March 15, 2019

The Honorable Mike Crapo, Chair
The Honorable Sherrod Brown, Ranking Member
U. S. Senate Committee on Banking, Housing & Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

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

Dear Chairman Crapo and Ranking Member Brown:

Thank you for taking the crucial step of soliciting stakeholder input on the critically important consumer and business issue of data privacy, protection and collection. The Allstate Family of Companies has always, and will continue to, prioritize the protection of our customers' and employees' privacy through rigorous data privacy measures. We welcome the opportunity to share our thoughts on how Congress and the federal government can help ensure maximum protection while also simplifying and streamlining the regulatory and compliance environment.

As a company that operates in every state and with major technology operations overseas, Allstate currently structures our data privacy and protection compliance practices in accordance with an increasingly complex patchwork of state and international requirements. A federal solution to this issue has been necessary for a long time and we are hopeful Congress, through the efforts of the Senate Banking Committee and others, can finally enact meaningful and uniform standards for all industries. Allstate's mission of protecting people from life's uncertainties will be enhanced by your efforts.

In general, Allstate's comments aim to further define and bring clarity to how a federal law can protect the rights every individual has over their personal information (PI). Allstate favors a law requiring companies to provide clear and conspicuous notification to individuals explaining how their personal information is collected, used, retained and disclosed, and to embed and maintain strong privacy protections in all business processes and practices. Allstate's recommendations for doing so include:

- Federal preemption – Any federal legislation should provide broad preemption of state laws and regulations helping create a uniform standard for data privacy that operates as a ceiling and not a floor.

- Transparency – Require that organizations provide greater transparency to the consumer in the form of exercisable consumer rights.

- Accountability – Demand responsibility and accountability from organizations handling personal information by requiring organizations to implement a risk-based approach addressing an organization's handling of PI.

- Timeline for Compliance – Allow organizations twenty-four months to comply with the law due to the enormous compliance, technology and financial undertaking these laws

require. An insufficient timeline for implementation may hasten compliance efforts and inadvertently create additional risk.

- Scope – Volume of personal information records maintained or processed by the entity should be factored when determining whether an entity is in-scope to this law. Significant volume should bring an entity in-scope of the law regardless of company revenue.

We are pleased to provide the following responses to your specific questions and look forward to working with the committee as you look to develop a uniform preemptive federal policy.

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?

Legislation and Regulation

Congress and regulators should give consumers control over and enhanced protection of their data and ensure consumers are notified of breaches in a timely matter by enacting the following:

- Provide more robust rights to the consumer to control their data. For instance, other privacy regulations have enacted the following consumer rights regarding their PI:
    - Opt-out of sharing
    - Access
    - Deletion (or right to be forgotten)
    - Portability
    - Ability to correct

  Enacting consumer rights in a federal privacy law will help provide consumers with more control over how their data is handled by organizations.

- Require organizations be transparent with consumers on how personal data are being used.

- Require organizations to protect data using:
    - Reasonable controls;
    - Risk-based protection practices;
    - Periodic updates and reviews of data being used;
    - Descriptive, not prescriptive, measures to foster innovation while maintaining protection;
    - Privacy education and training;
    - An appropriately staffed privacy program.

- Legislation that encourages organizations to follow best practices for data privacy, protection and collection by providing the following incentives and assistance:

    - Reduce enforcement penalties if organizations demonstrate good faith and reasonable efforts to follow industry best practices including, but not limited to, NIST Cybersecurity Framework and the NIST Privacy Framework (currently being developed).

- Enact a uniform, preemptive data breach notification standard to include:
    - A harm trigger;
    - A reasonable notification timeline – 30 days;
    - Alternative means of notification for major breaches;
    - Exemptions for law enforcement actions and involvement;
    - Credit monitoring offerings;
    - Electronic notifications of breaches.

2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

Congress and regulators should enact policies that establish the following protocols to ensure consumers are aware of the information being gathered and for what purposes:

- Create a model notification form in "plain language" to help consumers fully comprehend the data being collected and how it is used. Form language should be clear and conspicuous.

- Require notification at contract inception of data being collected and used. Notification should include the following disclosure information:
    - Categories of PI that an organization may have on an individual;
    - What sources the PI is gathered from;
    - How the PI is used, shared or sold;
    - Who the PI is shared with and why;
    - Allow consumers to select their PI sharing preferences;
    - Articulate how consumers can learn more about their PI being used and protocols for correcting data.

3) What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?

To ensure consumers have control over how regulators and organizations use their data Congress and regulators should enact policies that require that the use of PI be consistent with the notification contents articulated in the answer to Question 2 and if PI will be used for a new business purpose a new notification should be provided to consumers.

Individuals should also be allowed to appoint a registered "privacy agent" who can assist with the execution of use and understanding of their PI. Organizations should also be allowed to provide financial incentives to individuals who allow expanded use of their PI.

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?

To ensure information contained in a credit file is accurate, Congress and regulators should enact policies to allow consumers to submit clarification and correction requests to organizations and allow organizations to respond to such requests within a reasonable timeframe.

5) What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Congress and regulators should follow the proposed control protocols outlined in our response to Question 1 to allow consumers to easily identify and exercise control of data being collected, shared and used as a factor in establishing a consumer's eligibility for credit, insurance, employment and other purposes.

Thank you again for the opportunity to highlight the importance of federal data privacy legislation and we look forward to working with you throughout the process.

Sincerely,

Courtney V. Welton
Chief Privacy Officer, Deputy General Counsel
on behalf of the Allstate Family of Companies