 (Nov. 2019) (noting that "[m]ost financial app users are not aware of the personal and financial data the apps have access to") (available at: https://www.theclearinghouse.org/-/media/new/tch/documents/data-privacy/2019-tch-consumersurveyreport.pdf).

[20] Many financial institutions are both data holders and data users.

consumer to choose the type of data that is shared, with whom, for how long, and for what purpose. A standardized API along with other standards that have either been or are being created by FDX (such as authentication, authorization, certification, user experience and consent guidelines) create efficiencies in the ecosystem that help speed the adoption of API based data sharing. Without the FDX standards, the ecosystem would remain fragmented – using incompatible APIs, process and definitions. As a result of the development of the FDX API, over 28 million U.S. consumer accounts have already been transitioned away from screen scraping to a version of the FDX API.

In a little over three years, FDX has delivered key standards, guidelines and best practices into the marketplace. The following are the key FDX deliverables to date and those anticipated in the near future:

- FDX API Specification: Currently at version 4.5, the FDX API offers the ability to access over 620 different financial data elements, including banking, tax, insurance, and investment data, making it one of the most comprehensive Open Finance standards in the world. The FDX API utilizes foundational and globally interoperable standards for security, authentication, data transfer, authorization, API architecture, and identity and represents a global best-in-class solution set for user-permissioned data sharing.
- User Experience & Consent Guidelines: The User Experience and Consent Guidelines are intended to accelerate design decision-making during implementation of data sharing experiences. The guidelines specify what information and control must be given to consumers to ensure consistent data sharing experience regardless of where their data is held or who they are seeking to share it with.
- Taxonomy of Permissioned Data Sharing: In an effort to align industry stakeholders and help regulators and policymakers better understand and define the various roles and perspectives within the user-permissioned financial data ecosystem, FDX maintains a set of common terminology to be used as a taxonomy for the ecosystem. This documentation also includes a conceptual flow model to show how consumers interact with different participants within the current ecosystem that is evolving from legacy to new technology.
- Use Cases: Use cases are consumer-permissioned scenarios that help users minimize the amount of data they share by defining only the data elements that are needed for a given product or service. FDX use cases allow the financial services ecosystem to identify appropriately minimized and certifiable data sets needed to power an application and then utilize an industry-led standard like the FDX API to deploy and increase adoption of these use cases. So far, FDX has approved a Personal Financial Management (PFM) use case and expects to define and certify other specific use cases in the future, such as credit management and servicing, account verification, tax preparation and others

In addition to the above, FDX has two main artifacts directly relevant to any discussion of cybersecurity and privacy standards in the U.S. related to open banking (*FDX API Security Model* and the *FDX Control Considerations for Consumer Financial Account Aggregation Services*). These standards represent what FDX members believe are global best practices in

Cybersecurity in open banking. These documents are available free of charge at https://financialdataexchange.org/.

They provide guidelines in several security domains:

- Data Security
- Software Security
- Network Security
- Physical Security
- Operational Security
- Supplier Security

These documents set guidelines and recommendations that:

- Specify the collection and secure storage of FI customer account information leveraging industry standards and best practices.
- Put forth a new security reference architecture for enabling more secure financial data aggregation methods.
- Include security controls for aggregation service providers, aggregation technology providers, third-party vendors, and institutional account holders to adopt, with particular focus on identification, authentication, and authorization.
- Identify the need for authentication, authorization, and secure information exchange between aggregation service providers, FIs, and FI customers.
- Specify an FDX API security profile.
- Specify the methods for identifying intermediaries in the data sharing chain between Data Recipient and Data Provider.
- Specify best practices for securing sensitive data in transit.

The work being done by FDX has the benefit of facilitating the market's transition to APIs and management of cybersecurity risk in a host of ways, including providing for more secure data transmission methods, facilitating data minimization and enhancing consumer control. The Report only briefly mentions the API specification work done by FDX without mentioning other, important standards setting work done by FDX such as work on user experience and consent guidelines, taxonomy of permissioned data sharing, use cases, and security and privacy standards, all of which contribute significantly to addressing cybersecurity and privacy risks. The Report's sections on developments in the U.S. market should be revised to fully note the scope of FDX work and thereby facilitate a more accurate picture of the state of the U.S. market.

