



Larry Chadwick
Senior Managing Director,
Head of Government Relations

601 13th Street NW
Washington, DC
20005

Phone: (202) 637-8922
Email: lchadwick@tiaa.org

March 15, 2019

United States Senate Committee on
Banking, Housing, and Urban Affairs
Attn: Sen. Mike Crapo, Sen. Sherrod Brown
Via Email to: submissions@banking.senate.gov

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

Dear Senator Crapo and Senator Brown:

Teachers Insurance and Annuity Association of America (“TIAA”) appreciates the opportunity to share our views on how policymakers can improve the legal and regulatory framework governing the collection, use and protection of sensitive information by financial regulators and private companies.¹ For TIAA, protecting the sensitive data of our five million individual customers across more than 15,000 institutions is a top priority. In general, we believe that the existing regulatory regime governing data privacy for financial institutions, as established by the Gramm-Leach-Bliley Act (GLBA) in 1999, is strong and offers appropriate protections for our customers. However, there are some areas where we believe those protections can and should be enhanced.

Importantly, financial institutions governed by GLBA (“Covered Financial Institutions”) are not the only companies that handle sensitive financial information from their customers. In today’s increasingly complex marketplace, financial institutions must rely on the cooperation of third-party vendors to deliver the products and services customers expect and need. In order to provide that support, vendors often need access to sensitive customer information – but GLBA’s data protection requirements do not extend to third-party vendors of financial institutions. Rather, it is the responsibility of each Covered Financial Institution to ensure that its vendors comply with the institution’s GLBA-mandated information security program.

Instead of obligating Covered Financial Institutions to police the cybersecurity practices of their vendors, we believe it would be more efficient to subject a broader array of financial-services providers – including both Covered Financial Institutions and their vendors – to the GLBA data-protection framework. Allowing financial regulators to oversee and examine both

¹ *Request for Feedback on Data Privacy, Protection and Collection*, U.S. Sen. Comm. on Banking, Housing, and Urban Affairs (Feb. 13, 2019), *available at*: <https://www.banking.senate.gov/newsroom/majority/crapo-brown-invite-feedback-on-data-privacy-protection-and-collection>.

Covered Financial Institutions and their vendors to monitor GLBA compliance would lead to more consistent and robust cybersecurity practices across the industry and improve data protection for customers. We also support the development of a uniform, nationwide data breach notification standard to ensure that customers across the country are notified of data breaches by their financial-services providers in the same way and within the same timeframe, regardless of their state of residence.

With this in mind, we are happy to share our feedback with the Senate Committee on Banking, Housing, and Urban Affairs (the “Committee”). We hope this request is the beginning of an important and overdue dialogue on the need to reform existing data privacy protections.

About TIAA

TIAA is the leading provider of retirement services for those in the academic, research, medical, and cultural fields. For over one hundred years, TIAA’s mission has been to aid and strengthen the institutions and participants we serve by providing retirement and financial solutions that meet their evolving needs. Today, TIAA manages more than \$970 billion in assets for the five million clients we serve across more than 15,000 institutions.² We are proud of the fact that we have paid out over \$400 billion in retirement benefits over the last century, with more than \$5 billion in benefits being paid to our retired clients in 2017 alone.

With our strong not-for-profit heritage, we remain dedicated to the mission we embarked on in 1918 of serving the financial needs of those who serve the greater good. In order to serve those financial needs, TIAA collects and safeguards significant amounts of sensitive customer data. As such, we support having a robust and well-designed legal and regulatory framework governing the storage and use of customer information by not only financial institutions, but their third-party vendors as well.

All companies should be subject to a uniform, nationwide data breach notification standard.

Currently, state law governs the security breach notification requirements for any company that maintains personal information. This state-level framework has created a patchwork of inconsistent requirements across the country, meaning that individual consumers may receive different information (or no information) about the same data breach, depending on their state of residence. A breach that triggers required notification in one state may not even qualify as a “notifiable” event in another state that requires notification, for example, only when the impacted institution believes that consumers are likely to experience harm as a result of their data being exposed.

