PLAID

Chief Counsel's Office
Attn: Comment Processing
Office of the Comptroller
of the Currency
400 7th St. SW, Suite 3E-218
Washington, DC 20219

Ms. Ann E. Misback
Secretary
Board of Governors of the
Federal Reserve System
20th Street and Constitution Ave. NW
Washington, DC 20551

Mr. James P. Sheesley
Assistant Executive Secretary
Attn: Comments-RIN 3064-ZA24
Federal Deposit Insurance Corporation
550 17th St. NW
Washington, DC 20429

October 18, 2021

Response to Request for Comment on Proposed Interagency Guidance on Third-Party Relationships: Risk Management

(OCC: Docket ID OCC-2021-0011; Federal Reserve System: Docket No. OP-1752; FDIC: RIN 3064-ZA026)

Plaid appreciates the opportunity to respond to The Board of Governors of the Federal Reserve System ("the Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of the Comptroller of the Currency's ("OCC") proposed interagency guidance and request for comment regarding managing risks associated with third-party relationships.[1]

Our comments are intended to highlight areas of alignment with the proposed guidance, and to respond to specific areas where the proposed guidance may provide more clarity in a complex ecosystem that consists of financial institutions ("bank"), data aggregators, financial technology companies ("fintech"), and consumers. Specifically, Plaid believes that increased recognition of the unique relationship between financial institutions and data aggregators, and the separate relationship between data aggregators and their clients, will lead to improved third party management coordination and understanding.

About Plaid:

Plaid is a financial technology company that enables consumers to access and share their financial data in order to power technological applications they use to improve their financial lives. Plaid has built data sharing integrations with over 11,000 financial institutions and 5,500 fintech companies,

[1] Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38182 (July 19, 2021).

helping millions of consumers and small businesses access and share their data and reap the benefits of new and innovative digital financial tools. We offer services to both financial technology companies and financial institutions, and also provide consumer-facing applications to help consumers manage access to their financial data.

At Plaid, our mission is to unlock financial freedom for everyone. When consumers can easily and securely share their financial data in order to power data-driven products and services provided by fintechs and financial institutions, they benefit from the myriad innovative tools now available to help them manage their financial freedom.

Given our core business of supplying services to over 5,500 fintechs through our connectivity to financial institutions, we appreciate the opportunity to provide our perspective on clarifying opportunities for third party relationship management.

While we appreciate the purpose and intent of the proposed guidance to manage a variety of third-party risks, Plaid strongly believes there is a clear opportunity to refine the interagency guidance on the use of consumer permissioned data to better reflect the existing, four-way relationship between consumers, financial institutions, data aggregators, and fintech companies. We believe this can be achieved in a way that both supports financial institutions' third-party risk management requirements and clarifies regulatory expectations for these relationships, thus allowing consistency in the marketplace.[2]

The discussion of "business arrangement" should be clarified to establish that direct relationships between financial institutions and aggregators are unique and distinct from other "business arrangements," and should have oversight requirements specific to that relationship. (Question 4).

Plaid recognizes that the proposed guidance purposely leaves the term "business arrangement" vague in order to provide financial institutions leeway in monitoring external parties. However, this vagueness creates regulatory uncertainty to all involved stakeholders and risks stifling innovation. Moreover, the number of ways in which the term "business arrangement" can be interpreted imposes inconsistencies among financial institutions as to how best assess whether such an arrangement exists. This lack of clarity around whether the data provider-data aggregator relationship constitutes a "business arrangement" extends to data aggregator-client relationships, as discussed in more detail in the following question. As a result, financial institutions impose on themselves an obligation to conduct a significant amount of oversight on parties with whom they do not directly engage, often limiting consumer choice as a result.

