March 15, 2019

Via email to submissions@banking.senate.gov

The Honorable Mike Crapo
Chairman, Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20515

The Honorable Sherrod Brown
Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20515

Re: Response to Request for Information on Data Privacy, Protection and Collection

Dear Chairman Crapo and Ranking Member Brown,

The Securities Industry and Financial Markets Association ("SIFMA")[1] supports the Committee's efforts to assess consumer financial data privacy, protection, and collection and appreciates the opportunity to submit comments in response to your public request.[2] SIFMA members remain strongly committed to consumer financial data privacy and security. Privacy protections have long been an important part of our members' operations and governance structures due to the comprehensive federal, state, and international standards applicable to our members. These protections are critical for customers of financial institutions and the financial services industry generally.

While financial institutions have followed data protection, data privacy, and data breach notification regimes for over a decade, enhancing consumer data privacy has come to the forefront as a key issue for policymakers, businesses, and consumers due to more widespread use of data in the digital economy.

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] Senate Banking Committee Press Release, *Crapo, Brown Invite Feedback on Data Privacy, Protection and Collection* (Feb. 13, 2019) (available at https://www.banking.senate.gov/newsroom/majority/crapo-brown-invite-feedback-on-data-privacy-protection-and-collection).

The General Data Protection Regulation ("GDPR") in Europe and several notable data breach and data misuse events have resulted in federal policymakers considering changes to existing privacy laws. Further, both the National Telecommunications Information Administration ("NTIA")[3] and National Institute of Standards and Technology ("NIST")[4] have recently begun work to foster the development of themes for national privacy frameworks and data privacy best practices. SIFMA, along with other trade associations, has publicly commented on both efforts.[5]

Similarly, state lawmakers and regulators have also focused more attention on consumer privacy and data beach notification requirements. Last year California passed the Consumer Privacy Act ("CCPA"), which enhances data-related disclosures and allows consumers to have greater access to and control of the personal data that a business holds. The CCPA is a significant new data privacy regime and legislators in several states have already introduced legislation similar, but not identical, to the CCPA. The CCPA does, however, recognize the existing data protections that federal law already extends to financial services consumers by exempting personal data collected "pursuant to" Gramm-Leach-Bliley. Future state-by-state efforts to enact laws like the CCPA creates the potential to significantly further complicate compliance with privacy and data protection laws in the United States. These new laws, layered onto the existing web of 50 state (plus D.C. and U.S. territories) data breach notification requirements, may ultimately be detrimental and confusing to consumers.

The consumer financial system depends on the sharing of individuals' financial data for credit reporting, identity verification, underwriting determinations, fraud monitoring and detection, and many other essential functions driven by current regulatory requirements. Policymakers should be forewarned that imposing inflexible restrictions on the flow of data to third-party service providers or permitting consumers to opt out of routine data sharing with third parties, such as those proposed by some state legislators, could have long-term negative impacts on the economy. Congress should not consider broad opt-out provisions or a data deletion standard that could prevent a financial institution from efficiently completing a transaction or providing the good or service that the consumer has requested. For example, allowing consumers to opt out of reporting credit information to credit bureaus will restrict financial institutions' ability to determine consumer eligibility for personal loans and other financial services that the customer has requested.

SIFMA believes that the current privacy and data protection framework applicable to financial institutions provides consumers with transparency and control related to their personal data and serves as a solid model for a national data protection regime. Congress should, however, ensure that any privacy regime is flexible enough to permit the use of new technology and encourage innovation while still protecting

[3] https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy
[4] https://www.nist.gov/privacy-framework
[5] Letter to NTIA from SIFMA, BPI/BITS and ABA (Nov. 8, 2018); Letter to NIST from SIFMA, BPI/BITS and ABA (Jan. 14, 2019).

consumers. It is also critical to both consumers and businesses that any new federal law clearly preempts the existing (and growing) structure of state privacy and data protection laws and regulations. Without such preemption consumers in different states would likely have different consumer rights and businesses would have to build compliance regimes to account for various state laws. In addition, consumers will be bombarded with countless notices, disclosures, and requests from businesses which are otherwise unnecessary and will only overwhelm customers, especially if state laws are duplicative or in conflict with federal laws. Organizations will have to comply with an increasingly complicated network of requirements which will not ultimately benefit consumers.

Consumer privacy protections like those that currently apply to financial institutions under federal laws and regulations should broadly apply to any party that obtains, holds, or uses individuals' personal financial data. Entities that provide services such as wealth management tools, budgeting applications, and data aggregation should be held to the same data protection and security standards followed by regulated financial institutions. Any party that obtains, holds, or uses financial data must also take full responsibility for that data, including the provision of that data to third parties. Further, consumers deserve to know how third parties will access and use their financial account data. Consumers should be allowed to control which financial account data they chose to share with third parties and should have the clear ability to revoke that consent. These standards are already applicable to financial institutions and should be expanded to cover any entity that holds consumer financial information to adequately safeguard consumers' privacy. Importantly, such minimum standards must include clear regulatory oversight and accountability as well as liability for a failure to comply. Further, institutions that meet a defined set of reasonable data security and protection standards should have a safe harbor from liability if processes and procedures comply with the defined data security and protection standards.

It is important to note that the definition of "personal data" varies widely under state and federal laws and regulations, thus making the applicability of the requirements vary by the type of data and data holder across state and federal laws. Congress should seek to make any new definition of personal data consistent with existing federal law to the extent possible but also ensure that any state law definition is pre-empted, thus avoiding further uncertainty. Also, any federal privacy and data protection law should apply to individual consumers and include exemptions for institutional customer relationships which do not carry the same risks as individual consumers.

