October 18, 2021

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-ZA26
Federal Deposit Insurance Corporation
550 17th St. NW
Washington, DC 20429

Re: Proposed Interagency Guidance on Third-Party Relationships: Risk Management
Agency/Docket Numbers:
Docket No. OP-1752
Docket ID OCC-2021-0011
RIN:3064-ZA26

Envestnet Yodlee ("Yodlee") appreciates the opportunity to submit comments 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 ("OCC"; jointly "the agencies") in response to the agencies' proposed interagency guidance and request for comment regarding managing risks associated with third-party relationships.

About Yodlee

As a customer-permissioned data aggregator that has been enabling consumers to access their financial data globally across a vast spectrum of different types of financial accounts for the past two decades, and whose relationships with large financial institutions are subject to examination by the U.S. federal banking agencies under the Federal Financial Institutions Examination Council's ("FFIEC") supervision of large technology service providers, Yodlee appreciates the opportunity to share its expertise and insights as the agencies explore how best to streamline the Board's, the FDIC's, and the OCC's supervisory guidance regarding financial institutions' partnerships with third-party partners.

Yodlee is the leading customer-permissioned financial data aggregation platform globally, with more than twenty years in the industry, providing account aggregation capabilities with hosted

solutions and commercial application programming interfaces ("APIs") on a business-to-business basis to customers around the world, including 15 of the largest 20 U.S. financial institutions. These customers, which include both financial institutions and financial technology firms, offer data from Yodlee's platform to consumers through the customer's own financial wellness, affordability check, verification, and other solutions, which provide a single platform for consumers to track, manage, and improve their financial health across a host of different banks and platforms that provide financial advice and lending solutions. These applications can, for example, provide a single platform to track, manage, and improve consumer financial health across a host of different banks and financial institutions, provide financial advice, and offer expanded access to credit, in addition to many other use cases. Across our platform, more than 25 million consumers are currently utilizing their own financial data to access financial products and services that are improving their financial wellbeing.

As the leading enabler of consumer financial data access, Yodlee has been integrally involved in the Consumer Financial Protection Bureau's ("CFPB") exploration of a rulemaking regarding consumer-authorized data access under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act"). Yodlee was invited to testify at a November 2016 CFPB field hearing on the subject in Salt Lake City, submitted comments to the Bureau's request for information released in tandem with the hearing, and has regularly provided its perspective to the CFPB's Office of Innovation for the last several years. Yodlee also participated in the Bureau's 2020 symposium regarding the merits of a rulemaking under Section 1033 of the Dodd-Frank Act and continues to advocate for a strong CFPB rulemaking under that statute that would provide for an open finance framework under which data aggregation platforms are subject to direct CFPB supervision.

Yodlee welcomed President Biden's issuance in July of an Executive Order on Promoting Competition in the American Economy, which included a provision directing the CFPB to finalize a Dodd-Frank Section 1033 rulemaking. This rulemaking, when finalized, will provide a legally binding financial data right to financial institution customers and will create an open finance regime in the United States. We applauded this order as a critical step forward in the development of an open finance system in the United States, and are now respectfully urging the agencies, in this and other future policy reform efforts, to ensure coordination across the federal regulatory system toward the open finance framework that a Section 1033 rulemaking will establish.

Overview

As a longstanding provider of financial services, Yodlee is examined by the OCC as a Technology Service Provider under the Bank Service Company Act. Our bank relationships have been subject to FFIEC supervision since 2001 and, to our knowledge, Yodlee is the only data aggregation platform in the United States subject to such regulatory rigor. The scope of our examinations has included our cybersecurity policy and operations, risk management procedures, data governance, employee data access, and physical security.

To be clear: Yodlee strongly supports a consumer-centric financial regime in the United States, with appropriate regulatory oversight to provide for both consumer protection and the safety and soundness of financial institutions and the financial system more broadly. Such a framework should, in our view, include supervisory oversight of financial data aggregators and their relationships with non-bank financial applications by the CFPB under the statutory authority granted to it under Section 1033 of the Dodd-Frank Act. We have advocated for such a supervisory regime to include minimum governance requirements for third-party financial technology applications that connect to supervised aggregators' permissioned data, and clear lines of regulatory jurisdiction and supervisory expectations for all industry stakeholders. To achieve this goal, we believe that the agencies should, either through the FFIEC or individually, uniformly examine data aggregators' relationships with financial institutions. Yodlee's experience as an examined entity under the FFIEC's guidelines over the last 20 years has, in our view, demonstrated the benefit of regulatory rigor in the aggregation marketplace and has provided the significant benefit of consistent regulatory application of third-party relationship risk management requirements as opposed to myriad interpretations by individual financial institutions regarding regulatory expectations.

