The Clearing House

September 22, 2020

VIA E-MAIL (comments@fdic.gov)
Mr. Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street N.W.
Washington, DC 202429

Re: RIN 3064-ZA18 "Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services"

Ladies and Gentlemen:

The Clearing House Association and The Clearing House Payments Company (collectively, The Clearing House)[1] appreciate the opportunity to respond to the Federal Deposit Insurance Corporation's FDIC) request for information titled, "Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services."[2] The Clearing House commends the FDIC for its outreach to the industry on potential ways to address the sometimes prohibitive costs and strain on resources that can accrue to insured depository institutions as they strive to meet regulatory expectations relating to third-party risk management in deploying third-party technologies. The Clearing House has been engaged, both individually and collaboratively with other organizations, in significant efforts to address this issue as it relates to the sharing of data with customer permissioned third-parties (commonly known as "data aggregators") and their fourth-party clients. It should be noted that although insured depository institutions may not actually be "deploying" the technology in this circumstance, some financial institution regulators have nonetheless taken the position that institutions have obligations to employ some level of third-party due diligence and risk management.[3] The Clearing House writes to ensure that the FDIC is aware of developments in this space as it may inform aspects of the work that the FDIC is considering on standardization and certification. The frameworks that have and are being developed to address third-party risk management in the data aggregation space, including the development of standard setting and certification frameworks, may

[1] The Clearing House Association L.L.C. is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound, and competitive banking system. Its affiliate, The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the United States.

[2] "Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and other Services," 85 F.R. 44890 (July 24, 2020).

[3] *See*, OCC FAQ on *Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29*, ("OCC FAQ on Third-Party Risk") available at https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html

also inform how the industry and regulators might approach the management, assessment and oversight of third-party model deployment from a fintech into the financial institution ecosystem. Specifically:

1. The Clearing House supports the work of voluntary industry organizations that can bring together diverse stakeholders and align around common standards and certification programs. The FDIC should ensure that any further work that the FDIC may undertake relating to the development of standards and certifications fully aligns with work that is already taking place through voluntary industry organizations such as the Financial Data Exchange (FDX).
2. Substantial industry work and investment are already taking place to create efficiencies in addressing third-party risk management expectations as they relate to data aggregation, including the development of an efficient assessment tool and a potential registration portal. The FDIC should ensure that any further work that the FDIC may undertake relating to how third-party risk management issues may be addressed fully aligns with work that is already taking place in the industry.
3. The approach the industry has and is developing to manage the risks associated with data transmission in the data aggregation space should be looked to as an important component in managing third-party risk in model deployment.
4. The FDIC should coordinate with other financial institution regulators in order to avoid the development of a bifurcated approach that could create inefficiencies in the market and inhibit industry solutions from reaching scale.

Since the passage of § 1033 of the Dodd-Frank Act, the relationship between depository financial institutions and permissioned third-party recipients of customer bank data has been the subject of significant interest from the regulatory community.[4] The Clearing House has been actively engaged, both individually and as a member of FDX, in work to assist the ecosystem in developing safer, more transparent and more secure API connectivity that can facilitate data sharing without the bank customer providing data aggregators or their fourth-party fintech clients with bank account internet platform IDs and passwords. Fundamental to achieving a transition to APIs at scale, however, is (a) the development of API standards and a certification relating to the implementation of API standards, and (b) the ability to manage and efficiently scale third-party risk management activities relating to data

---

[4] Activity has included an RFI, a yet to be released ANPR, and the articulation of "Principles for Consumer-Authorized Financial Data Sharing and Aggregation" from the Consumer Financial Protection Bureau and FAQ's on Third-Party Risk Management Guidance as it relates to data aggregation activities. *See*, *Request for Information Regarding Consumer Access to Financial Records,* 81 F.R. 83806 (Nov. 22, 2016); *Principles for Consumer-Authorized Financial Data Sharing and Aggregation*, available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; CFPB announcement regarding to be released ANPR on *Consumer-Authorized Access to Financial Data*, available at: https://www.consumerfinance.gov/about-us/newsroom/cfpb-anpr-consumer-authorized-access-financial-data ; OCC FAQ on Third-Party Risk.

aggregators and their fourth-party fintech clients. Both of these activities are discussed in more detail below.

In addition, many fintechs will build models that require the ongoing transmission of data from a financial institution through either a data aggregator or a direct interface with the financial institution through an API. The approaches the industry has and is developing to manage the risks associated with data transmission in the data aggregation space may therefore be instructive in managing aspects of third-party risk in model deployment.