There are instances in which a data provider-data aggregator pairing has a clear business arrangement, such as when an aggregator is providing aggregation services to a bank. However, when a data aggregator is merely providing consumer-permissioned information to a data recipient,

[2] See OCC Bulletin 2013-29, FAQ 4.

there is no business arrangement between the aggregator and the bank, regardless of the method of data access. Instead, there is a diminished level of relationship, in which the aggregator does have a direct interaction with the bank and may have signed a data agreement to facilitate this access, but is not offering material services to that bank. Consumer harm resulting from the activities of an aggregator or its clients are subject to the jurisdiction of the Consumer Financial Protection's Bureau (the "Bureau") jurisdiction and would be addressed through its existing authorities.

As such, any final guidance should clarify that bank-aggregator relationships do not constitute a "business arrangement" and should be subject to an appropriately focused and distinct set of diligence expectations for banks and supervised by the agencies overseeing this guidance. Additionally, the Bureau should use its authority to supervise data aggregators, which would establish more appropriate diligence requirements for consumer-permissioned access and provide clear instruction to banks that aggregators in good standing with their supervisory body are meeting necessary access requirements.[3]

The OCC's 2020 FAQs should clarify that a bank's diligence obligations resulting from a data access agreement are distinct from diligence obligations for business arrangements where the third party is providing a service to the bank, and that those obligations should be appropriately tailored to the unique relationship between fintechs and aggregators. (Question 18)

Plaid welcomes the opportunity to provide its perspective on the OCC's 2020 FAQs, specifically FAQ #4, as proposed for inclusion into the interagency guidance. As the agencies are aware, aggregators have two primary methods for accessing consumer-permissioned data: by Application Programming Interface (API) or by screen scraping. In order to access data via API, aggregators and financial institutions enter bilateral agreements, negotiated on a bank-by-bank basis.

The FAQs refer to these bilateral agreements--entered into between data aggregators and banks--as a business arrangement. According to FAQ #4, diligence between a bank and an aggregator depends on the "level of formality of any arrangements" for sharing consumer-permissioned data, potentially creating the perception of more due diligence requirements than a screen scraping-based relationship. This can create a disincentive for banks to enter into bilateral agreements that in certain circumstances would benefit the bank and its customers.

While the financial industry actively works towards adoption of APIs through industry-led bodies like the Financial Data Exchange (FDX), it is clear that API adoption is a costly process, particularly for smaller institutions. To help offset the resource burden, Plaid launched Plaid Exchange,[4] a low-lift API, to help speed along this transition for these institutions and allow for a secure, reliable method for their customers to connect accounts to apps and services. Since launch, we have enabled core

[3] Section 1024, DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT
[4] https://plaid.com/blog/introducing-plaid-exchange/

providers Jack Henry Banno[5] and Q2[6] to allow banks on their platforms to integrate with our API, in the hopes of bolstering adoption.

A perceived heightened need for due diligence over API-based access and screen scraping access could slow down this shift to API-based access. The OCC should clarify that a bank's diligence obligations resulting from a data access agreement are distinct from diligence obligations for a vendor or other business arrangement where the third party is providing a service to the bank, and that those obligations should be appropriately tailored to the unique relationship between banks and aggregators, as discussed in Question #4. A streamlined and simplified approach to aggregator-bank relationships, regardless of access method, will alleviate many inhibitors to progress on behalf of consumers.

The proposed description of third-party relationships can be made clearer through specification that aggregator customers are not third or fourth parties to financial institutions. (Question 3).

Along with acknowledging that data access facilitation between an aggregator-bank is not a traditional "business arrangement," the guidance should clarify that aggregator customers are excluded from this definition as well. In any final guidance, the description of third-party relationships should be clarified to recognize that consumer-chosen relationships--such as relationships between financial institutions and fintech companies that do not directly integrate with those financial institutions, but instead rely on a data aggregator to establish connectivity for consumers--denote an indirect relationship, not subject to bank risk management activities.

