October 18, 2021

Via e-mail: regs.comments@federalreserve.gov
Ms. Ann E Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Ave., N.W.
Washington, D.C. 20551

Via e-mail: comments@fdic.gov
James P. Sheesley
Assistant Executive Secretary
Attention: Comments-RIN 3064-ZA26
Legal ESS
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, D.C. 20429

Via https://regulations.gov/
Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street S.W.
Suite 3E-218
Washington, D.C. 20219

Re: *Proposed Interagency Guidance on Third-Party Relationships: Risk Management,* 86 F.R. 38182 (July 19, 2021), FRB Docket No. OP-1752, FDIC RIN 3064-A026, OCC Docket ID OCC-2021-0011

To Whom It May Concern:

The Clearing House Association L.L.C. and The Clearing House Payments Company L.L.C. (collectively, "The Clearing House")[1] submit this comment letter in response to the proposed interagency guidance on third-party risk management (the "Proposal").[2] The Clearing House appreciates the opportunity to comment on the Proposal. While the Proposal broadly covers risk management

[1] The Clearing House is a nonpartisan organization that engages in research, analysis, advocacy, and litigation focused on financial regulation that supports a safe, sound, and competitive banking and payments system. The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the U.S. *See* The Clearing House's web page at: www.theclearinghouse.org.

[2] "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," 86 FR 38182 (July 19, 2021).

expectations relating to third-party relationships generally, The Clearing House's comments are confined specifically to how the proposal would apply to relationships between financial institutions (FIs) and data aggregators and their fourth party clients and how the agencies can work to improve the ability of FIs, and particularly small FIs, to conduct such relationships in a safe, sound, and secure manner.

The Clearing House supports the development of uniform guidance relating to managing the risks inherent in third-party data aggregation relationships. However, as is more fully explained below, The Clearing House believes more should be done by the agencies in coordination with other federal regulatory agencies, such as the Consumer Financial Protection Bureau ("CFPB") and the Federal Trade Commission ("FTC"), to create a unified framework for third-party risk management and data access related to data aggregation activities.

Since 2017, The Clearing House and its members, through The Clearing House's Connected Banking initiative, have been focused on creating an environment that facilitates the transition of data aggregation activities for all FIs, regardless of size, away from higher risk credential-based data access and screen scraping, to a safer, sounder, more transparent, and more consumer controlled application programming interface ("API") environment.[3] The Connected Banking initiative is powered by the combined expertise of the world's most sophisticated banks.[4] While, consistent with the expectations outlined in the agencies' Proposal, much progress in facilitating an API environment to allow data sharing in a safe and secure manner has been made, unique challenges continue to be posed by data aggregation activities that require additional work beyond the Proposal. Specifically, The Clearing House makes the following recommendations:

1. The Clearing House supports the development of uniform guidance, including uniform application of the FAQs;
2. The interplay between the Proposal and the anticipated rulemaking by the CFPB under Dodd Frank § 1033 requires coordination between the FDIC, FRB, OCC and CFPB in order to create a unified framework;
3. The agencies should affirm that FIs have the right to conduct appropriate due diligence and impose reasonable restrictions on time, place, manner, and scope of data access by third parties as well as periodic customer re-authorizations / re-authentications;
    a. Regardless of such affirmation, there will remain important limitations on what FIs can do to protect themselves and their customers from harm when it comes to third party data aggregation activities and the activities of their fourth party clients;

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

[4] The Clearing House is owned by the world's largest commercial banks. Information about The Clearing House's owner banks is available at: www.theclearinghouse.org/about/owner-banks.

   b. FI due diligence and attempts to impose reasonable restrictions are not and cannot be a meaningful substitute for the direct regulation and supervision of data aggregators and downstream parties;
4. The agencies should work with the Federal Trade Commission (FTC) to clarify application of the Gramm Leach Bliley Act to data aggregators, to strengthen the FTC's safeguards rule, and should work with the CFPB to ensure that there is a regulatory and supervisory framework in place that imposes standards and supervision on data aggregators that is commensurate with the standards imposed on FIs when FIs are handling similar customer information.
5. The agencies should end credential-based access and screen scraping in light of the inherent risks associated with such activities.
6. The agencies should continue to monitor, support, and facilitate the benefits of cross-industry and trade initiatives that promote safe and secure access through common interoperable standards, industry-wide utilities, and shared assessment activities.

I. Background

A. The Clearing House's Connected Banking Initiative

TCH's Connected Banking initiative seeks to enable "innovation and customer control through a more secure exchange of financial data."[5] 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 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, 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 fraudster. Indeed, it is interesting to note that some data aggregator and data user agreements reviewed by TCH *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

[5] *See* information regarding TCH's Connected Banking initiative, *supra* note 3.

practice apparently being viewed by those data aggregators and data users as a significant risk to their own data security and integrity. [6]

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 of creating operational challenges for FI data holders.

APIs offer significant advantages to credential-based data access and screen scraping.