I. API Standards and Certification

Work on API standards and the development of a certification model as they relate to data aggregation activities has been and continues to be undertaken by the industry through FDX. FDX is an international, nonprofit organization operating in the US and Canada that is dedicated to developing a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data, aptly named the FDX API. FDX is currently comprised of 136 members, including financial data providers (i.e. financial institutions), data recipients (i.e. third-party financial technology companies or fintechs), data access platforms (i.e. data aggregators and ecosystem utilities), consumer groups, financial industry groups and other permissioned parties in the user-permissioned financial data ecosystem. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC). The Clearing House is a founding member of FDX and has representation on the FDX Board of Directors. In addition, many of The Clearing House member banks are also members of FDX.

FDX exists chiefly to promote, enhance and seek broad adoption of the FDX API technical standard (formerly the Durable Data API), which allows for users within the financial data ecosystem to be securely authenticated without the sharing or storing of bank customer login credentials with third or fourth parties. Broad adoption of the FDX API promises to create a more secure and reliable flow of user-permissioned data between banks, aggregators, fintech applications, payments and online lenders. This standard has been under the stewardship of the FS-ISAC and some of the largest financial institutions in the U.S. have implemented this standard in the last several years.

Through FDX, The Clearing House, many of its member banks, data aggregators, fintechs and other stakeholders are already engaged in much of the activity as it relates to data aggregation that is potentially contemplated by the FDIC. Specifically, FDX is fully engaged in standardization across the spectrum of consumer data sharing. This includes:

- Defining Use Cases: Use cases are consumer-permissioned scenarios that help users control the amount of data they share by defining only the data elements that are needed for a given product or service. FDX seeks to approve and certify specific use cases in the future, such as personal financial management (PFM), credit management and servicing, account verification and tax preparation.

- Developing a Certification Program: As stated in the RFI, creating a standard alone cannot promote or guarantee adherence to the standard. A qualification and certification program are needed to ensure common implementation and interoperability of any technical standard. Products (i.e., programs and apps for consumer permissioned financial data sharing) can be approved by a certification program to test technical compatibility/interoperability prior to being marketed as a compliant product. The industry, through FDX, is working on a certification program to certify adherence to FDX standards.

- Develop User Experience and Consent Guidelines Best Practices: An industry group like FDX has the ability to document the steps and show examples of recommended user experiences across the end-to-end data sharing workflow to permit users to establish their financial data sharing connections with ease and full transparency and control. These steps will span across the lifecycle of creating a connection, managing a connection, and revoking a connection, including the steps of disclosure, authentication, and authorization. Important work relating to the development of user experience and consent guidelines and best practices is already underway through FDX.

The Clearing House supports the work of voluntary industry organizations like FDX that can bring together diverse stakeholders and align around common standards and certification programs that adapt to changing needs and innovations in the marketplace. The FDIC should ensure that any further work that the FDIC may undertake relating to the development of standards and certifications fully aligns with work that is already taking place through voluntary industry organizations like FDX. The standard development and certification process framework deployed by the industry through FDX may further serve the industry in developing standards and a certification process framework for model risk management.

II. Third Party Risk Management Activities

Like other financial institution regulators, the FDIC has certain expectations relating to a financial institution's management of its third-party relationships. Specifically, the FDIC notes that it "reviews a financial institution's management of significant third-party relationships in the context of the normal supervisory process" and will examine "the quality and effectiveness of an institution's risk management program as it pertains to the safety and soundness and consumer protection aspects of third-party arrangements."[5] The costs and other resources required to fulfill these expectations can, however, as the FDIC further notes, be "prohibitive" and, particularly for community banks, can "create barriers to entry…by limiting the institutions' ability to effectively and timely on-board third parties."[6]

The OCC and the Federal Reserve Board have also outlined certain expectations regarding financial institution management of third-party relationships.[7] In addition to guidance, the OCC has

---

[5] 85 F.R. 44890, 44890-44891.
[6] *Id.* at 44891
[7] OCC Bulletin 2013-29 (October 30, 2013); FRB Guidance on Managing Outsourcing Risk (December 5, 2013).

issued a specific FAQ outlining its views on third-party risk management as it specifically pertains to data aggregation activities. That FAQ notes that even if a bank "is not receiving a direct service from a data aggregator" and even "if there is no business arrangement" between the bank and the data aggregator, banks still have risk from sharing customer-permissioned data with a data aggregator and bank management should perform due diligence to "gain assurance that the data aggregator maintains controls to safeguard sensitive customer data."[8]

In The Clearing House's experience, even for large national banks, the due diligence process required to effectively on-board a third party, whether there is a business arrangement or not, can take a year or more and require the commitment of substantial resources. The process can be similarly daunting for third-parties, which can be faced with varying third-party risk management requests for each financial institution with whom they establish a relationship.

