DUFF & PHELPS

March 14, 2019

VIA E-MAIL SUBMISSION

Senator Mike Crapo, Chairman
Senator Sherrod Brown, Ranking Member
United States Senate Committee on Banking, Housing and Urban Affairs
United States Senate
534 Dirksen Senate Office Building
Washington, D.C. 20510

Re: Request for Advice on Data Privacy, Protection and Collection Legislation

Dear Senators Crapo and Brown:

Thank you for your invitation to share our thoughts and suggestions regarding the way personal data is collected, used and protected by regulators and private financial companies. Americans are rightly concerned about protecting their data and are looking to Congress to establish clear guidelines.

The Duff & Phelps Institute is a think tank affiliated with Duff & Phelps, a comprehensive global consulting firm with over 4,000 employees in more than 30 countries worldwide. The Institute provides thought leadership on issues requiring the exercise of good governance, with the goal of developing responsible business decisions and sound public policy. We value the opportunity to share our expertise with the Committee, and respectfully set forth our comments below.

Duff & Phelps, LLC
55 East 52nd Street
Floor 31
New York, NY 10055

T +1 212 983 7710

rosemary.fanelli@duffandphelps.com
www.duffandphelps.com

1. What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

   A. ***We recommend that Congress establish a formal definition of "cyber security", and a formal definition of "privacy protection."*** There are important distinctions between these two concepts and they are too often conflated. Our experience is that failing to conceptually separate security and privacy tends to lead to confusion, and ineffective protection measures.

      In our view, "cyber security" relates to access to non-public data by unauthorized persons. "Privacy" is defined as the policies and operational decisions by an institution to share data. Access by designated organizations to data that is authorized to be shared is not a data security issue. Certainly, company decisions relating to data sharing and data monetization can be questioned, but the implementation of company policies with respect to sharing is not a violation of cyber security.

      Defining cyber security and cyber privacy is vital to clarify what does and does not represent a failure of cyber security.

   B. ***We recommend that Congress set forth specific guidelines as to when breach notification is necessary.*** Currently, there exist dozens of different state-level notification requirements which create confusion and inconsistent results. Congress should enact a single, uniform law which would define the circumstances under which notifications are needed for a failure of cyber security, or a failure in privacy (e.g. violating a published privacy policy). Right now, different state rules require residents of different states to receive different notifications under different time-frames, and they even differ in the type of data that must be stolen for the breach to be a reportable event. Put simply, these state-level differences mean that someone

who must be notified because they live in one state would not be required to be notified if they lived in a different state.

Additionally, we believe that credit bureaus should have a specific duty to take reasonable steps to notify affected persons within 72 hours of gaining knowledge that the data of an individual has been available and likely viewed by an unauthorized entity.

Congress should, however, consider more flexible measures for accounts with characteristics that can make the notification process more complex. For example, extra time should be permitted for notifications where:

- The person being notified is known to the bureau to be a minor.
- The person being notified is known to the bureau to be deceased and the bureau does not know the identity of an executor.
- The person being notified is not a U.S. national and does not reside in the U.S.
- The address (either physical or email) is incorrect, and the email is "bounced," or the physical mail is returned by the postal service as undeliverable.

C. ***Congress should establish record-keeping requirements.*** To properly notify users of a breach, it is essential that parties maintain records sufficient to identify with particularity those whose data is affected when an incident occurs. Without effective document retention, it becomes difficult – if not impossible – to differentiate those customers affected by a breach from those who are not. We also suggest a data retention period of five (5) years, which would equate to the record retention periods of regulated financial industry entities.

4. What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

A. ***We recommend that Congress set a uniform and consistent standard to measure the sufficiency of a cybersecurity operation.*** Although we understand a specific set of controls is not practical (because of differences in organizations and technology evolution), benchmark and reference points to industry standards (such as NIST, ISO 27000 series, CoBIT 2019) are possible and would be useful. We believe that using a NIST framework in particular – or one substantially similar – should be considered an acceptable minimum standard.

B. ***We recommend that Congress require firms to appoint a Cybersecurity Officer and conduct annual cybersecurity risk assessments.*** Our experience indicates that one key to a successful cybersecurity program is the designation of a responsible person who should be responsible to management and the Board of Directors. Additionally, any such "Cybersecurity Officer" and/or "Privacy Officer" should be required to conduct an annual risk assessment to evaluate the specific risks faced by the company. This provides a basis for selecting preventive and monitoring/detection tools and validating their incident response program. The requirement should include a sign-off by the Board of Directors or CEO as having been actually completed and constitute an accurate statement of risk. In considering this recommendation, we believe it is important to recognize that some so-called risk assessments are little more than check-the-box-on-the-form exercises and do not consider the circumstances of an organization or the rapid evolution of threats facing public and private sector organizations. Congress has an opportunity to call for effective risk assessments that are compatible with the NIST Framework, or any other widely recognized frameworks that have been cross-walked to NIST.

C. ***We recommend that Congress require a written policy on cybersecurity matters and conduct annual training***

on the policies. We recommend that any oversight or control program be specifically set out in writing. Any such "Cybersecurity Manual", or "Privacy Protection Policies" should, at a minimum, identify the responsible Cybersecurity or Privacy Officer, describe the firm's oversight and control program, the way the program is designed to prevent cyberbreaches, and set forth the firm's notification procedures in the event of a breach. In addition, the firm should conduct annual training for all employees highlighting the various ways wrongdoers are able to effectuate data breaches, including the use of false links and emails disguised to come from clients or other firm personnel.

We thank you again for the opportunity to contribute to this important legislative matter. If you have any questions or comments, please feel free to contact Rosemary Fanelli at 212-983-7710 or at Rosemary.Fanelli@duffandphelps.com.

Respectfully submitted by:

THE DUFF & PHELPS INSTITUTE