TIAA believes that the time has come for a national uniform data breach notification standard. Consumers deserve to know that their data will be treated with a consistent level

² Asset and participant data are as of December 31, 2018.

of care, regardless of an individual's state of residence – and a uniform standard would provide that every victim of a data breach will be treated equally. We also believe that any uniform notification standard should require covered institutions to provide methods of redress for data breach victims so that these individuals can protect their personal and financial information from further threats.

For the financial institutions under this Committee's jurisdiction, a nationwide breach notification standard would reduce compliance costs, as firms would no longer be faced with an inconsistent landscape of notification requirements that vary from state to state. Customers would not only benefit from the resulting cost savings, but also from high levels of data protection and more consistent data breach notices.

Covered Financial Institutions' third-party vendors should be directly subject to GLBA's data protection requirements.

To better safeguard sensitive consumer information, we believe it is necessary to subject Covered Financial Institutions' third-party vendors to the same data protection regime that currently applies to the institutions themselves. Covered Financial Institutions offer a wide and growing range of products and services to meet the needs of their customers. Market forces demand continuous innovation – and in order to facilitate this innovation and provide an ever-increasing array of services, Covered Financial Institutions often look to third-party vendors for assistance (e.g., providers of cloud storage services). These vendors can help financial-services companies develop solutions that are more efficient, faster, and simpler for customers – but to do so, vendors often need access to the institution's customer data.

Currently, GLBA requires all Covered Financial Institutions to maintain the confidentiality of their customers' information and adopt and maintain physical, administrative, and technical controls to address foreseeable risks to the integrity and confidentiality of such information. Not only are Covered Financial Institutions required to have these systems in place, they must also ensure that their third-party service providers (who are not directly subject to GLBA) maintain the same controls.

TIAA believes it is time to extend the mandated data protections that apply to Covered Financial Institutions to the entire range of companies that have access to customer data for purposes of providing (or assisting in providing) financial services. The current GLBA framework is, appropriately, very flexible and risk-based, which allows Covered Financial Institutions to adapt their data protection practices as risks change. However, the current system is also costly and inefficient, as each institution must independently ascertain whether its third-party vendors have adopted sufficient controls and practices to protect sensitive customer information. This can be an unwieldy and inconsistent process, and may ultimately result in weaker data protections. Moreover, the ability of any Covered Financial Institution to impose the needed rights and requirements with respect to its third-party vendors depends heavily on the bargaining power of the parties involved (for example, a large technology company may not agree to provide services to a mid-sized Covered Financial Institution if doing so would require the adoption of new data protection controls by the technology company). In contrast to GLBA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the European Union's General Data Protection Regulation (GDPR) impose data protection obligations directly on third-party service providers, establishing a minimum level of cybersecurity standards that vendors must meet.

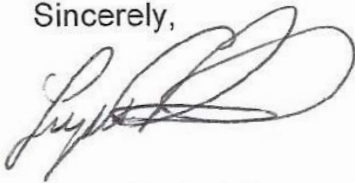
The GLBA framework works well for financial institutions today, as it requires functional regulators to enact and enforce consistent regulations. Banking regulators have also developed an extensive catalog of examination guidelines and guidance around data protection through the Federal Financial Institutions Examination Council (FFIEC).³ We believe this GLBA data protection regime is generally well-designed and effective, and we support its extension beyond financial institutions to third-party vendors that handle customer data.

Conclusion

TIAA appreciates the Committee's efforts to examine the regulatory and legislative framework governing the privacy, protection, and collection of consumer data by financial regulators and private companies. We believe our proposed changes will make this framework more robust and effective, ultimately helping to ensure that consumer data is well protected.

If you would like to engage further on any aspect of this letter, please do not hesitate to contact us.

Sincerely,

A handwritten signature in black ink, appearing to read "Larry Chadwick", written in a cursive style.

Larry Chadwick

³ *Cybersecurity Awareness*, FFIEC (Nov. 5, 2018), available at: <https://www.ffiec.gov/cybersecurity.htm>.