> 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

[6] *See, for example,* Plaid, "End User Privacy Policy," at "Registration" (Feb. 22, 2021) (available at: https://plaid.com/legal/) (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 or allow any other application or service to act as you"); *and* Robinhood Financial LLC & Robinhood Securities, LLC, "Customer Agreement," at "K. Electronic Access" (June 2020) (available at: https://cdn.robinhood.com/assets/robinhood/legal/Customer%20Agreement.pdf) (prohibiting Robinhood users from sharing their usernames, account numbers, and passwords with any third parties).

aggregator's access to certain account information or account services, such as making electronic fund transfers.[7]

To facilitate the shift from credential-based access and screen scraping to APIs, TCH is actively engaged in the development of new technology standards, infrastructure, and innovative solutions to address risk management requirements, a model legal agreement, and ongoing industry collaboration.[8] The initiative is guided by the goal of acting "in the best interest of consumers [to] enhance safety and foster efficiency in financial services."[9]

TCH's Connected Banking initiative has resulted in a number of important deliverables:

- 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 accelerating the ability of data holders, data aggregators and data users to establish safe and secure direct connections through APIs. Recognizing that legal agreements between data holders and authorized entities can take considerable time and resources to develop, TCH, in collaboration with its member banks and in consultation with data aggregators and data users, developed a publicly-available Model Agreement that can be used as a reference to facilitate the development of API-related data sharing agreements.
- API Technical & Security Standards: TCH and many of its member banks are founding members of the Financial Data Exchange (FDX), an organization through which cross-industry participants can develop, maintain, and facilitate the adoption of common API standards for sharing consumer financial data.[10] 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 and enhances the security and reliability of the flow of user-permissioned data between data holders, data aggregators, and data users.

---

[7] CFPB, "Taskforce on Federal Consumer Financial Law Report[,] Vol. 1," p. 496 (Jan. 2021) (available at: https://files.consumerfinance.gov/f/documents/cfpb_taskforce-federal-consumer-financial-law_report-volume-1_2021-01.pdf).

[8] *Id.*

[9] *Id.*

[10] Additional information on TCH'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).

- 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. Historically each FI has performed one-off due diligence inquiries. In order to create efficiencies and encourage the development of API relationships, TCH developed a uniform assessment instrument. The instrument has been implemented in the market today and effectively streamlines due diligence. The instrument allows due diligence information to be collected once by assessment vendors and then shared by assessment vendors with multiple FIs through their secure portal, thereby alleviating largely redundant processes across the financial ecosystem. The uniform assessment instrument is particularly useful in creating efficiencies for small FIs that may not be able to match the resources larger FIs dedicate to risk management due diligence.
- Central Utility Option: TCH 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. 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. The efficiencies provided by Akoya may be particularly beneficial to small FIs that may not have the resources or skill to develop their own APIs.
- Consumer Research: TCH'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 they 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

- 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.[11]

B. The Proposal

The FRB, FDIC, and OCC have each issued guidance for their respective supervised organizations addressing third-party relationships and appropriate risk management practices. The FRB issued guidance in 2013,[12] the FDIC in 2008,[13] and the OCC in 2013, supplemented by FAQs issued by the OCC in 2020.[14] The Proposal is based on the OCC's guidance, with the possible inclusion of the FAQs, and would substitute the Proposal for each agencies' separately issued guidance – creating uniform guidance for the management of third-party risks across the FI ecosystem, a goal that The Clearing House strongly supports.

---

[11] *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). The issue of consumer confusion and need for regulation is further illustrated by allegations in the recent class action against Plaid, Inc. (*See Cottle, et al. v. Plaid, Inc.*, No. 20-cv-03056 (N.D. Cal. Apr. 30, 2021).) Plaintiffs alleged in that litigation that "Plaid embeds its software into fintech apps, and that when users seek to link their financial accounts to the apps, Plaid's software presents them with login screens that look like those used by their individual financial institutions. However, Plaid does not disclose to users that they are interfacing with Plaid rather than the banks. Once deceived, users provide their login information which is transmitted directly to Plaid, and Plaid uses the information to access their bank accounts." (*Cottle, et al. v. Plaid, Inc.*, Order on Defendant's Motion to Dismiss the Consolidated Amended Class Action Complaint, p. 17 (N.D. Cal. Apr. 30, 2021) (quoting the consolidated amended class action complaint).) The plaintiffs further alleged that "Plaid makes no effort to meaningfully disclose how it operates and deemphasizes the link to its privacy policy, which Plaintiffs allege is itself substantively inadequate. Finally, Plaid uses the login information to obtain all available data about the users from their financial institutions, regardless of whether it relates to the fintech apps' money-transfer purposes. This includes information that shows users 'healthcare, educational, social, transportation, childcare, political, saving, budgeting, dining, entertainment, and other habits" along with corresponding geolocations. Plaid then sells this personal data to third parties." *Id.*

[12] Federal Reserve, "SR 13-19 / CA 13-21: Guidance on Managing Outsourcing Risk" Letter (Dec. 5, 2013, updated Feb. 26, 2021) (available at: https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm).

[13] FDIC, "Financial Institution Letter FIL-44-2008[,] Guidance for Managing Third-Party Risk" (June 6, 2008) (available at: https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.pdf).

[14] OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" (Oct. 30, 2013) (available at: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html); and OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" (Mar. 5, 2020) (available at: https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html). The OCC also issued foreign-based third-party guidance, OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance" (May 15, 2002) (available at: https://www.occ.gov/news-issuances/bulletins/2002/bulletin-2002-16.html) which supplements this proposed guidance.

