October 25, 2018

ELECTRONICALLY SUBMITTED

Comment Intake
Mr. David J. Redl,
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration Financial Industry Regulatory Authority
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC, 20230

Re: Request for Comments on Developing the Administration's Approach to Consumer Privacy [Docket No. 180821780-8780-01]

To Whom It May Concern:

Envestnet Yodlee ("Yodlee") appreciates this opportunity to share our perspective in response to the National Telecommunications and Information Administration's ("NTIA") and Department of Commerce's ("the Department") request for comments on advancing consumer privacy while protecting prosperity and innovation. As the leading financial account aggregation platform provider globally, and with nearly two decades in the industry, Yodlee strongly believes in the ability of technological innovation to safely empower consumers by increasing competition and providing broader access to technology-based financial tools that drastically improve both consumers' and small business' financial wellbeing.

Yodlee is a business-to-business, consumer-permissioned financial data aggregation and analytics platform that enables financial institutions and financial technology firms alike to provide consumers with innovative new products and services that can help them improve their finances. These customers use the Yodlee platform to connect millions of retail and small businesses and individual consumers and investors with their own financial data to provide financial wellness 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.

Customers also use Yodlee's platform to establish the authenticity of account holders in real time and to improve the real-time affordability checks required by providers of credit. Yodlee's customers include 12 of the 20 largest banks in the United States and top global banks in more than 20 countries, including Bank of America, Goldman Sachs, Wells Fargo, and American Express. Leading global financial innovators like Kabbage and PayPal are also Yodlee's customers.

The Department's decision to seek public comment on consumer privacy is timely since industries across sectors are increasing their efforts to collaborate with regulators and policymakers on this important consumer protection issue. The issue is particularly relevant for international firms like Yodlee that have been engaged with policymakers globally to provide input into their national or, in some cases, continental, privacy standards.

As it relates to Yodlee, the growth of the financial technology ("fintech") sector has presented consumers with tools that can promote competition, improve market stability, meaningfully help improve financial wellness, and, ultimately, foster improved economic outcomes for consumers and small businesses alike Below, Yodlee respectfully shares our views from the perspective of operations in the fintech sector on the two part approach the Department outlines: 1) Privacy Outcomes and 2) High-Level Goals and Federal Action.

I. Privacy Outcomes

A. Through this RFC, the Department is first seeking feedback on what it believes are the core privacy outcomes that consumers can expect from organizations.

1. Are there other outcomes that should be included, or outcomes that should be expanded upon as separate items?

Yodlee strongly supports these policy outcomes as key identifiers and provides additional comments and suggestions on their definitions below.

2. Are the descriptions clear? Beyond clarity, are there any issues raised by how any of the outcomes are described?

1. Transparency. Yodlee agrees with the Department's expectations of transparency, as well as with its statements that it may be achieved via various means and that a lengthy description is not always (hardly ever) the best mechanism for the desired outcome. Yodlee adds to this that, in our experience, consumers are trained in one of two ways to deal with their need for transparency. The first is to "hope for the best" and blindly accept the terms without really understanding them. The second is to place reliance on brands or trust marks with the general belief that these provide a level of assurance that their privacy is well managed. It is the latter situation that can be improved with the evolution of well defined, less sectoral, programs for privacy data handling and enforcement.

2. Control. Yodlee supports a definition of reasonable control, which also requires a definition of what constitutes personal information, particularly in the financial space. In Yodlee's view, personal information should be defined as any data elements that a consumer creates in the course of one's financial life, such as transaction data. These controls also need to be harmonized with existing regulations. In the financial services sector, decades of existing statute and regulation, including the Bank Secrecy Act and anti-money laundering rules, could require financial firms to retain data for law enforcement or investigatory purposes. A privacy standard that affords, for example, consumers with a blanket "right to be forgotten" could very well create

a scenario under which a financial firm would be forced to select whether to comply either with existing laws and regulations or the new privacy regime. As another example, the privacy regime enacted under the Gramm-Leach-Bliley Act, designed to enforce the account holder's consent over the use of their data by the financial institution is frequently misrepresented to deny the account holder's use of their data with other third parties. Accordingly, ensuring harmonization across the existing regulatory framework is crucial to prevent such situations.

3. Reasonable Minimization. Yodlee agrees with the definition and supports minimization by use-case first rather than by privacy risk. Use case restrictions may cause the consumer harm and will, at a minimum, deny intended benefits. Privacy risks can be addressed by a variety of other safeguards that allow responsible consented use of the data. Yodlee believes every piece of a consumer's financial data should be made available for that consumer to share with third parties of their choosing, but not all data is necessary for every use case. As a responsible party in the ecosystem, Yodlee's view is very straightforward: only the data that is necessary to provide the use case for which the consumer has provided their consent should be collected and used in connection with that use case. However, this position should not be construed to imply that the firm holding the data is permitted to unilaterally minimize the data available for the consumer. In a holistic consumer-centric ecosystem, the consumer is empowered to determine what data to share with what party, and their consent cannot be overridden.