The market is new and distinct from traditional third-party relationships, in which a bank contracts with a vendor to offer a desired service to the bank, to one in which the bank's customers actively choose to share their financial account information with an external party. Such data sharing is not new--consumers historically shared their financial data manually, providing printouts of bank statements to mortgage providers when applying for loans, or voided checks with account and routing numbers to employers in order to enroll in payroll. In the last ten years however, financial data sharing has become increasingly digital, facilitated by data aggregators that share this information at a consumer's request.

In both scenarios, the bank has no direct relationship with the external entity providing the separate financial service to their customer. Rather, they have a shared customer benefitting from an interconnected system. Typically, a data aggregator facilitating the passage of data delivers connectivity to both the data provider, often a bank, and the requesting entity, often a fintech. In these instances, the fintech has a business relationship with the data aggregator and the consumer, but has no relationship with the data provider. Critically, the data recipient's business relationship with the consumer is completely independent of the bank's relationship with the consumer. The consumer, not

[5] https://plaid.com/blog/plaid-exchange-jack-henry/
[6] https://plaid.com/blog/q2-and-plaid-partner-to-bring-open-finance-to-millions/

the bank, selects the fintech they wish to do business with, which in some cases may be a direct competitor with the bank. Treating the data recipient as a third or fourth-party to the bank would both misunderstand the structure of the relationships between banks, aggregators, fintechs, and consumers, and put banks in a position where they would have the power to block their customer from using a competitor's services, including the services of other banks..

The guidance as it stands does not clearly acknowledge this lack of a direct vendor-type relationship between the fintech and the financial institution, resulting in significant regulatory uncertainty as to whether a bank is obligated to conduct oversight management on any fintechs servicing mutual consumers. This has caused significant confusion and inconsistencies in approach within the ecosystem, with many banks being driven to managing aggregator customers as a traditional fourth-party to a vendor, due to a fear of noncompliance with the guidance or based on varied views imposed by the agencies. Without clear guidance in this regard, the resulting interpretation is onerous for both the bank and the fourth-party, given the sheer size of the ecosystem. As previously mentioned, Plaid connects to 11,000 banks and 5,500 fintechs. If carried out to the full extent, this would leave each individual aggregator customer subject to fourth-party due diligence by 11,000 financial institutions and risk holding the bank, including small community banks, liable for services 5,500 fintechs offer to their customers. Importantly, the 5,500 customers on the Plaid network include many financial institutions, resulting in banks conducting due diligence on other banks.

This is an unmanageable burden for the majority of fintechs and banks, effectively stifling innovation as the majority of resources are diverted to risk assessment. Compounding these issues, data providers use this regulatory uncertainty as a means to justify blocking access to data for companies offering competing products and services. When a bank restricts data access to a data recipient due to perceived third or fourth-party obligations, the consumer has no recourse to restore their data access. The result is that the consumer ultimately does not receive or does not gain full access to the product or service that they have requested.

The active Dodd-Frank Section 1033 rulemaking conducted by the Consumer Financial Protection Bureau provides an alternative to monitor the type of relationships that arise from the current evolved data-sharing marketplace. The Bureau should supervise data aggregators and their customer compliance programs to ensure clear and appropriate oversight, and alleviate current uncertainty by financial institutions that they are responsible for this oversight. (Question 11).

As the agencies consider guidance related to bank and data aggregator partnerships, it will be critical for the agencies to consider and closely follow the Consumer Financial Protection Bureau's Rulemaking to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) relating to consumer access to financial records. In particular, any Section 1033 rulemaking will impact any final guidance the agencies provide on third-party risk management and thus should be considered as a part of this interagency process.

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) was enacted to allow consumers to benefit from access to their own financial data and gives the consumer control over sharing it with the different financial services providers of their choice. Plaid is deeply committed to ensuring that consumers can connect their financial data, whether from a fintech or bank, to access a novel or competing service at another fintech or bank, and submitted comments outlining our stance on how an effective consumer-permissioned open finance ecosystem should work.