The FAQs serve to clarify application of the guidance to various circumstances, including data aggregator relationships. Specifically, FAQ #4 clarifies that data aggregator relationships are third-party relationships within the meaning of the guidance, regardless of whether the data aggregator is acting on behalf of the bank or the bank's customer and notes that banks have a responsibility to manage these relationships "in a safe and sound manner with consumer protections." [15] The OCC goes on to note the risks inherent in such relationships, stating that "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."[16] Integral to the risk management process is the performance of due diligence – "to evaluate the business experience and reputation of the data aggregator and to gain assurance that the data aggregator maintains controls to safeguard sensitive customer data."[17] The FAQ goes on to note that when banks enter into agreements with data aggregators for access to sensitive customer data through an API, such relationships are clearly "business arrangements" and are covered by the guidance, regardless of whether or not the data aggregator is providing a service to the bank or merely acting on behalf of the bank's customer.[18]

The FAQ also discusses screen scraping, noting that although the bank may not have a business or contractual relationship with the screen scraper the bank still has an obligation to "engage in appropriate risk management for this activity" given that screen scraping can pose operational and reputational risks to the bank.[19] Specifically, banks' information security monitoring systems should "identify large-scale screen scraping activities" and, once identified, banks should "conduct appropriate due diligence to gain reasonable assurance of controls for managing this process."[20]

II. Discussion

A. The Clearing House Strongly Supports the Development of Uniform Guidance, including uniform application of the FAQs

The Clearing House strongly supports the agencies' goal of developing uniform guidance as it applies to third-party risk management and believes that such uniformity should include uniform

---

[15] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 14, at Frequently Asked Question #4.
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*

incorporation of the FAQs.[21] Without the incorporation of the FAQs, FIs that are not currently subject to the OCC's guidance may be left to wonder whether the Proposal applies to data aggregator relationships. Uniformity is needed in this area for several reasons.

First, consumer protection should not be dependent on the particular charter of a given institution. Third-party risk management practices are not only essential to protecting the safety and soundness of the institution itself, but are also, given the myriad of risks that can arise from third-parties, essential to protecting an institution's customers as well.[22] Consumers expect and should receive uniform levels of consumer protection across the FI ecosystem.

Second, a uniform approach is needed particularly as it relates to data aggregation, and, therefore, incorporation of the FAQs, which are the only part of the proposed guidance that specifically interprets and applies the proposed guidance as it relates to data aggregation issues, is also essential. The industry, including The Clearing House and its owner banks, have been actively establishing industry utilities and processes to facilitate the movement from credential-based data access and screen scraping to safer and more secure API access. Utilities such as Akoya and tools such as the shared assessment tool are needed to facilitate that movement. These developments, however, can only operate successfully and scale if there is a uniform set of expectations in terms of prudential regulatory guidance that applies to the ecosystem. The shared assessment tool, for example, has been calibrated to meet the expectations set forth in the OCC's guidance on which the proposal is based, including the FAQs. If different prudential agencies adopt different third-party risk management expectations, or different interpretations of the same guidance by, for example, not adopting the FAQs, inefficiencies will be created that will hamper the operation and scale of industry utilities and tools that are needed to bring about positive change in the industry.

Third, the lack of a uniform approach would create potential reputational risk for FIs. Some bank customers and even some consumer groups often fail to understand the risk inherent in data access

---

[21] The Clearing House notes that while the agencies "seek public comment on the extent to which the concepts discussed in the OCC's 2020 FAQs should be incorporated into the final version of the guidance," the FFIEC's recently-issued guidance titled "Authentication and Access to Financial Institution Services and Systems" (issued Aug. 11, 2021; and available at: https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf) already makes reference to the FAQs. Specifically, the guidance notes that a comprehensive risk management program will include "an assessment of risks and effective mitigating controls for credential and API-based authentication when CPEs [customer permissioned entities] access a financial institution's information systems and customer information." (At p. 9 of the guidance.) The guidance goes on to cite the OCC's FAQs for a discussion of "different types of business arrangements associated with CPEs." (At p. 9, footnote 22.)

[22] As the agencies note in the proposal, a key element of third-party risk management is ensuring that "the third-party has identified, and articulated a process to mitigate, areas of potential consumer harm, particularly in which the third-party will have direct contact with the bank's customers, develop customer-facing documents, or provide new, complex, or unique products." 86 FR at 38189

activities – both for the bank and for consumers themselves.[23] Such individuals and entities, oblivious to bank obligations required under relevant third-party risk management guidance, often accuse banks of acting with dubious motives in spite of the legitimate concerns outlined by the agencies in the Proposal. Uniform guidance is needed to create uniform expectations and approaches throughout the ecosystem such that all FIs will abide by the same rules.

Finally, small FIs are unlikely to have the bargaining power of larger FIs and will be dependent on the guidance and the expectations set forth therein to level set with data aggregators on the reasonable steps that FIs can and should be taking to protect their data, systems and customers. Without the full force of the guidance to back them up, small FIs may not have the bargaining power to require the due diligence and impose the reasonable protections that the Proposal envisions. In short, a failure to adopt the Proposal, including the FAQs, may place small FIs at a distinct disadvantage in their negotiations with data aggregators.