4. Akoya

While the development of API and other standards such as those developed by FDX play a critical role, standards still need to be implemented through actual API connectivity. Without the creation of a central utility, each data holder needs to establish individual connectivity with each data aggregator or data user. This one-to-one model, which would require a plethora of

individual and potentially differently configured connections across the ecosystem, can be made more efficient for data aggregators, data users, and data providers alike. Akoya provides an option that solves for the inefficiencies of this model by providing a one-to-many architecture, whereby each data holder can reach any Akoya connected data aggregator or data user through a single API connection with the central utility, Akoya. Data aggregators, data users, and data holders alike all have the opportunity to benefit from only integrating once with the Akoya Data Access Network in order to be able to securely exchange consumer-permissioned financial data with one another. The efficiency offered to the market by Akoya may be particularly beneficial to smaller financial institutions and their third-party service providers as they seek to implement API-based data sharing capabilities.

In addition, Akoya facilitates the control, transparency, safety and security that are needed to address cybersecurity and privacy risks in the data aggregation space. Consumers using Akoya never give out their usernames and passwords (or credentials) and instead login directly with their data holder to authenticate and then grant access to a data aggregator or data user. Further, Akoya is fully compliant with the FDX API specification. Members of the Akoya Data Access Network receive web applications that provide documentation, reports and information on data elements that are being accessed and the products that are accessing them. Consumers can review, update, and revoke data access to their authorized entities through an interface provided within their existing digital experience at the FI data holder.[21] Further, Akoya only acts as a pass through for consumer data and does not store it, avoiding the concentration risk associated with the massive amounts of consumer data that is being stored in many data aggregator models today.[22]

Surprisingly, the Report makes no mention of Akoya in its discussion of developments in the U.S. market, a particularly significant omission in light of the significant cybersecurity and privacy benefits Akoya provides. NIST should revise the Report to address this fundamental gap in the Report's content.

5. Legislative and Regulatory Developments

a. Dodd-Frank Act, § 1033

Any discussion of standards in the U.S. relating to open banking must start with an analysis of the requirements of § 1033, which establishes a consumer's right to access certain information.[23] While § 1033 sets forth important rights, it also contains important limitations. Specifically, the statute requires the transmission to permissioned parties of data only – it does not require that covered persons enable transactional processes that may be initiated by the data

[21] Additional information about Akoya and the Akoya Data Access Network is available at: https://akoya.com/.
[22] *See Id.* (noting that Akoya uses "a passthrough model").
[23] Specifically, a "covered person" must "make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or the account, including costs, charges and usage data." The statute further specifies that "[t]he information shall be made available in an electronic form usable by consumers." (*See* 12 U.S.C. § 5533(a).)

recipient.[24] Much of the discussion in the NIST Report seems to assume that open banking in the U.S. will enable transactional processes.[25] While open banking has the *potential* to do so, it is important to note that such potential is not a requirement of the U.S. legislative framework on open banking and the Report should be revised to note that limitation.

b. CFPB Principles

The CFPB released its Principles in October of 2017. The Principles, which took into consideration feedback provided by a wide range of stakeholders in response to the CFPB's prior RFI, set forth the CFPB's vision for how consumers should be protected when they authorize third-party companies to access their financial data to provide certain financial products and services.[26] The Principles were "intended to help foster the development of innovative financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives."[27] The Principles are fully supported by The Clearing House and its member banks, have guided the work of The Clearing House and other industry stakeholders as we have sought to implement the Bureau's vision, and remain highly relevant today. Since their release in 2017, much has been accomplished by the industry as it has worked towards making the Bureau's vision a reality, driven by a shared desire to protect consumers and the safety and security of the financial services ecosystem as the market for services using consumer-authorized financial data continues to develop.