Yodlee's Commitment to Data Security and Risk Management

Yodlee is committed to leading industry practices for data security, regulatory compliance, and privacy. As a technology service provider to leading global financial institutions, we adhere to the strong security and risk management standards required to partner with the largest and most heavily regulated financial institutions in the world safely and securely. As a result of these partnerships with sophisticated financial institutions, Yodlee is consistently examined by both the FFIEC and our bank partners. For example: in the most recent 24-month period, we have undergone nearly 200 audits by financial institutions.

Yodlee has been a leading provider of cloud-based financial technology services to global financial institutions and innovators for almost two decades. Our risk programs are designed to meet not only their expectations, but also some of the most stringent security, privacy and compliance standards in the world. Envestnet's Enterprise Security Group focuses on information, network, and application security and manages a comprehensive program of risk-driven policies and procedures to maximize the Information Security Program ("ISP"), including guidelines and frequent audits. The ISP covers all aspects of the production, development, staging, and corporate environments as well as vendor relations and personnel management.

Yodlee prioritizes its comprehensive risk management program, which is designed to intelligently focus resources and efforts to minimize security risk profiles. The process consists of formal risk assessments at the organizational and product level. In addition, risk management is incorporated into all facets of our processes, including integration with application development, data center operations, and internal security processes. We have long followed industry best practice guidelines in the design and implementation of our network security environment. Other key controls include:

- Central bastion hosts
- Multi-factor authentication
- Resilient and redundant infrastructure
- Data encryption
- Centralized Security Incident and Event Management (SIEM)

Yodlee does not believe that the notions of customer-permissioned financial data access and appropriate regulatory oversight for permissioned data connectivity are mutually exclusive. The proliferation of well-designed open finance systems across the globe, each of which include significant participation from competent regulatory authorities, is, in our view, evidence that the most appropriate path toward providing a safe and secure ecosystem in which consumers and small business may access their financial data without undue restriction is one in which clear, unambiguous regulatory expectations are set for all stakeholders. We believe that the combination of the CFPB's forthcoming rulemaking under Section 1033 of the Dodd-Frank Act and the agencies' proposal to harmonize their third-party relationship risk management supervisory guidelines presents a significant opportunity to achieve a similar outcome in the United States to the frameworks we have seen built in the United Kingdom, Europe, Australia, Brazil, South Africa, and many other countries.

Accordingly, we submit the following responses to those questions included in the agencies' proposal for which Yodlee has an informed perspective based on our significant experience in the marketplace over the last two decades.

A. General

Question 2. What other aspects of third-party relationships, if any, should the guidance consider?

Wider proliferation of bank partnerships with third-party providers faces two major barriers: (1) financial institutions' concern that one of their regulators may not approve of the partnership or the third party and, (2) particularly for smaller banks, the significant resources required to onboard and maintain a third-party partner in a manner the financial institution deems to be compliant with existing third-party relationship risk management requirements. This is especially true for financial technology providers since their offerings are relatively new and regulatory expectations for the types of services they provide are not uniformly interpreted across the wide spectrum of financial institutions.

As financial institutions subject to existing laws and the agencies' third-party risk management expectations have sought to implement partnerships with financial technology partners, including data aggregators, they understandably have also sought to codify duties and obligations on those market actors who are connecting to their systems. These realities manifest themselves currently as provisions embedded in proposed bilateral data access agreements that financial institutions require third-party data aggregators to execute as a condition of building permissioned data

access connectivity for their customers. The absence of clarity with respect to what types of obligations and responsibilities sit with each downstream data user has caused absorption of risk and liabilities on these other market participants that runs the risk of stifling innovation and limiting competition in the best of cases and collapsing the entire data access system in the worst. Unfortunately, guidance published by prudential regulators in this space to date has only served to exacerbate the likelihood of this potential outcome by increasingly placing responsibility for oversight of the permissioned data access marketplace on data holders and, accordingly, increasingly restricting the ability of financial institutions' customers to connect their data with third-party service providers.

Many new and smaller fintech providers are currently ill-equipped to understand, let alone implement, needed precautionary customer protections in the current market. That leaves data aggregators with few choices. To address demand from consumers requesting services from other types of financial technology firms not already subject to regulatory guidelines, the aggregator must create its own framework that allows the aggregator to comfortably absorb responsibility for the oversight and ongoing compliance of its data user customers. All of this is occurring without any actual legal guidance or applicable regulatory obligations for the financial technology firms themselves.