B. The interplay between the Proposal and the anticipated rulemaking by the CFPB under Dodd Frank § 1033 requires coordination between the FDIC, FRB, OCC and CFPB in order to create a unified framework

The Proposal is intended to create consistent third-party risk management guidance to assist FIs in managing third-party relationships, including addressing "consumer protection, information security, and other operational risks."[24] Data aggregator relationships are amongst those third-party relationships that are covered by the Proposal, which appropriately emphasizes both the need to protect the FI and the FIs' customers given the risks that are inherent in these kinds of relationships.[25]

At the same time that the agencies are moving to adopt a consistent third-party risk management framework that would apply to data aggregator relationships, the CFPB is engaged in a potential rulemaking to implement Section 1033 of the Dodd-Frank Act on data access.[26] Section 1033(a) provides that, subject to rules prescribed by the CFPB, a covered person shall make available to a consumer, upon request, information in the

---

[23] *See* "Consumer Survey: Financial Apps and Data Privacy," *supra* note 5, at pp. 2 & 5 (noting that consumers' understanding of how non-bank financial applications access information and the risks they pose is limited). *See also* Letter from U.S. PIRG and fourteen other organizations, many of which refer to themselves as "consumer groups," to CFPB Acting Director David Uejio (Aug. 11, 2021) (available at: http://www.economicliberties.us/wp-content/uploads/2021/08/CFPB-letter-8.11.21_Final.docx) (accusing financial institutions of creating "obstacles to prevent consumers from easily accessing their financial data in order to maintain control of consumers' data for their own ends" and claiming that self-serving data-related behavior" is illustrated by The Clearing House pushing the CFPB to give large banks equal rights to consumers in determining the trustworthiness of third-party vendors").

[24] 86 FR 38184

[25] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 14, at Frequently Asked Question #4.

[26] "Consumer Access to Financial Records," 85 FR 71003 (Nov. 6, 2020).

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 to the account including costs, charges and usage data.[27]

The standards and requirements set forth by the agencies in the Proposal, which emphasize FI responsibility for safety, soundness, and consumer protection, and the standards and requirements to be set forth by the CFPB, which will undoubtedly emphasize data access, risk being inconsistent. Absent coordination by the agencies with the CFPB to create a unified framework for third-party risk management and data access as it relates to data aggregation activities, FIs may well be caught between two competing sets of regulatory expectations.

This is due in no small part because the tools that banks have to address safety, soundness and consumer protection issues with data aggregators are at best blunt tools. First, all but perhaps the biggest banks with the richest troves of data lack the degree of negotiating power that would be needed to impose the kinds of safety, soundness and consumer protection requirements that the Proposal outlines. The status quo – credential-based data access and screen scraping - is always a potential fall-back for any data aggregator that doesn't want to adhere to the kinds of structure and requirements that sound third-party risk management practices may impose. FI control is even more attenuated when it comes to data aggregator clients, or "fourth parties" who could be considered "subcontractors" under the Proposal.[28] There may be thousands of fourth party data recipients that receive data from a particular data aggregator. The identities of these fourth parties are seldom disclosed to FIs and, even if disclosed, the ability of FIs to do third-party risk management due diligence on all of them is a practical impossibility.

Second, FIs whose systems are being targeted with credential-based data access and screen scraping from data aggregators that do not or will not comply with reasonable risk-management controls and requirements will likely face a Cornelian dilemma of either continuing to allow the data aggregator to have access to the bank's systems or cutting off the data aggregator's access until such controls can be put in place. In the first instance, the bank may risk exceeding its own risk tolerance, running afoul of regulatory expectations and having its business, systems and customers harmed. In the second instance, the bank risks upsetting its own customers who may not understand the bank's actions as motivated

[27] 85 FR 71004.
[28] 85 FR 71005 - 71006.

by the banks' desire to ensure their protection and the bank may suffer reputational harm as a result.[29]

Finally, while a FI may attempt to block a non-compliant data aggregator by blocking a data aggregator's IP address, that action provides only a temporary solution. Nothing prevents the data aggregator from obtaining a new IP address from which the data aggregator can then seek renewed access to the FI's systems. FIs also face the practical reality that technology is always evolving and regardless of actions taken by an FI to block a non-compliant data aggregator, data aggregators and fintechs will always have a vested interest in obtaining the data, which is the lifeblood of their business.

As is more fully set forth in Section II(E), to be able to ensure that data access is occurring in a safe and sound manner consistent with the Proposal, FIs must have the ability to prohibit credential-based access and screen scraping once an FI is providing data access through an API on fair and reasonable terms and the agencies should affirm that ability in the guidance. Further, to ensure that the industry as a whole transitions to APIs and that risks to the ecosystem are being appropriately managed, the agencies should consider establishing a definitive end to credential-based access and screen scraping, which could be phased in based on the size of the institution.[30]

---

[29] Data aggregators have been quick to portray such bank actions as anticompetitive and motivated by considerations other than sound third-party risk management. For example, JPMorgan Chase (JPMC) is working towards imposing stricter security standards that will result in JPMC's customers' passwords getting "out of the system," by requiring secure tokens to be used by third parties such as aggregators, resulting in a safer and more secure data sharing environment. Actions like the one being taken by JPMC, however, have sometimes been portrayed as controlling and threatening by technology company executives and Silicon Valley. (*See* Laura Noonan, "JPMorgan to ban fintech apps from using customer passwords," Financial Times (Jan. 2, 2020) (available at: https://www.ft.com/content/93dcfc52-210b-11ea-b8a1-584213ee7b2b) (noting that JPMC is moving to implement more robust security standards, and quoting Bill Wallace, JPMC's head of digital, about the importance of removing customer passwords from systems); *and* Jennifer Surane, "Big Banks' Clampdown on Data Puts Silicon Valley Apps on Alert," Bloomberg (March 26, 2019) (available at: https://www.bloomberg.com/news/articles/2019-03-26/jpmorgan-s-clampdown-on-data-puts-silicon-valley-apps-on-alert) (noting that a number of Silicon Valley ventures say they've been threatened by banks' implementation of security measures).