The active Section 1033 rulemaking provides an alternative to monitor the type of relationships that arise from this evolved data-sharing marketplace. Banks, aggregators, and fintechs must coordinate on an oversight ecosystem appropriate to ensure consumers are protected from harm, but one that does not artificially enforce third-party or fourth-party risk management requirements where those relationships do not exist. To this end, we recommended that the Bureau supervise data aggregators, which should include supervisory power over the aggregator's customer onboarding and compliance programs.

Such a supervisory regime, incorporating our suggestions in this comment letter for simplified and streamlined bank--aggregator relationship management, would allow prudential oversight of those relationships while the Bureau oversees the aggregator--fintech relationship. Data providers can rely on the clear oversight of entities accessing end consumer data, led by the appropriate agency to oversee this type of access. As discussed in our response to Question #3, current uncertainty over the need to diligence aggregator customers has led to significant negative consequences. By working closely with the Bureau during rulemaking to develop this supervisory model, the agencies will be able to alleviate outstanding concern and associated burden.

We welcome appropriate, collaborative, risk-based, and voluntary Standard Setting Organizations and respective independent certification processes in order to reduce duplicative due diligence processes. (Question 13).

We welcome a consolidated due diligence model led by industry and reviewed by agencies. Plaid echoes the sentiment by the Financial Technology Association that the banking regulators jointly pursue the development of voluntary public-private standards setting organizations (SSOs), along with related independent certification processes, as previously proposed by the FDIC.[7] Recognition by a trusted independent certification body should act as a safe harbor for entities that voluntarily opt-in to certification. Without this provision, such certification risks becoming merely a rubber stamp with very little true benefit to parties in the ecosystem.

[7] FDIC, *Request for Information on Standard Setting and Voluntary Certification for Models and Third-Party Providers of Technology and Other Services* (July 24, 2020), available at https://www.federalregister.gov/documents/2020/07/24/2020-16058/request-for-information-on-standard-setting-and-voluntary-certification-for-models-and-third-party.

In practice, the process of third-party management requires repetitive diligence reviews by financial institutions that are burdensome to both these institutions and their third parties. Oftentimes, this diligence is not adaptive to the most modern technologies and not appropriately risk-tiered, rather it is a "one-size fits all" approach that does a disservice to a constantly adapting security ecosystem. For this reason, it is important that any standard setting organizations include stakeholders across various sizes and risk-profiles, in order to build appropriate risk-based standards that can be independently certified by technology-forward bodies.

It is also crucial that standards and related bodies do not enforce anti-competitive actions to data access. Incumbent developed standards and certifications may serve to artificially restrict access to data through vague risk-assessment and oversight requirements as a means to construct barriers to competing products and services. Appropriate guardrails, including diversity of participants in the process and appropriate recourse to access limitations, must be included during development.

Conclusion

The growth of financial technology, powered by consumer-permissioned data sharing, has led to lower costs for consumers, greater inclusivity in financial services,[8] and a wider range of available products and services to millions of consumers historically left out of the mainstream.[9] Many of these benefits are a direct result of consumers gaining new choices both inside and outside their traditional financial institutions as a result of a competitive and dynamic ecosystem.

We believe the agencies' proposed guidance continues to foster this dynamic ecosystem and are heartened by the streamlined interagency guidance requirements, the principles-based approach, and the focus on a tiered, risk-based model. Our comments in the document serve to further enforce these features of the guidance by addressing opportunities for improvement related to the nuanced relationship between banks, aggregators, and fintechs.

We appreciate your consideration of our comments and suggestions. We would be pleased to provide additional information or to discuss our comments and suggestions with you in detail. Please feel free to contact us at kneal@plaid.com or jpitts@plaid.com.

Sincerely,

John Pitts,
Global Head of Policy, Plaid

Katie Neal
Outreach and Advocacy Lead, Plaid

[8] https://plaid.com/blog/the-fintech-effect-consumer-impact-and-a-fairer-financial-system/
[9] *See* Mehrsa Baradaran, How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy (2015).