While the Report mentions the Principles, and further notes the CFPB's October 2020 advanced notice of proposed rulemaking on regulations to implement § 1033 of the Dodd Frank Act, the Report does not undertake any attempt to reconcile the Report's recommendations (that open banking initiatives should adopt cybersecurity and privacy frameworks such as the NIST Cybersecurity and Privacy Frameworks) with the standards set forth in the Principles. As is more fully set forth in section II(F) of this letter, such an undertaking would be a valuable contribution to advancing cybersecurity and privacy activities in the U.S. and should be undertaken by NIST before finalizing the current recommendations in the Report.

c. Third-Party Risk Management Guidance

The Federal Reserve Board ("FRB"), the Office of the Comptroller of the Currency ("OCC") and the Federal Deposit Insurance Corporation have each published guidance on third-party risk management.[28] While not specific to open banking and data aggregator relationships

[24] In data processing parlance, the requirements set forth in § 1033 are "read only, not write."
[25] *See* "Cybersecurity Considerations for Open Banking Technology and Emerging Standards," *supra* note 2, at pp. 2, 4-6, 13 & 25.
[26] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," *supra* note 3.
[27] *Id.*
[28] *See* "Third-Party Relationships: Risk Management Guidance" *and* "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 18. *See also* Federal Deposit Insurance Corporation, "Guidance for Managing Third-Party Risk," FIL 44-2008a (available at: https://www.fdic.gov/news/financial-institution-letters/2008/fil08044a.pdf); Board of Governors of the Federal Reserve System, "Guidance on Managing and Outsourcing Risk" (Dec. 5, 2013) (available at:

(through which most open banking activity in the U.S. is currently accomplished), the guidance sets forth broad expectations for how banks and other federally regulated depository financial institutions will manage risks associated with various third-parties, including risks related to cybersecurity and privacy. In addition, the OCC has published FAQs detailing specific obligations applicable to relationships relating to consumer data access and the agencies have also published an ANPR seeking to create uniformity in their guidance on third-party risk that will potentially incorporate the OCC's FAQs.[29]

The agencies' guidance on third-party risk management and the OCC's FAQs, combined with agency regulations related to the Gramm-Leach-Bliley Act ("GLBA") and FFIEC guidance on cybersecurity issues, set forth important standards that banks and other federally regulated financial institutions must consider in their facilitation of consumer data access for permissioned third-parties.[30] Yet, none of these important standards are mentioned in the Report and no attempt is made to ensure that the Report's recommendations are consistent with these regulatory frameworks. As is more fully set forth in section II(F) of this letter, NIST should undertake a gap analysis between the NIST Cybersecurity and Privacy Frameworks and existing regulatory frameworks applicable to consumer data access. Such an undertaking would be a valuable contribution to advancing cybersecurity and privacy activities in the U.S. and should be undertaken by NIST before finalizing the current recommendations in the Report.

6. Comparison to Other Jurisdictions – The U.S. is Leading Open Banking Adoption

The Report appears to set up a comparison between the U.S. and other jurisdictions that does not fully give credence to the many developments in the U.S. market that are noted above. Fundamentally, with a market driven approach and a far more complicated financial ecosystem, the U.S. has to date connected far more consumers to open banking platforms than the U.K. has with a regulatory driven approach. While operating with a significantly smaller population than the U.S., open banking in the U.K. reached 4 million consumers and half a million small business by January 2022. In comparison, FDX's voluntary and market-led approach in the U.S. reached 28 million consumers by the same time with no regulatory mandate, or government resources, and without the benefit of a multi-year head start.

Additionally, comparisons between the U.S. market and other markets may be of little value given substantive differences. As noted in the Report, the U.K., European Union, Australia, Mexico, and Brazil are pursuing regulatory approaches to technical standards for user-

https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf); *and* Board, FDIC, and OCC, "Proposed Interagency Guidance on Third Party Relationships: Risk Management," 86 Fed. Reg. 38,182 (July 19, 2021) (available at: https://www.govinfo.gov/content/pkg/FR-2021-07-19/pdf/2021-15308.pdf).

[29] "Proposed Interagency Guidance on Third Party Relationships: Risk Management," *supra* note 28, at pp. 38, 184, 196-38, 203.

[30] *See* OCC, Board, FDIC & Department of the Treasury, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness," joint final rule (Dec. 19, 2000) (available at: https://www.federalreserve.gov/boarddocs/press/boardacts/2001/20010117/attachment.pdf); *and* Federal Financial Institutions Examination Council, "Cybersecurity Awareness" (May 2017) (available at: https://www.ffiec.gov/cybersecurity.htm) (providing guidance and numerous requirements, tools, and resources).