The Clearing House, through its connected banking initiative, has sought to address and create a solution for this problem in a way that will scale for all financial institutions.[9] First, The Clearing House, working with subject matter experts from across the industry, has developed and piloted a standardized, common third-party risk management assessment tool that is capable of being utilized by any financial institution in fulfilling its third-party risk management obligations relating to data aggregators and their fourth-party clients. When fully implemented, the assessment tool will allow for a single assessment to be conducted with the results of that assessment and supporting documentation being posted on a secure online portal with permissioned access to the universe of financial institutions doing business with that third-party. The assessment tool will provide information that each financial institution can use to make its own risk management decision regarding its relationship or potential relationship with the assessed entity and can be supplemented with additional information at the financial institution's request.

Second, The Clearing House is exploring the potential development of a registration portal, which would provide a central repository for key information relating to data aggregators and their fourth-party fintech clients. The information would include key details regarding the entity's corporate structure, business, and contact information, as well as keep track of standards certifications such as that being proposed by FDX. It would also be used as an initial screening vehicle to determine the level of assessment to which the party would be subject, enabling financial institutions doing business with the data aggregator or fourth-party fintech to obtain ready access to relevant information and eliminating the need of data aggregators and fourth-parties to respond individually to many duplicative requests for similar information. The registration portal would be made available for secure access to financial institutions, data aggregators, and fintechs throughout the ecosystem. In this way, The Clearing House seeks to bring needed efficiencies to the ecosystem that will enable the migration from screen scraping to safer, more secure APIs.

---

[8] OCC FAQ on Third-Party Risk Management, FAQ #4.

[9] The goal of the connected banking initiative is to enable innovation and customer control through a more secure exchange of financial data. More information regarding The Clearing House's connected banking initiative is available at: https://www.theclearinghouse.org/connected-banking.

The assessment tool that has been developed and registration portal that is being developed by The Clearing House could be extended or modified to address certain issues relating to model risk management. The assessment tool could easily be modified to take into consideration, for example, the information sharing practices needed to support operation of the model and other issues related to model development, deployment and integrity. Similarly, the registration portal could also be modified to include key details regarding the third-party fintech provider of the model, including any certifications related to the third-party and therefore provide a central clearing house for important information relating to the management of model risk. In this operating model, the certification or model validation would be performed once by a qualified party, which firms could rely on to meet SR 11-7 guidance. It is critical that there is ex-ante acceptance of this validation practice by all regulators for this approach to gain traction among firms.

Finally, it is important that the regulatory community develop a common approach to third-party risk management as it relates to data aggregation and model risk management activities and that the regulatory community, including the FDIC, take into consideration the activities already being engaged in by the industry in whatever further work the FDIC undertakes on standards and certification. The solutions being developed by The Clearing House and others in the industry will need to scale and, in order to bring efficiencies to the market, it will be important to avoid bifurcation that could be introduced through different regulatory approaches that could be applicable to differently chartered banks. The development of different standards or approaches applicable to different financial institutions may severely impair the efficiency of the solutions being developed by the industry if data aggregators and fintechs as well as model developers end up needing to comply with a myriad of different regulatory approaches imposed on differently chartered financial institutions. This, in turn, in the data aggregation environment, would impair the end goal of creating safer, more transparent, and more secure API connectivity and would also continue to impair the willingness of financial institutions to engage in the deployment of models that promise to bring greater efficiencies to the market.

III. Conclusion

Substantial industry activity is already taking place to address and create efficiencies relating to the substantial investment in time and resources that third-party risk management activities may impose and to leverage standards and certification frameworks. The FDIC should ensure that any further work that the FDIC may undertake relating to the development of standards and certifications and third-party risk management fully aligns with work that is already taking place in the industry. Further, while that work is currently targeted to data aggregation activities, the frameworks that have and are being developed to address third-party risk management in the data aggregation space may inform how the industry might approach the management, assessment and oversight of third-party model deployment from a fintech into the financial institution ecosystem overall. Importantly, regulatory coordination will be key to ensuring that approaches are aligned and that developments that could impede the success of industry work are avoided, including avoiding the development of regulatory bifurcation that could prevent industry solutions from reaching scale. The Clearing House would welcome the opportunity to further brief the FDIC on work that it is undertaking to facilitate the movement of data sharing activities to APIs and to bring efficiencies to the market that are needed to support that transition and how these frameworks may be useful in other circumstances.

Respectfully submitted,

[redacted]

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