[30] The agencies have successfully set target dates to meet regulatory expectations in other areas, successfully transitioning the industry away from practices that did not meet regulatory expectations. For example, the Federal Reserve, FDIC, and OCC jointly issued a statement on banks' transition away from USD LIBOR that, as part of an orderly, safe, and sound transition away from use of the rate due to regulatory concerns, encourages banks to cease entering into new contracts that use USD LIBOR as a reference rate as soon as practicable, but, in any event, to cease entering into such contracts by December 31, 2021. (*See* Federal Reserve, FDIC, OCC, "Statement on LIBOR Transition" (Nov. 30, 2020) (available at: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201130a1.pdf).)

A unified framework is needed that not only provides for data access, but empowers FIs to establish the kinds of controls and mitigate the kinds of risks covered by the agencies' Proposal. This must include ultimately addressing the risks associated with credential-based access and screenscraping by ending such practices once an FI has made API access available on fair and reasonable terms. The development of a unified framework can only be achieved through strong coordination among the agencies and the CFPB.

C. The agencies should clearly and directly affirm that FIs have the right to conduct appropriate due diligence, impose reasonable restrictions on time, place, manner, and scope of data access by third parties, and require the periodic re-authorization of data access

The Proposal, in FAQ #4, speaks only in the broadest terms about risk management obligations as they relate to data aggregators. The Proposal notes that banks have "a responsibility… to manage these relationships in a safe and sound manner with consumer protections."[31] The Proposal further notes that a "key focus" should be on "[i]nformation security and the safeguarding of sensitive customer data."[32] Finally, even where there is no business arrangement between the bank and an aggregator, i.e., where a data aggregator is gaining access to data through screen scraping, the Proposal anticipates that FIs should "gain assurance that the data aggregator maintains controls to safeguard sensitive customer data."[33] While these statements are helpful in terms of illuminating supervisory expectations relating to the management of third-party risk relating to data aggregators, more specificity is needed.

While the Proposal sets forth high-level expectations that FIs *will* manage the risks relating to data aggregators, the Proposal stops short of actually empowering FIs to take *specific action to do so*. As the Proposal notes, "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."[34] Clearly, FIs have legitimate interests in protecting themselves and their customers from data aggregation related risk. To empower FIs to actually do so, however, the agencies need to go further in the Proposal and affirm that FIs have the right to impose reasonable time, place, manner, and scope restrictions. Time, place, manner, and scope restrictions should include any circumstances in which the FI has a good faith belief that access may be fraudulent, may present security risks to the consumer, the

[31] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 14, at Frequently Asked Question #4.
[32] *Id.*
[33] *Id.*
[34] *Id.*

FI or the financial system generally, may relate to misuse of the consumer's data, or may relate to data beyond that which is reasonably related to the product or service being provided to the consumer or as reasonably needed to protect the security, efficiency, and operational integrity of the FI data holder's own systems.[35] It is only with such affirmation that FIs will be able to transition the market away from the risks inherent in credential-based data access and screen scraping, and to a safer, more secure, customer controlled API environment that is consistent with the expectations set forth by the agencies in the proposal.

In addition, the agencies should also empower FIs to impose periodic re-authorization requirements to ensure that an FI's customers continue to want to provide data to the third-party. There is no regulatory or supervisory construct for data aggregators that imposes reasonable authorization requirements. This means that an authorization, once obtained, may potentially be used indefinitely. Further, consumers often believe that by deleting the app for which the original authorization was obtained, they will have accomplished revoking the authorization.[36] Unfortunately, this is not true.[37] Consumer data may, therefore, be needlessly exposed even when a consumer believes they have effectively revoked authorization. This creates unnecessary risks in the ecosystem that can be managed through simple and regular re-authorization or re-authentication.[38] FIs have a legitimate interest in ensuring that their customers continue to want to supply the data that is being harvested from bank systems and FIs' right to require regular re-authorization should be affirmed by the agencies.

---

[35] Data minimization is an integral component of consumer information security, as it can effectively reduce the unnecessary distribution of sensitive consumer data.

[36] *See* "Consumer Survey: Financial Apps and Data Privacy," *supra* note 5, at p. 6 (noting that a significant number of consumers believe that data is only accessed by non-bank applications until the application is deleted).

[37] *See Id.* at p. 7 (noting that many applications continue to access consumers' financial information indefinitely, even after they have been deleted). *See also* University of Southern California, "The Websites Have Ears: Tracking and Privacy on the Internet," Illumin Magazine (Nov. 27, 2020) (available at: https://illumin.usc.edu/the-websites-have-ears-tracking-and-privacy-on-the-internet/) (noting that "zombie cookies" are able to "regenerate themselves after being deleted and have been used by companies like Google and Facebook [to track individuals]"); Shweta Khare, "Follow the Cookie Crumbs: The Privacy Concerns Behind Data Tracking," NTT Application Security (Jan. 28, 2021) (available at: https://www.whitehatsec.com/blog/follow-the-cookie-crumbs-the-privacy-concerns-behind-data-tracking/) (noting that "[s]upercookies can extract data from [ ] cache files and regular cookies even after being deleted"); *and* Citi, "ePrivacy and Data Protection," Citi GPS: Global Perspectives & Solutions (2017) (available at: https://www.citibank.com/commercialbank/insights/assets/docs/ePrivacyandData.pdf), pp. 21-22 (noting the design and use of zombie cookies).

[38] "Authentication and Access to Financial Institution Services and Systems," *supra* note 21, at pp. 12 & 14 (suggesting customer / user re-authentication after a period of inactivity within a service or system, and privileged user re-authentication prior to making system configuration changes or executing significant system processes, are prudent controls).