4. Security. Yodlee believes all stakeholders *must* participate under defined standards for conduct, safety, and governance in the collection, processing, storage, and use of a consumer's data. These standards should serve as a baseline for any consumer privacy regulations. Across the various countries in which we operate, Yodlee holds the consistent position that any party that is a holder of a consumer's data should ultimately hold the responsibility for protecting that consumer from harm resulting from the breach or misuse of that data. This notion has been acknowledged in several countries that have implemented Open Banking or other open data initiatives, and we therefore suggest that this straightforward consideration of responsibility for security should be included in the scope of this framework and in any resulting privacy proposals. In technical terms, Yodlee's safeguards employ a wide range of security measures including: least-privilege access controls to all systems and consumer data elements, data masking and encryption, hardened configurations and comprehensive monitoring of all access to customer data with real-time alerting of anomalous activity or behaviors.

5. Access and Correction. Yodlee agrees with this definition and believes the notion that standardization of consumer data access, provided that it is in accordance with U.S. law and regulation, is both a fundamental consumer right and a market-driven imperative. Yodlee encourages focus on how to balance the consumer's ability to exercise their rights with the hosting organization's perceptions or risk and harm. Yodlee has found that organizational self-interest is used to interfere with consumer rights.

6. Risk Management. Yodlee agrees with Department's description of risk management, but urges guidance to organizations to ensure that subjectively perceived risks do not interfere with the consumers' rights to access and use their data.

7. Accountability. To build an ecosystem in which responsibility for notifying and making consumers whole is easily understood and enforced, the Department should consider the institution of traceability as part of any data privacy proposals it ultimately recommends. The concept of traceability conveys that any party accessing a consumer's data with the consumer's permission is identified through technical mechanisms, such as unique, coded headers embedded in the authorization call that the party uses to access the consumer data, required to provide its service. Accordingly, every entity to which a consumer has permissioned their data is identifiable. In the event of a data breach, this chain of identifiers can be used as forensic evidence to trace the source of the breach to the party that was responsible for it.

Accountability is a principle that logically follows traceability. A successful framework will implement traceability as a means of ensuring that any party responsible for a breach of consumer credentials is liable for any financial loss incurred by the consumer. To ensure this is the case, Yodlee suggests that the Department pursue the goal of an ecosystem in which every party that holds consumer data is able to make their customers whole in the event a breach of their systems results in consumer financial loss. In other geographies, this has been accomplished through a combination of capital and minimum levels of liability insurance commensurate with the potential risk each party presents to consumers in the case of a security event. Under a system in which both traceability and accountability are implemented, all parties involved in a breach would be aware of what entity was responsible and would have assurances that the responsible party is held liable for any losses, thus addressing the key hurdle that traditional financial institutions now face under the existing statutory and regulatory framework when their consumers elect to use third-party tools.

II. High-Level Goals and Federal Action

B. The Department is also seeking feedback on the proposed high-level goals for an end-state for U.S. consumer-privacy protections.

Are there other goals that should be included, or outcomes that should be expanded upon?

1. Harmonize the regulatory landscape. One of the systemic disadvantages facing the fintech ecosystem in the United States as compared with many other countries that have imposed standards with regard to consumer-permissioned data access, security, and privacy is the immense relative regulatory fragmentation that exists for the U.S. financial system. There are at least eight federal regulatory agencies with jurisdiction over at least some portion of financial data access in the United States: the Bureau of Consumer Financial Protection, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Reserve Board of Governors, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Federal Trade Commission. There are also regulatory authorities in each state that have jurisdiction over entities that play a role in the fintech market, financial services providers and fintech firms alike. A range of industries in the United States encounter a similar fragmentation within the regulatory frameworks that govern them.

Yodlee strongly believes that an important step towards a level playing field and greater consumer protections is a framework under which greater domestic, public-private coordination provides harmonization, rather than divergence, which, in turn, would spur innovation and improved consumer and small business financial outcomes. Yodlee is supportive of the notion of a national set of minimum data privacy and control standards that would encapsulate best practices, provided that standard is enforceable and effective. Furthermore, from an international competitiveness perspective, it is imperative U.S. policymakers and regulators establish a framework that maintains some degree of interoperability with other regimes globally so that U.S. industry does not face a competitive disadvantage in the years ahead.

