March 5, 2019

ELECTRONICALLY SUBMITTED

Hon. Mike Crapo, Chairman
U.S. Senate Committee on Banking and Urban Affairs
239 Dirksen Senate Office Building
Washington, DC 20510

Hon. Sherrod Brown, Ranking Member
U.S. Senate Committee on Banking and Urban Affairs
503 Hart Senate Office Building
Washington, DC 20510

Re: Invitation for Feedback on Data Privacy, Protection and Collection

Chairman Crapo and Ranking Member Brown:

Envestnet Yodlee ("Yodlee") appreciates the opportunity to share our perspective regarding the debate surrounding consumer data privacy and policies Congress may pursue to strengthen and modernize relevant statutes. As the leading consumer-permissioned financial account aggregation platform provider globally, with nearly two decades in the industry, Yodlee strongly believes in the ability of technological innovation to empower consumers and fuel better financial outcomes by increasing competition and providing broader access to technology-based financial tools that drastically improve their financial wellbeing, while adhering to best-in-class privacy and data security standards.

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 those consumers improve their financial health. These customers use the Yodlee platform to connect millions of retail and small businesses, 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 personalized financial advice, and offer expanded access to responsible credit products.

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 13 of the 20 largest banks in the United States and top global banks in more than 20 countries, as well as many of the top financial technology firms around the world.

The Committee's request for comments on consumer data privacy, protection, and collection is timely, as industries across sectors are seeking to collaborate with regulators and policymakers globally as market stakeholders seek to strike the appropriate balance between consumer privacy and innovation in a 21st century economy. This issue is particularly relevant for international firms, like Yodlee, that have been engaged with policymakers globally for the last several years

to provide input and expertise into national and continental privacy regimes. We respectfully provide a narrative in response to several questions the committee has posed, which we hope will inform the work you and your colleagues will undertake with regard to consumer privacy in the new Congress.

The financial technology industry has created incredible benefits for consumers through innovative financial tools. Yodlee and many of its customers operate in jurisdictions across the globe, each with unique privacy and data regimes, as well as in ecosystems that have implemented Open Banking standards. Accordingly, we endeavor to operate under several high-level universal principles that serve our central mission of delivering benefits to consumers' financial wellbeing in a fully consent-driven model that protects their privacy. These same principals should be applied to any successful data privacy regime in the United States. These principals consist of four core components:

1) Consumers must be able to safely access and share, without undue restriction, their financial account data with providers of their choosing for the purpose of obtaining some benefit, product or service;

2) Consumers must provide affirmative consent on the basis of clear and conspicuous disclosure regarding the use of their data;

3) All entities who handle consumer account information must adhere to that consent, as well as best practices for security standards and implement traceability/transparency protocols that can be used to trace what entities held a consumer's data; and

4) The entity responsible for a consumer's financial loss or breach of personal data must make the consumer whole for their direct losses.

In order for any digital ecosystem to work effectively, Yodlee believes it is imperative that consumers have the absolute ability to provide their consent to grant and to revoke access to, and use of, their personal data to third parties of their choosing. Clear and understandable disclosures coupled with affirmative consumer consent must be at the foundation of any framework that seeks to ensure strong consumer privacy protections and sound data security. In the absence establishing the consumer's consent as the fundamental building block for such protections – or in a system that allows the consumer's consent to be overridden by any entity that accesses or holds their personal data – the consumer's control of their data has been lost and the ecosystem is not appropriately serving its end users. In other words: the consumer must be fully empowered to decide how to use their own financial data.

In order for all parties in the ecosystem to rely on consumer consent, that consent must be tied to an unassailable identity. In the financial context, once the consumer's identity has been verified, consumers must be able to access their accounts, transactions, and other personal data an entity with which they do business holds without obstruction or selective withholding of information.

Additionally, with their consent, a consumer should have the ability to responsibly share their own data with other entities and third parties within the ecosystem however they choose in order to receive some benefit from a product or service that relies on that consumer's permissioned data. Any entity to which the consumer permissions their data should be required to comply with appropriate privacy regulations, and the consumer should understand clearly what data they are permissioning in exchange for receiving a product or service.

Furthermore, 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 to power the use case of their choice. In the financial services market, these services include lending, financial wellness, financial planning, credit verification, automated saving, and investing, among many others.

To build an ecosystem in which responsibility for notifying and making consumers whole is easily understood and enforced, further consideration should be given to the institution of traceability as part of any data privacy regime. 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, as a requirement to provide its service. In a traceable ecosystem, 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, with significantly more certainty than exists in systems without traceability, 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, through fraud or a data breach, for an end user losing funds is responsible for making that end user whole for their direct losses. Accordingly, Yodlee supports the notion of an ecosystem in which every party that holds consumer data is able to make their customers whole for their direct losses 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.

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. To the extent possible, Yodlee would respectfully encourage federal policymakers to endeavor to harmonize efforts related to building data security and privacy regimes. A failure to do so will see the United States fall behind competitively as many other governments globally are pursuing such frameworks.

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 both enforceable and effective and applied as universally as possible. Furthermore, from an international competitiveness perspective, it is imperative that federal and state policymakers establish a framework that maintains some degree of interoperability with other regimes globally to ensure that American companies – and consumers – do not face a competitive disadvantage relative to

other regimes globally in the years ahead. True harmonization will be achieved 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 state and federal government agencies with the goal of ensuring strong consumer protections and accountability across all industries.

The landscape of the financial sector is somewhat unique with regard to data privacy and security given the multitude of existing statutes and regulations governing the collection, processing, and storage of financial data. Accordingly, while Yodlee is supportive of a holistic approach, clear guidance is required for how any new privacy regime will interact with myriad existing statutes.

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" or "right to deletion" 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 national privacy regime for financial data 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 sometimes misrepresented to deny consumers the use of their data with other third parties. Accordingly, ensuring that a consumer is afforded both the ability to protect but also the ability to permission their financial data in any new privacy regime is critically important.

As a company that operates in multiple jurisdictions globally, Yodlee has experience operating under many different 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 might 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 both of what a consumer's personal data may be and the privacy rules governing that data. 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 Committee may benefit from ongoing monitoring of the European market for signs of what provisions are working and where challenges with compliance remain nearly nine months after implementation.

With thousands of U.S. multinational companies, including Yodlee, 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 the Committee to further examine this framework for effective consumer protections. Of course, adjustments would be required to determine whether a framework resembling GDPR could work in the U.S. market, especially as more individual states seek to implement their own privacy frameworks, which has a potential to increase regulatory fragmentation, rather than harmonization.

Yodlee appreciates the opportunity to provide input on your request for comments and thanks you for your thoughtful and exhaustive approach to ensuring a sound, effective, and consumer-focused approach as Congress considers a path forward to providing solutions to this important issue. Yodlee hopes you and your colleagues on the Committee find this input beneficial. We look forward to further collaboration with the Committee on its efforts.

Sincerely,

Steven Boms
On behalf of Envestnet | Yodlee