D. The agencies should clarify application of GLBA to data aggregators and work with the FTC and CFPB to ensure that there is a regulatory and supervisory framework in place that imposes standards and supervision on data aggregators that is commensurate with the standards imposed on FIs when FIs are handling similar customer information

Empowering the actions noted above will be helpful, but absent a robust regulatory and supervisory framework that imposes meaningful standards and supervision on data aggregators it will still be inadequate. Banks cannot and should not be expected to shoulder the burden of policing an entire industry, particularly where the data aggregator is not a third-party vendor to the bank and the bank's only connection with the data aggregator is a result of the bank working to accommodate its customer's desire for data to be made available. Further, not all FI data holders have the wherewithal to perform such due diligence on data aggregators and, more importantly, no FI, regardless of size, will be able to address security practices at the thousands of fintech data users that comprise data aggregator clients. While FIs may attempt to address security issues in bilateral agreements, such agreements must be individually negotiated and data aggregators have a powerful default position to simply continue credential-based access and screen scraping if the FI attempts to impose requirements that the data aggregator does not wish to incorporate. Agency guidelines should reflect these realities.

The Proposal notes that a "key focus" of an FIs risk management activities relating to data aggregators should be on information security. This issue can and should be more directly addressed by ensuring that data aggregators are subject to a meaningful regulatory framework, including supervision for information security practices.

Federally chartered banks are subject to detailed Federal Financial Institutions Examinations Council (FFIEC) guidance on information security and the interagency rules implementing Gramm Leach Bliley and, more importantly, supervision and enforcement by the Federal financial regulatory authorities. Even state chartered FIs are required to comply with detailed security measures and will be subject to state regulatory supervision and enforcement actions. Those regulatory frameworks are key to protecting consumers and preventing data breaches, transmission errors, unauthorized access and fraud, all of which are fundamental concerns that go to the heart of data sharing activities. Data aggregators and fintech data users that sit underneath them, on the other hand, are, *at most*, subject to the much less stringent FTC safeguards rule and, in most instances, no regulatory supervision and only after the fact enforcement by the FTC.[39] Yet even application of the much weaker standards in the FTC's

[39] *See* FTC, "Standards for Safeguarding Customer Information" (codified at 16 C.F.R. Part 314) (notably, the FTC safeguards rule contains general requirements that are less detailed than the requirements provided under the Gramm-Leach-Bliley Act (differences between the two sets of requirements include standards regarding board and management involvement, employee background checks, vendor oversight, authentication, and incident response programs)). *See also* 81 FR 61632 (Sept. 7, 2016) (requesting public comments on the standards for safeguarding

safeguards rule to data aggregators is in doubt. As the CFPB has noted, "there may be some uncertainty about whether a data aggregator is a 'financial institution' subject to [GLBA] and [the] Privacy and Safeguards Rules."[40] Effective information security protection should *begin* with the agencies working with the FTC to ensure that there is *no room for ambiguity* as to whether GLBA applies to data aggregators and fintech data users. Consumers deserve no less protection.

In addition, the agencies should work with the FTC to ensure that the safeguards rule is strengthened as it applies to data aggregators and their fintech clients. While the disparities between the FTC's safeguards rule and FFIEC standards are legion, a single example may be illustrative. Entities that *are* subject to the FTC's safeguards rule are not even required to have an incident response plan. This means that even if GLBA application to data aggregators and fintech data users is clarified, a data aggregator or fintech that is engaged in the business of handling potentially millions of customers' sensitive, personal financial data is not required under the FTC's safeguards rule to have *any* plan in place to respond to an information security incident, such as a widespread data breach. While the FTC began work in 2016 to modernize the safeguards rule, that work was never completed.[41] An updated standard is needed and the agencies should work with the FTC to ensure that the safeguards rule is modernized so that meaningful consumer protection is provided and standards are imposed that are equivalent to those imposed on FIs when handling similar information.

Regulatory standards alone, however, are not sufficient without meaningful supervision and enforcement.[42] The agencies should work with the CFPB to ensure that the CFPB in the context of its

---

customer information, including comment on whether a response plan should be a required element of an information security program).

[40] "Taskforce on Federal Consumer Financial Law Report[,] Vol. 1," *supra* note 7, pp. 513-514.

[41] In the meantime, data aggregation and fintech users have multiplied exponentially. 54% of U.S. banking consumers use financial apps to engage in personal financial management, investing, borrowing, and person-to-person payments; the aggregation system is thought to reach approximately 95% of U.S. deposit accounts; and one large aggregator in the U.S. estimates that it alone connects to one in four financial accounts in the U.S. (*See* "Consumer Survey: Financial Apps and Data Privacy," *supra* note 11, pp. 2 & 4; Michael Deleon, "A buyer's guide to data aggregation," Tearsheet (Feb. 19, 2019) (available at: https://tearsheet.co/data/a-buyers-guide-for-data-aggregation/); *and* Zack Meredith & Zeya Yang, "The all-new Plaid Link," Plaid Blog (Oct. 2, 2020) (available at: https://plaid.com/blog/the-all-new-plaid-link/).) Additionally, the COVID-19 pandemic appears to be playing a role in accelerating U.S. consumers' adoption of fintech applications, with older generations in particular using fintech applications in increasing numbers. (*See* Krivkovich, White, Townsend & Euart, "How US customers' attitudes to fintech are shifting during the pandemic," McKinsey & Company (2020) (available at: https://www.mckinsey.com/industries/financial-services/our-insights/how-us-customers-attitudes-to-fintech-are-shifting-during-the-pandemic).)