Requiring data aggregators to exercise such diligence without clear, uniformly applied examination guidance is untenable and ineffective given the large and growing number of market participants. Each data aggregator has necessarily implemented its own process of governance and oversight of the data users on its platform as a means of complying with disparate requirements from its bank partners, each of which is based on financial institutions' interpretation of existing regulatory requirements. With our decades of experience being subject to our own regulatory obligations in this market, Yodlee has an appreciation for the significant benefit to the entire marketplace that can be delivered through clear, unambiguous regulatory expectations applied in this space that are examined directly rather than through individual audits by thousands of financial institutions.

Question 10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?

In our view, the most important element of a well-designed third-party risk management framework for third-party technology providers like Yodlee is the provision of clear instructions with regard to the agencies' expectations of the minimum requirements needed to partner with a regulated financial institutions and clarity with regard to exactly what types of documentation can be provided to fully satisfy a bank examiner. Clear, objective requirements for third-party partnerships that leave little room for interpretation by regulated entities results in a more efficient, uniformly applied onboarding process for third-party technology firms that partner with banks.

Such guidance can establish this necessary clarity by publicly and clearly addressing the following and by extending direct oversight to financial data aggregators' relationships with

financial institutions: whether a vendor's product or service is effective; whether the service provider and its product or service follows the laws, regulations, and best practices for protecting bank customers and maintaining safety and soundness; and whether the vendor meets minimum data and cyber security requirements, including through earning other certifications.

Question 11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?

As the holders of consumer accounts, banks have almost exclusive authority to facilitate or restrict consumer-permissioned access to account data. As noted above, banks may cut off the data flow to aggregators, revise their user agreements to encourage or prevent consumers from sharing account data, modify account security infrastructure to enable or preclude aggregators from accessing account information, and/or seek onerous contractual terms such as demanding unlimited liability for breach exposure, implementing data use limitations or use case restrictions, or insisting on requirements to delete consumer information at their request. Typically, such restrictions are justified by the financial institution as necessary compliance with safety and soundness concerns resulting from the current risk-management regime which places all due-diligence responsibility on the financial institution.

As a solution, in recent years a significant number of national banks have requested that customer-permissioned data aggregators like Yodlee enter into bilateral data access agreements with them. The agreements would, when enacted, facilitate a transition from either existing dedicated data feeds that these banks have established over the last twenty years or from screen scraping technology to data access utilizing APIs built by the bank. However, the slow and expensive process of developing proprietary APIs and executing bilateral data access agreements is not providing for ubiquitous deployment of API connectivity across the full spectrum of U.S. financial institutions.

As a member of the board of the Financial Data Exchange ("FDX"), we are supportive of a transition from other technologies to APIs and have publicly announced the execution of several data access agreements with national banks. However, we also acknowledge that this transition is likely to prove more difficult for smaller financial institutions for several reasons. First, the foundational element of enabling this transition – building and implementing an API specifically for customer-permissioned data access – can be capital intensive for smaller institutions.

Second, in the absence of both a clear consumer data right or an open finance ecosystem in the U.S. financial marketplace, negotiating each of these agreements has taken, on average, approximately two-and-a-half years from inception to execution and has required significant investment from both counterparties, both financially and in manhours. Yodlee does not believe that small financial institutions are well positioned to devote this level of expense and labor intensity to negotiate data access agreements with every financial aggregation firm in the market. From a purely technology-focused perspective, smaller financial institutions are beholden to their technology processors, which historically have been slow to innovate.

While we support the joint agency proposal to create uniform guidance on this issue, we are concerned that the existing process does not sufficiently address the existing barriers to a consumer-controlled open finance system. In our experience, we have seen banks using existing guidance documents to justify ad-hoc restrictions to data access. The existing supervisory strategy merely provides guidance, while ultimately leaving banks with all the responsibility for interpreting and enforcing third-party compliance. In common scenarios where a bank restricts data access to a third party under the guise of safety and soundness concerns, the third-party provider lacks the ability to provide a counter argument or make any changes that could assuage the bank's concerns.