2. Legal clarity while maintaining the flexibility to innovate. Yodlee supports this provision.

3. Comprehensive application. Yodlee supports this goal and believes the only way for true harmonization is when all stakeholders are held to the same standard and operate under the same set of regulations. Comprehensive application will be best achieved through active collaboration and coordination between the private sector and government agencies with the goal of ensuring strong consumer protections and accountability across all industries. With respect to the financial services sector, the landscape is somewhat unique given the multitude of existing regulations and requirements with regard to the collection, processing, and storage of data. Accordingly, while Yodlee is supportive of a holistic approach, clear guidance is required for how a new privacy regime will coincide with myriad existing statutes.

4. Employ a risk and outcome-based approach. While Yodlee agrees that new regulations should not be enacted unless they can be effective, a risk-based approach is only effective alongside a set of minimum standards for security and liability, coupled with a strong outcome-based approach. Risk is not easily determined and varies by use case. Accordingly, some institutions may interpret risk in a way that prevents consumers from fully accessing their full personal or financial data. For example, some financial institutions have historically restricted third-party access to consumer transaction data despite the consumer's express consent for that access. These blockages have relied on both prohibitive covenants within the terms and conditions between financial institutions and their customers, which customers must accept in order to open an account, as well as the implementation of technological barriers to block aggregation services from accessing consumer account information. Accordingly, a risk-based approach must not contribute to the reasoning behind blockages such as these, where consumer consent has been expressly permissioned.

5. Interoperability. Yodlee agrees that the goal of a seamless cross-border and cross-industry flow of data is important to limiting disruption across regulatory jurisdictions, both domestically and internationally. Within the United States, when seeking interoperability, several issues must be considered, including: the different regulatory and statutory environments across different industries, the different technologies within those respective markets, and the varying degrees of sensitivity of the data being collected, processed, and retained by the entities across the markets, jurisdictions, and industries.

As a company that operates in multiple jurisdictions globally, Yodlee has experience operating under myriad regulatory frameworks. To the extent that the private sector and other regulatory agencies come together to develop best practices that could be adopted broadly across the financial services sector and other industries, the European Union's recently-enacted General Data Protection Regulation ("GDPR") is a framework that U.S. policymakers may look to as a basis for what could work in the U.S. ecosystem.

GDPR, in large part due to its attempt to universally apply to every conceivable use or application of a consumer's data, takes a very broad view of what a consumer's personal data may be and the privacy rules that accompany them. Though designed to provide European consumers with complete control over how their data is used, GDPR has the potential to make more difficult some uses cases that provide consumer benefit in the financial services context.

In order to inform its own development of privacy proposals, the Department may benefit from monitoring the European market in the months ahead for signs of what provisions are working and where challenges with compliance remain. With thousands of U.S. multinational companies already complying with GDPR requirements, and with the Federal Trade Commission having acknowledged it will enforce those standards on U.S. companies who have adopted them, it may behoove U.S. policymakers to further this framework for effective consumer protections. Of course, adjustments would be required to ensure that the GDPR framework works in the U.S. market.

6. Incentivize privacy research. Yodlee supports this goal.

8. Scalability. Yodlee supports this goal and believes that factors for scalability in a multi-pronged, risk-based approach should include not only the type and size of the organization, but also the type of personal information and data being collected, the number of consumers or end-users, and the number of connections to other parties. This approach should also include previously mentioned support for minimum security and liability standards in order to ensure full participation across industry while also understanding higher standards will be required in various use-cases.

III. Conclusion

Yodlee commends the Department's leadership on advancing consumer privacy and for its outreach to the public as it considers how best to pursue an effective balance between consumer protection and innovation.

Looking ahead, Yodlee believes it is incumbent upon the Department to make a clear designation as to which agency or intergovernmental task force will be responsible for seeing these proposals to fruition in order to ensure a clear roadmap that provides uniformity, harmonization, and greater clarity. Without this designation, accompanied by a plan for future steps in the process high-level principles will lack the necessary tools for execution, continuing the current regulatory fragmentation without a solution. Meeting the goals identified in this notice will require ongoing dialogue and coordination across the private sector, dozens of federal agencies,

as well as myriad state agencies across the nation. A clearly defined plan establishing who will be leading the effort moving forward is necessary to ensure effectiveness.

Lastly, with regards to the Department's discussion on definitions of key terms, Yodlee believes that continued dialogue and examination is required to ensure any standard definitions are the result of comprehensive interaction with the industries under unique regulatory regimes (e.g. financial services, health care, etc.) in the broader endeavor for harmonization.

Yodlee appreciates the opportunity to provide input on the Department's request for comments and thanks the Department for its thoughtful and exhaustive approach to ensuring a sound, effective, and consumer-focused approach to any future privacy regime. Yodlee hopes the Department finds this input beneficial. We look forward to further collaboration with the Department on its efforts.

Sincerely,

Steven Boms
On behalf of
Envestnet Yodlee