[42] The FTC, for example, has limited supervision and enforcement powers. *See* FTC, "A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority," FTC memorandum (May 2021) (available at: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority). *See also* "Prepared Statement of the Federal Trade Commission: Strengthening the Federal Trade Commission's Authority to Protect Consumers" (Apr. 20, 2021) (available at:

rulemaking on Section 1033 incorporates a meaningful supervisory framework.[43] The security of consumer data has been the subject of considerable concern by Congress and others, which have focused on the perceived misuse of consumer data by numerous fintech companies.[44] Similarly, the Facebook/Cambridge Analytica scandal shows that even with appropriate contractual limitations in place, absent robust third-party risk management processes and appropriate supervision and enforcement the security of data cannot be assured.[45] In the context of data sharing under Section 1033, the data at issue, dealing with a consumer's financial information and often including PII, is even more sensitive than generalized consumer data and its distribution and use should be subject to heightened concern.

---

https://www.ftc.gov/system/files/documents/public_statements/1589164/prepared_statement_of_the_ftc_before_the_senate_committee_on_commerce_science_and_transportation.pdf); *and* "Prepared Statement of the Federal Trade Commission: The Urgent Need to Fix Section 13(b) of the FTC Act" (Apr. 27, 2021) (available at: https://www.ftc.gov/system/files/documents/public_statements/1589400/p180500house13btestimony04272021.pdf) (noting that the FTC lacks authority and requesting that Congress act to clarify Section 13(b) of the FTC Act so as to preserve / strengthen the FTC's ability to enjoin illegal conduct). As we have seen from the 2017 Equifax data breach that exposed the personal information of 147 million people, the extensive risks to consumers who are victims of a data breach cannot be effectively remedied by an after-the-fact civil money penalty. Proactive examination and, where necessary, remedial action are the most effective tools to help prevent consumer harm from occurring in the first place.

[43] The CFPB could also use its rulemaking power to impose meaningful information security standards on data aggregators and their fintech clients in the absence of FTC action on the safeguards rule. *See* CFPB, "Rules and policy" (available at: https://www.consumerfinance.gov/rules-policy/) (noting that the CFPB generally has authority to make rules governing consumer finance markets and that it can "create new rules when warranted"). *See also* Adam J. Levitan, "The Consumer Financial Protection Bureau: An Introduction," Review of Banking & Financial Law, Vol. 32, pp. 344-347 (2012-2013) (available at: https://www.bu.edu/rbfl/files/2013/10/Levitin.pdf) (noting ways that the CFPB's rulemaking authority reaches "covered persons" and "service providers").

[44] *See, for example*, NPR, "Amazon, Tik Tok, Facebook, Others Ordered to Explain What they Do With User Data (Dec. 15, 2020) (available at: https://www.npr.org/2020/12/15/946583479/amazon-tiktok-facebook-others-ordered-to-explain-what-they-do-with-user-data); Lauren Feiner, "Big Tech Testifies: Bezos Promises Action if Investigation Reveals Misuse of Seller Data, Zuckerberg Defends Instagram Acquisition," CNBC (Dept. 8, 2020) (available at: https://www.cnbc.com/2020/07/29/tech-ceo-antitrust-hearing-live-updates.html (accessed Jan. 7, 2021); Elizabeth Dwoskin, "Facebook is Accused of Digital 'Surveillance' Against Its Competitors," The Washington Post (July 29, 2020); *and* Michael Grothaus, "How Our Data Got Hacked, Scandalized, and Abused in 2018," Fast Company (Dec. 13, 2018) (available at: https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018).

[45] *See* Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times (April 4, 2018) (available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html); *and* Paolo Zialcita, "Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal," NPR (Oct. 30, 2019) (available at: https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal).

To more fully ensure the protection of consumers and the FI ecosystem, the agencies should work with the CFPB to ensure that there is a regulatory and supervisory framework in place that imposes standards and supervision on data aggregators that is commensurate with standards imposed on FIs when FIs are handling similar customer information. Given data aggregator and data user access to similarly sensitive information, data aggregators that are the recipients of such information should be subject to CFPB regulation and supervision that includes functionally similar requirements as those imposed on FIs, including supervision and enforcement that the CFPB should provide through a larger participant rule or otherwise.[46] In order to ensure a fully secure ecosystem, such requirements should follow the data with data aggregators being responsible for passing on and enforcing security requirements to data users.

E. The agencies should end credential-based access and screen-scraping in light of the inherent risks associated with such activities

While industry consortia continue to make progress on initiatives that provide significant consumer protection advantages over credential-based access and screen scraping, data aggregators have been reluctant to abandon credential-based access. Credential-based access and screen scraping can offer data aggregators and data users maximum access to all of a consumer's data held at an FI, meaning they have little incentive to transition to APIs and other methods of access that are both more secure and better enable informed customer consent and data minimization. Sharing access credentials poses significant risk to consumers' financial health, and puts the consumer at risk of account take-over, unauthorized payment transactions, and identity theft. In 2019, FinCEN Director Kenneth A. Blanco stated that his agency had "seen a high amount of fraud, including automated clearing house (ACH) fraud, credit card fraud, and wire fraud, enabled through the use of synthetic identities and through account takeovers via fintech platforms." [47] These concerns are echoed by the agencies in the proposal.[48]

In light of the clear consumer risks and risks to FIs involved with credential-based access and screen scraping and the disincentives of data aggregators and data users to move away from

---

[46] Such supervision would necessarily include supervision over the data aggregators' third party risk management program pursuant to which the data aggregator would be responsible for evaluating and managing risks associated with its data user customer's use of consumer data.