permissioned financial data sharing and data access. Such a regulatory-driven approach is common in these jurisdictions because these markets tend to have a single financial regulator and a concentrated banking market (*i.e.*, 9 major banks in the U.K., 4 in Australia, 4 in Mexico, etc.). The resulting technical standards often apply to a significant portion of the market all at once. However, without an ecosystem approach that considers the needs of a large and complex market, and its diverse participants (especially important in the U.S. with over 14,000 financial institutions), such technical standards can be ill-fitting to smaller market participants. In addition, regulatory driven standards in these jurisdictions have required significant technical resources and have incurred substantial start up and opportunity costs. Finally, and most importantly, regulatory standards in these jurisdictions have become more akin to regulatory compliance – meeting regulatory minimums – rather than standards that seek to address the full market, prioritize, or solve market problems, or that are able to adapt to market needs. The result has been standards that cover limited financial data elements, and adoption and utilization rates that are below market-led approaches, like those of FDX in the U.S., despite the weight of a government mandate and significant public resources. Moving the U.S. market towards API adoption for open banking is a far more complicated task than moving the U.K., European Union, Australia, Mexico or Brazil to an open banking standard. Such substantial differences and their impact should be noted in the Report's sections on the developments in various markets.

C. NIST Should Revise the Report to More Fully Set Forth the Risks Associated with Open Banking

The Report provides only a cursory discussion of the risks associated with open banking. Of the Report's 28 pages, only one actually focuses on risks and even that page is heavily focused on both "positive outcomes" *and* risks.[31] The lack of any real, substantive discussion of the risks associated with open banking seems odd for a report titled, "Cybersecurity Considerations…" and which is purportedly intended to help stakeholders "understand open banking and the associated cybersecurity and privacy issues."[32]

While there are benefits to open banking, there are substantial risks as well. As the OCC has noted:

> Information security and the safeguarding of sensitive customer data should be a key focus for a bank's third-party risk management when a bank is contemplating or has a business arrangement with a data aggregator. A security breach at the data aggregator could compromise numerous customer banking credentials and sensitive customer information, causing harm to the bank's customers and potentially causing reputation and security risk and financial liability for the bank.[33]

The risks associated with open banking include cybersecurity, privacy, fraud, liability limitations, risk to bank IT systems, risks associated with credential-based access and screen

[31] "Cybersecurity Considerations for Open Banking Technology and Emerging Standards," *supra* note 2, at p. 23.
[32] *Id.* at p. iii.
[33] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 18, at FAQ #4

scraping, and concentration risk. Many of these risks are exacerbated because open banking extends data access and usage outside of the highly-regulated and supervised depository financial institution ecosystem. Each of these risks should be explored in detail and analyzed in the Report:

Cybersecurity Risk: Risks include data breaches, hackers, malicious software and third-party apps as well as insider threats.

Privacy: The risk that sensitive banking credentials and personal financial information may be disclosed to unauthorized third parties.

Fraud: The risk that banking credentials or other sensitive personal financial information will be leveraged to perpetrate fraud.

Liability Limitations: The risk that a consumer will be unable to recover for damages caused by a permissioned third party as a result of a cybersecurity or privacy breach because of a liability limitation imposed by that third party on the consumer.[34]

Risk to Bank IT Systems: Risks include, in credential-based access, the inability of banks to identify and distinguish the party accessing the data – it could be a consumer, a permissioned third-party, or a criminal actor. Banks must build mechanisms to help identify the accessing party, but not all banks may have the wherewithal to do so. In addition, the only source available to banks to aid in identifying the accessing party is an IP address, which data aggregators may frequently change. Risks in screen-scraping include the ability of screen scrapers to access parts of bank systems that were not intended for high volume access, with the potential to crash the system or create availability issues elsewhere. While APIs allow for greater control and security, the development and maintenance of APIs can require significant capital, technical expertise, and can divert resources from other projects. Small banks may be particularly challenged in matching the investment that is required and may lack the technical skills to build and manage APIs.

