Insured Retirement Institute
1100 Vermont Avenue, NW | 10th Floor
Washington, DC 20005

t | 202.469.3000
f | 202.469.3030

www.IRIonline.org
www.myIRIonline.org

March 15, 2019

Sen. Michael Crapo
United States Senate
239 Dirksen Senate Office Building
Washington, DC 20510

Sen. Sherrod Brown
United States Senate
503 Hart Senate Office Building
Washington, DC 20510

Dear Senators Crapo and Brown:

The Insured Retirement Institute (IRI)[1] appreciates the opportunity to provide you with feedback and comments regarding the use and protection of sensitive consumer information by financial institutions. IRI acknowledges and appreciates the leadership you have demonstrated both by requesting information from all stakeholders and for your willingness for the Senate to address consumer data protections.

This letter reflects feedback IRI received from our members responding to your call for input prior to introducing potential legislation during this Congress. IRI has long supported measures to protect consumers' privacy and personal information. IRI's 2019 Federal Retirement Security Blueprint includes common-sense, bipartisan policies to help Americans achieve their retirement goals, calls for Congress to enact legislation providing for a uniform standard for data protection which is complementary to the existing framework of international, federal, and state regulatory regimes governing data protections.

Additionally, IRI believes that any proposal to govern data security should:

- Be developed in a manner to enable collaboration with cross jurisdictional counterparts;

[1] The Insured Retirement Institute (IRI) is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, and distributors such as broker-dealers, banks, and marketing organizations. IRI members account for more than 95 percent of annuity assets in the United States, include the top 10 distributors of annuities ranked by assets under management, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, and the advancement of digital solutions within a collaborating industry community. Learn more at irionline.org.

- Provide safe harbors for the existing, comprehensive regulatory regimes governing the insured retirement industry – including the *Gramm-Leach Bliley Act* (GLBA)[2] and the *Health Insurance Portability and Accountability Act* (HIPAA)[3];
- Establish its foundation on a risk-based approach;
- Proportion solutions for organizations which are collecting data as a legitimate business practice, not selling data for profit; and,
- Share accountability for compliance with both the licensee and any third-party service providers.

IRI believes that policies developed in compliance with these principles would best negate any unintended consequences for the insurance and securities industry and provide a workable standard. The comments provided below are consistent with IRI's principle of protecting consumers' personal information while ensuring their access to options which will help them better prepare for a secure and dignified retirement.

CURRENT REGUALTORY REGIME GOVERNING PRIVACY PROTECTION AND COLLECTION

The insured retirement income industry is governed by one of the most stringent regulatory regimes with oversight from federal, state, and international bodies. This governance includes regulatory regimes covering the use and protection of customer data from programs including GLBA, HIPAA, legislation and regulations enacted or adopted by the individual states (e.g., the *New York DFS Cybersecurity Regulation*[4]*, South Carolina Insurance Data Security Act*[5] and the *California Consumer Privacy Act*[6]) and the European Union's *General Data Protection Regulation* (GDPR)[7]. The current regime, however, subjects the retirement income industry to an inconsistent patchwork of regulation which varies from regulator to regulator and across state and national borders.

The GLBA sets forth a comprehensive scheme for collection, protection, and dissemination of personally identifiable information (PII) by financial institutions, including disclosure regarding the uses of such information and with whom it may be shared. Financial institutions may share PII with affiliates or vendors for purposes of developing product offerings, providing services to customers, or other lawful purposes as permitted by individual state laws, but we are not aware of instances where financial institutions sell such information.

[2] Gramm Leach Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).
[3] Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996).
[4] N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2017).
[5] South Carolina Insurance Data Security Act, S.C. Code Ann § 38-99-10 (2018).
[6] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018).
[7] Commission Regulation 2016/679, 2016 O.J. (L119) 1.

IRI COMMENTS ON PROPOSED LEGISLATION

We understand that the primary thrust of regulation in this area would be to make consumers aware of what institutions are doing with their data and give them a chance to take action if they are not comfortable with the practices of the firm. This regime already exists under GLBA. Adoption of additional standards for safeguarding of PII and notification in the event of breaches may be appropriate, but they should be narrowly crafted and should provide a safe harbor if complied with. Aside from that, we believe GLBA establishes a comprehensive regulatory regime for financial institutions in the area of data privacy and not in need of substantial revision.

In addition to GLBA, there are numerous other provisions of federal law (Anti-Money Laundering FINRA rule, Fair Credit Reporting Act, Bank Security Act, etc.) which obligate financial institutions to collect and utilize clients' personal data. Providing access, correction and deletion rights to certain data points – services offered by numerous IRI members to their clients – needs to be properly balanced to ensure financial institutions are able to fulfill their obligations under the laws cited above and compromise the effectiveness of enforcement.

Potential legislation would also need to address enforcement. Currently, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have separate and differing regulatory regimes, each with its own enforcement arms.[8] Given the numerous regulators involved in oversight, a harmonization requirement on any rulemaking built upon the existing requirements of the GLBA would be a workable solution to mitigate differing enforcement structures. While the solution to the enforcement question may be to default authority to the Federal Trade Commission, a robust discussion of preemption and consideration for existing enforcement authority contained in a uniform standard would be required.

Any federal statute must consider the current regime and be cognizant of the compliance issues facing all industries. The need to avoid duplicative and contradictory privacy-related obligations on an organization is of utmost importance. Additionally, consideration should be given to how a federal regulation would work with the privacy laws of other nations (i.e. GDPR) to ensure that there is not a conflict in privacy procedures or regulations that would impede cross-border data transfer.

IRI respectfully requests the proposed legislation take these factors into consideration and provide further exemptions for organizations in compliance with the existing regulatory regime. Additionally, potential federal legislation could help address this inconsistency by providing

[8] The National Conference of State Legislatures maintains a database of the individual security breach notification laws. This database is available at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

uniform standards across industry sectors, ensure adequate disclosures are provided to consumers, and set a consistent standard for breach notifications. IRI further respectfully requests that any proposed legislation take these factors into consideration to provide the retirement income industry and American retirement savers with safeguards while ensuring a harmonized regulatory framework.

On behalf of IRI and its members, thank you again for the opportunity to provide our input on the proposed legislation. As always, IRI would be pleased to serve as a resource for you and would welcome the opportunity to discuss the ideas we have suggested in this letter at your convenience. If you have any questions or require additional information, please contact me at jjennings@irionline.org or (202) 469-3017.

Sincerely,

Paul J. Richman
Chief Government and Political Affairs Officer
Insured Retirement Institute