[47] Prepared remarks of FinCEN Director Kenneth A. Blanco to the Federal Identity Forum and Exposition (Sep. 24, 2019) (available at: https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid).

[48] "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," *supra* note 14, at Frequently Asked Question #4 ("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").

credential-based access, the agencies should take affirmative steps to end credential-based access as a means to sharing consumer financial data. We recognize that larger depositories may be better positioned to implement API data access sooner, and we believe the agencies should explore a phased mandatory end to credential-based access according to depository institution size, providing smaller institutions a longer period of time to move away from this fundamentally dangerous and consumer-*un*friendly practice.

In addition, the agencies should modify the guidance to clearly and unequivocally allow FIs to block credential based data access and screen scraping once an FI is offering data access through an API on fair and reasonable terms. Agency support in the form of clear guidance is needed so that FIs may be empowered to effectuate the agencies' vision for safe and secure data access that will protect consumers and the financial ecosystem.

F. The agencies should continue to monitor, support and facilitate the benefits of cross-industry and trade initiatives to facilitate safe and secure access through common interoperable standards, industry-wide utilities and shared assessment activities

While the agencies can and should set regulatory and supervisory standards relating to data aggregation activities, there is significant work that must be done by the industry to implement the technical standards and other details that will ultimately effectuate the agencies' vision. Significant progress has been made on developing a framework for data sharing that aligns with the expectations set forth in the Proposal. The work being done by the industry through FDX provides the necessary standard by which Consumers can more safely and securely obtain information from account providers to use for the consumer's benefit without requiring consumers to share their account credentials with third parties. Further, work being done by TCH and Akoya is geared toward accelerating the adoption of the FDX standard and more fully building out the industry infrastructure needed to support it, particularly for small FIs.[49] Fundamentally, TCH believes that the agencies should continue to rely on private sector market-led efforts for technical standard setting and other activities of the kind engaged in by FDX, Akoya and TCH.

It is therefore important that the agencies continue to monitor, support and facilitate the benefits of cross-industry and trade initiatives to facilitate safe and secure access through common interoperable standards. Regulatory frameworks should encourage such initiatives as essential to the

[49] Much of the work being done by TCH and Akoya is geared to addressing issues that will be faced by smaller institutions in implementing API environments. TCH's Assessment Tool created efficiencies relating to due diligence and third party risk management. Akoya created efficiencies relating to connectivity and is also working on the development of a rule set that may substantially alleviate the burdens of bilateral contracting. TCH further recognizes that third party service providers, which provide much of the back office infrastructure for smaller FIs, will also play a critical role in API adoption.

development of data aggregation activities. Specifically, there are a number of actions that the agencies could take that would be helpful to these private sector efforts. First, TCH encourages the agencies to find ways to explicitly endorse or reference technical standards and certification organizations like FDX and the work that they are doing.[50] Second, as more fully set forth herein, there are a number of issues on which the agencies could provide greater regulatory clarity and uniformity, allowing the industry to then work together to develop or further enhance existing standards to implement the agencies' vision. Finally, the agencies should work with other agencies, such as the CFPB and FTC, to ensure that the Federal financial regulators are speaking with one voice on issues affecting the data aggregation market. The development of uniform guidance is essential to the development of industry standards, utilities and other tools that are needed to effectuate the agencies' vision. Without such uniformity, the market will be fractionalized and solutions will not scale. The Proposal, including uniform adoption of the FAQs, is an important step toward creating that uniformity.

III. Conclusion

The Clearing House agrees with the agencies' vision for safe, sound and secure data access outlined in the Proposal and supports the development of uniform guidance relating to managing the risks inherent in third-party data aggregation relationships. Such guidance will assist FIs of all sizes in managing the risks associated with data access, creating a safer financial ecosystem and decreasing risk for consumers. More must be done, however, beyond the guidance itself, to make the agencies' vision a reality. Key coordination must occur between the agencies and the CFPB and FTC to create a holistic, unified regulatory and supervisory framework that appropriately addresses the risks associated with data access activities. Further, FIs, both big and small, must be empowered by the agencies to take the steps needed to truly manage the risks associated with credential-based access and screen scraping, including taking steps to stop such access once an FI offers API access on fair and reasonable terms. Further, while much work is being done by the private sector, and much has been accomplished, to enable safe, sound data access practices, it is unlikely that private sector efforts alone will be able to put an end to credential-based data access and screen scraping. Given the risks inherent in such practices, the agencies should consider a regulatory sunset, perhaps phased in by institution size.

---

[50] Once such example of endorsement of a market-led standard is the Financial Stability Oversight Council's (FSOC) annual report in which FSOC recommended that member agencies support adoption and use of standards in mortgage data, including consistent terms, definitions, and data quality controls. The recommendation pointed to the Mortgage Industry Standards Maintenance Organization (MISMO). (*See* "2020 Annual Report," Financial Stability Oversight Council, pp. 13 (Dec. 4, 2019) (available at: https://home.treasury.gov/system/files/261/FSOC2020AnnualReport.pdf (accessed Jan. 7, 2021)).

The Clearing House appreciates this opportunity to comment on the Proposal, and looks forward to serving as an ongoing resource to the agencies as they continue to address third-party risk issues relating to data access.

Sincerely,

/s/

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