[34] The risks of credential-based access and screen scraping are largely borne by consumers and FI data holders. Existing terms and conditions imposed by data aggregators largely disclaim all or most responsibility for any loss that may result from data aggregator or data user activities. To the extent not accepted by data aggregators and data users, losses will be borne either by consumers or data holders. Consumers bear risks related to misuse of their data and data breaches, including identity theft, breach of privacy, and fraud. FI data holders hold the majority, if not all, of the liability that would accrue from a data breach or the unauthorized use of consumer data, including all of the cost of recredentialing the consumer to prevent further losses and potential liability for unauthorized transfers. (*See* Letter from The Clearing House Association, L.L.C. to the Consumer Financial Protection Bureau, "Re: Docket No. CFPB-2020-0034 / RIN 3170-AA78[;] ANPR -- Consumer Access to Financial Records" (Feb. 4, 2021) (available at: https://www.theclearinghouse.org/-/media/new/tch/documents/advocacy/consumer-access-financial-records-02-04-2021.pdf), pp. 5, 9 & 40 (noting that any rulemaking should "prohibit data aggregators and data users from disclaiming liability to either the consumer or the data holder for acts or omissions relating to data while it is in their custody or control," and that in the absence of a legal framework from regulators financial institutions that hold data must rely on bilateral agreements to allocate liability).

Risks Associated with Credential-Based Access: Credential-based data access puts third parties in control of bank customer IDs and passwords. In addition, many data aggregators also collect answers to security questions. Given such information, it may be difficult if not impossible for banks to determine whether a permissioned third-party, a criminal actor, or the bank customer is accessing the consumer's information and accounts.

Risks Associated with Screen-scraping: Screen scraping frequently results in more data being collected than is needed to power the product or service being permissioned by the consumer. Ultimately, this results in more data being at risk for cybersecurity and privacy threats.

Concentration Risk: Data aggregators hold massive amounts of sensitive consumer information, providing an attractive target for hackers and criminal actors. As the Consumer Financial Protection Bureau ("CFPB") has observed, "currently [in the U.S. market,] *most* authorized data access is effected via data aggregators."[35] One U.S. data aggregator, which powers more than 4,000 financial services applications, is connected to a financial account of 1 in 4 U.S. adults, and, from a recent settlement, is known to have had information on more than 98 million households.[36]

As noted above, the risks of open banking are widespread for financial institutions and consumers, yet the Report inexplicably narrows them in its content and discussion. For example, in the comparison of open banking to conventional e-banking and P2P financial platforms the Report inexplicably states for open banking that "[p]rivacy and security issues are of concern among large proportions of lenders and consumers." Rather than citing only "lenders" the Report should note that privacy and security concerns broadly effect depository financial institutions and consumers. The Report also notes for P2P platforms, that "[c]ybercriminals have been reported to use compromised identities from massive data breaches to get loans." The risk, however, is not limited to just "loans" but extends to identity theft, the initiation of fraudulent transfers and other harm to consumers and banks. There is significant risk in open banking and the free flow of sensitive consumer information to fintechs and other third parties that such information can be used in the facilitation of fraud, and in creating other cybersecurity and privacy risks that broadly effect consumers and the banking system. The Report should be revised accordingly.

The Report also states, without foundation, that open banking can actually "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. But banks (both large and small institutions) are already held to substantially the same regulatory frameworks for data security (as noted in the regulatory

[35] Consumer Financial Protection Bureau, "Consumer Access to Financial Records," 85 Fed. Reg. 71,003, 71,006 (Nov. 6, 2020). *See also* "Taskforce on Federal Consumer Financial Law Report[,] Volume I," *supra* note 10, at p. 495, n. 139.

[36] *See* Plaid, "Plaid only shares your data with your consent[,] you're in good hands," Plaid Marketing (2022) (available at: https://plaid.com/how-we-handle-data/); *and* Penny Crosman, "Plaid settles class-action lawsuit for $58 million," American Banker (Aug. 6, 2021) (available at: https://www.americanbanker.com/news/plaid-settles-class-action-lawsuit-for-58-million) (noting that 98 million U.S. persons' accounts were accessed).

standards set forth above) and are supervised and examined for information security compliance. The Report fails to note, however, that fintechs are not held to the same standards. Therefore, it is difficult to understand how open banking would "improve security" absent the imposition of common standards on the entire ecosystem. The Report should be revised to note these facts.

Finally, the Report states, without foundation, that "having an open platform should stimulate the means of securing financial systems, such as by enabling better methods for detecting and preventing fraud." But open banking actually expands opportunities for fraud, through data sharing and an expansion of the firms that touch (and often store) that data, many without oversight and examination and without being held to the same standards as banks. Further, consumers are often subject to extreme limitations imposed by data aggregators and fintechs on any liability that the consumer may suffer as the result of a cybersecurity and data breach leaving them without a remedy. Banks in comparison are subject to robust supervision and examination, have clear regulatory obligations to make consumers whole (*e.g.*, the Electronic Funds Transfer Act and Regulation E) and employ sophisticated systems to detect and defend against fraud and protect their customers. The Report should strike the reference to open banking platforms enabling better methods for detecting and preventing fraud as there is no foundation for such a statement.