The simplest solution to this problem would be the creation of a regulatory structure in which the agencies exert direct supervision over and retain full responsibility for interactions between financial institutions and data aggregators, while the CFPB, upon finalization of a rule under Section 1033 of the Dodd-Frank Act, is similarly responsible for supervising the relationship between data aggregators and third-party providers, and by extension, the end users. We would also urge the agencies to avoid formalizing any mandate, explicit or otherwise, that requires supervised financial institutions to transition to API environments for the purposes of enabling their customers to provide access to transaction data to third-party providers. Instead, providing clear regulatory expectations to institutions that elect to continue using existing technological processes for permissioned data access will allow smaller financial institutions to continue to take advantage of technology-based tools that can provide better financial outcomes for their customers while providing for appropriate safety and soundness protections.

As the agencies consider existing guidance and regulations regarding third-party risk management, Yodlee would offer that the notion of any third-party service provider existing under a well-managed federal regulatory regime is a fundamental underpinning of a well-functioning open finance system. By contrast, the United States' patchwork of state-led data privacy and portability regimes, the fragmentation of federal jurisdiction over financial products and services among several different regulatory agencies, and a lack of a clear legal right for consumers to access and permission access to their own financial data has created obstacles to enabling a true open finance regime in the United States.

As regulators contemplate the future of digital banking, we would respectfully suggest considering using the various statutory tools within their authority to require data aggregation firms to adhere to the data protection and privacy requirements of the Gramm-Leach-Bliley Act and to submit to supervisory oversight by the appropriate federal agency or agencies. As larger numbers of bank customers adopt third-party financial tools, and as banks grapple with the compliance expectations of the federal agencies when they execute bilateral data access agreements with financial aggregators, such an action would provide for better clarity and improved customer and safety and soundness protection throughout the financial system.

Question 18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?

The OCC made clear in its March 2020 third-party relationship risk management guidance its enhanced regulatory expectations for banks that enter into data access agreements with aggregators as compared to those that enable their customers to access their data through other technologies. While these expectations are sensible, they have, in practical terms, further complicated the data access landscape, primarily for two reasons. First, the enhanced regulatory expectations for those institutions that choose to deploy APIs to facilitate data connectivity has emerged as a potential additional barrier for smaller institutions to implement APIs. Additionally, the OCC's guidance with regard to its expectations for those institutions that facilitate data access through legacy technologies has in some cases stymied connectivity. While we support the joint agency proposal to create uniform guidance on this issue, we are concerned that the OCCs 2020 FAQs have increased the complexity of the data access landscape.

Since the issuance of this guidance, we have noticed an increase in banks using their existing supervisory responsibilities to justify ad-hoc restrictions to data access based on their interpretation of their regulators' expectations. In common scenarios where a bank restricts data access to a third party under due to regulatory compliance concerns, the third-party provider is entirely beholden to the bank's stated interpretation of regulatory expectations. Unfortunately, the OCC's 2020 FAQs have served to exacerbate this market dynamic and have created an environment in which the largest financial institutions are in a position of increased control over whether and how their customers will have the ability to share access to their financial data. This gray area is the direct result of an insufficiently developed regulatory regime, in which regulators place growing burdens on institutions to meet increasingly complex expectations, without providing clear means of assurance.

Regardless of institution size, the current regulatory regime puts the onus on banks to take responsibility for ensuring compliance with regulatory expectations and gives them significant latitude to decide what data elements to allow their customers to share, with which third parties, and how. To be able to compete, all banks must be able to offer these products and services to their customers while ensuring that they are meeting regulatory requirements - particularly keeping sensitive customer information safe and secure. The largest banks are most readily able to meet these demands both by developing products themselves and by driving, through the influence of their market share, how the marketplace engages with third parties.

Therefore, we offer that the simplest solution to this problem would be to remove the interpretive role banks play today in this space through the creation of a regulatory structure in which the agencies supervise and retain full responsibility for interactions between banks and data aggregators, while the CFPB, upon finalization of a rule under Section 1033 of the Dodd-Frank Act, is similarly responsible for supervising the relationship between data aggregators and third-party providers, and by extension, the end users. We view this construct as conforming to the letter and spirit of President Biden's recent Executive Order on competition.

Conclusion

As a partner to most of the largest banks in the United States, the leading financial data aggregation firm globally, and an FFIEC supervised technology service provider, we believe Yodlee has a uniquely informed perspective on how best to balance safety and soundness requirements with digitally powered innovations in the financial marketplace. Once again, Yodlee appreciates the opportunity to provide our perspective as a financial data aggregator to the agencies on their proposed risk management guidance for third-party providers.

Thank you in advance for your consideration of this submission, and for your continued work on this critical issue.

Sincerely,

[redacted]

Chad A. Wiechers
Senior Vice President, Data Access & Strategy
Envestnet Yodlee