D. The Definition of Open Banking Used in the Report and Associated Discussion Should be Revised to Take into Account That a Material Amount of Open Banking Activity in the U.S. is Not Yet Accomplished Through APIs

The definition of open banking used in the Report doesn't fully align with the current state of the U.S. market. The Report defines "Open Banking" as "a new financial ecosystem that is governed by specific security profiles, application interfaces, and guidelines with the objective of improving customer choices and experiences."[37] Currently a material amount of open banking in the U.S. is not yet API based but, rather, relies on credential-based access and screen scraping, which carry significant additional risks as outlined above.[38] Further, there are no uniformly

[37] "Cybersecurity Considerations for Open Banking Technology and Emerging Standards," *supra* note 2, at p. 1, Section 1. *See also* p. 2, Section 1.3 (noting that "[o]pen banking describes a new kind of financial ecosystem that gives third-party financial service providers open access to consumer banking, transactions, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (APIs)"); *and* p.4, Section 1.3 (noting that "[i]n OB, banking entities interact with each other via APIs at the customer's direction and can offer better services on an a la carte basis").

[38] Statistics on the use of open banking in the U.S. are not readily available. Nevertheless, surveys of U.S. consumers suggest a very high degree of use of technology to manage money and make payments, as well as a high degree of account linking, including by API. (*See* Mastercard, "The Rise of Open Banking," p. 4 (2021) (finding 9 in 10 U.S. and Canadian consumers use technology to manage money, and 8 in 10 link their accounts); Letter from John Pitts, Plaid, to CFPB Director Kathy Kraninger (Feb. 19, 2020) (available at: https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf) (noting that as of the beginning of 2020, roughly 1 in 3 U.S. adults use fintech applications and 2,500 consumer financial applications use Plaid's technology); *and* Majority Memorandum, House Financial Services Committee, "Preserving the Right of Consumers to Access Personal Financial Data" (Sept. 16, 2021) (available at: https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-20210921-sd002.pdf), pp. 3-4 (noting that APIs help facilitate open banking and new financial products and services)).

adopted "security profiles, application interfaces, and guidelines" for open banking currently, though organizations like FDX have made great strides in setting standards that are being implemented by financial institutions in the U.S. Any definition of open banking used by NIST should comport with existing reality, particularly if the Report is to include a meaningful discussion of cybersecurity considerations and privacy issues associated with open banking. The Report should be revised accordingly.

E. The Report's Recommendations Should be Revised to Acknowledge that, While NIST Frameworks May be Beneficial Tools to Assist in Managing Risks Associated with Open Banking, the Frameworks are Voluntary and There is No Regulatory and Supervisory Structure in the U.S. to Ensure Compliance

The Clearing House Agrees that the NIST Cybersecurity and Privacy Frameworks are useful tools in managing cybersecurity and privacy risks, an assertion that is supported by their broad use by depository financial institutions today. But the Frameworks use by depository financial institutions that are subject to other, detailed cybersecurity, privacy and information security standards and supervision and examination for compliance with such standards is markedly different than the realities that would confront their use in much of the open banking ecosystem.

Fundamentally, in the open banking ecosystem compliance by data aggregators and fintechs will remain an issue given the lack of bank-like cyber and information security standards and the lack of supervision applicable to them. The NIST recommendations therefore understate the limited usefulness of the Cybersecurity and Privacy Frameworks and the gaps that must still be addressed in the open banking ecosystem. While banks can fill some of the gaps through the exercise of their third-party risk management responsibilities, which the Report should acknowledge, such responsibilities are no substitute for more robust cyber and information security standards coupled with meaningful supervisory oversight. Fundamental to the Report's recommendations, therefore, should be the development of bank-like information security standards for data aggregators and fintechs coupled with direct regulatory supervision.

F. The Report Recommendations Should be Revised to Acknowledge Existing Regulatory Standards in the U.S and NIST Should Undertake a Gap Analysis Between the NIST Frameworks and Existing Regulatory Standards to Ensure the Frameworks are Fully Aligned with U.S. Regulatory Guidance Applicable to Open Banking

As noted above, there are substantial regulatory standards that banks must comply with when facilitating consumer-permissioned data sharing. These standards include the CFPB Principles, OCC and other federal financial regulatory guidance on third-party risk management, FFIEC guidance on information security and cybersecurity risk management, and the federal financial regulators' regulations implementing GLBA. The NIST frameworks on the other hand are broad, voluntary, meant to be universally applied and in many instances may not be

sufficiently specific or sufficiently aligned with existing regulatory standards as they pertain to open banking.

The CFPB Principles, for example, set forth detailed expectations regarding data minimization and consumer control.[39] The NIST Frameworks allude to data minimization and control issues but the Frameworks are not sufficiently specific to encompass and ensure compliance with the standards set forth by the CFPB.[40] Similarly, the CFPB Principles provide that permissioned data access should "not require consumers to share their account credentials with third parties."[41] The NIST Frameworks contain no such requirement but speak broadly to the use of credentials.[42] Finally, the CFPB Principles contain detailed standards on consumer transparency, including that consumers should be informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers' accounts, including the identity and security of each such party, the data they access, their use of such data, and the frequency at which they access the data.[43] While the NIST Privacy Framework speaks broadly to the issue of transparency, it contains no similarly detailed analogue to the CFPB standard.[44] These are but three examples of where there are gaps between the NIST frameworks and existing regulatory standards.

The recommendation that open banking frameworks comport with the NIST frameworks is not itself inherently bad – as alignment in cybersecurity frameworks and privacy frameworks where possible is important to create efficiencies across an enterprise. But the recommendation should be predicated on a firm understanding of whether or not the Frameworks align with existing regulatory expectations. Therefore, before releasing the paper and making recommendations, NIST should undertake a gap analysis between the NIST frameworks and

[39] *See, e.g.*, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," *supra* note 3, at principle #2, Data Scope and Usability ("Third parties with authorized access only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary"), and principle #6, Access Transparency ("Consumers are informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers' accounts or other consumer use of financial services. The identity and security of each such party, the data they access, their use of such data, and the frequency at which they access the data is reasonably ascertainable to the consumer throughout the period that the data are accessed, used, or stored.")

[40] *See, e.g.*, National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity[,] Version 1.1" (April 2018) (available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf), p. 19 (noting that "[t]o address privacy implications, organizations *may consider* how their cybersecurity program *might* incorporate privacy principles such as: data minimization ….") (italics added for emphasis); "Privacy Framework," *supra* note 4, at p. 5 (while the development and implementation of "appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks" is noted in the framework, it is silent on who should actually be exercising that control).

[41] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," *supra* note 3, at Principle 1 (Access).

[42] *See, e.g.*, "Framework for Improving Critical Infrastructure Cybersecurity[,] Version 1.1," *supra* note 40, at PR.AC-1 and PR.AC-6.

[43] "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," *supra* note 3, at Principle 6 (Access Transparency).

[44] "Privacy Framework," *supra* note 4, at p. 6.

existing regulatory standards to ensure the frameworks are fully aligned with existing U.S. regulatory guidance applicable to open banking.

III. Conclusion

Substantial rulemaking activity is under way at the CFPB, and any worthwhile and lasting discussion of cybersecurity considerations and emerging standards relating to open banking will need to take such rulemaking into account. Accordingly, The Clearing House recommends that the Report be withdrawn and tabled until such rulemaking activity has been completed. Alternatively, if NIST decides to proceed with the Report, substantial revisions must be undertaken to ensure that the Report sets forth an accurate and balanced understanding of the current state of open banking in the U.S. and the cybersecurity considerations associated with it. NIST has done significant and valuable work in the past and we trust that it will either table or modify the Report to ensure it is of comparable character to other work that NIST has produced. We appreciate this opportunity to comment on the Report. If you have any questions regarding the contents of this letter, we would be happy to discuss them with you. You may reach me at (336) 769-5314 or Rob.Hunter@theclearinghouse.org.

Respectfully submitted,

/s/

Robert C. Hunter
Deputy General Counsel and Director of Regulatory & Legislative Affairs