Finally, while there are beneficial aspects to both GDPR and the CCPA, neither should form the basis for a U.S. federal standard for consumer privacy and data protection. Each regime has beneficial aspects but there are many provisions that are unnecessarily burdensome with minimal consumer benefits. For example, SIFMA would support targeted enhancements to the existing upfront privacy disclosures which already require financial institutions to disclosure to consumers related to data collection, data sharing, and a consumers' right to opt out of certain data sharing. Conversely, certain rights of access and deletion are operationally challenging particularly for financial institutions which must retain data by law or

regulation. Rights to request or access data should be focused on categories of data, as opposed to specific pieces of data.

1. Consumer Control and Protection of Financial Data; Data Breach Notification

SIFMA members take cybersecurity and data breach protection very seriously, as data loss can result in consumer harm and reputational damage for the financial institution that is difficult to reverse. The financial services industry is among the most heavily regulated industries for cybersecurity and data protection, and compliance with these standards is a priority for SIFMA members.

a. Consumer Control and Protection of Data

Consumer control over personal financial data is a critical element in protecting that data. The financial services industry is currently governed by many requirements that both provide consumers control over their data and dictate how financial institutions must protect that data.

- **Gramm-Leach-Bliley Act ("GLBA")** imposes significant security and confidentiality requirements on regulated financial institutions to protect against anticipated threats and unauthorized access to consumer financial records that may result in substantial harm to the consumer. GLBA also requires financial institutions to disclose the firm's information sharing policies, including disclosure of nonpublic personal information ("NPI"). Consumers have the right to opt out of certain information sharing with unaffiliated third parties. Regardless of the consumer's opt-out, GLBA also restricts financial institutions from sharing account numbers or access codes with third parties (other than credit reporting agencies) for marketing.
- **Fair Credit Reporting Act ("FCRA")** provides consumers with significant protections of personal financial information, including the consumer's right to access their credit file and correct any wrong information. FCRA also limits how consumer credit information can be used and shared by financial institutions.

b. Data Breach Notification

The current patchwork of state data breach notification requirements is complex and unnecessarily burdensome for organizations of any size. Currently all 50 states (plus D.C. and U.S. territories) have distinct data breach notification requirements with a variety of unique breach notification triggering provisions, disclosure formats, and reporting timelines for regulators and consumers. As a result, organizations reporting a breach that affects consumers across multiple states must provide separate

notices to consumers depending on their state of residence if that can be determined. Consumers with multiple addresses in different states may receive multiple different notices about the same breach event.

In 2000, the Securities and Exchange Commission ("SEC") issued Regulation S-P as required under GLBA but did not include an express consumer data breach notification requirement for broker-dealers or investment advisers. The SEC has since implied data breach reporting requirements through examinations and enforcement, but not through formal guidance or rulemaking. As a result, in many states, non-banks, such as broker-dealers cannot avail themselves of state exemptions for organizations that are subject to federal data breach notification requirements.

To further complicate the notification requirements, under GLBA, banking regulators issued a joint notice outlining the customer notification process in the event of a breach in 2005. The FFIEC guidance states that notification is required:

> "When a financial organization becomes aware of an incident of unauthorized access to sensitive consumer information, the organization should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the organization determines that misuse of its information about a consumer has occurred or is reasonably possible, it should notify the affected consumer as soon as possible."[6]

This guidance also outlines the minimum information required to be included in the notice to consumers. Ironically, these requirements are in direct conflict with some state notification obligations.

Congress should establish a federal data breach notification regime that clearly and fully preempts state laws as well as existing federal regulations and guidance. A federal regime that fails to do so will only further complicate and confuse the existing framework of privacy and data protection laws including information sharing restrictions, notice and privacy policy obligations, and data breach notification requirements. Any entity holding personal financial data should be subject to the same data breach reporting requirements if personal financial data is compromised. As a result, financial institutions and non-financial institutions which hold consumer financial information would be subject to the same data breach reporting requirements and use the same form, thus improving reporting to regulators and reducing possible consumer confusion. Furthermore, a new federal privacy law should not be a "floor" for state legislatures to further build upon, thus encouraging additional requirements that would confuse consumers even more and stifle innovation.

SIFMA proposes a uniform federal data breach notification that requires organizations to:

[6] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (March 29, 2005).

- Upon becoming aware of unauthorized access to sensitive non-encrypted consumer information, investigate to determine the likelihood that the breach will result in material risk of consumer harm (i.e., identity theft or financial loss).

- After completing the investigation, notify primary regulators within 72 hours of determining that there is an obligation to notify the regulator of an event. Such a trigger point gives organizations the necessary time to properly investigate a suspicious event, therefore reducing the potential risk of over-reporting to regulators and consumers and alleviating unnecessary burdens on all parties.

- Notify affected consumers without unreasonable delay if the organization reasonably determines that the incident has or will result in identity theft or other financial harm. Notification should not be required if after investigation the covered entity reasonably determines breach has not and will not likely result in identity theft or other financial harm. For example, a breach of encrypted data would not pose a reasonable likelihood of harm without the encryption key also being compromised.

- Offer notified consumers a minimum of one year of credit monitoring services or equivalent services.

These standards would provide clear, effective and consistent notification of data breach events that are reasonably likely to result in financial harm to a consumer.

c. Amendment and Deletion of Information

SIFMA supports providing consumers with greater transparency and control related to personal information. However, certain rights, including the consumer's right to request amendment or deletion of certain data, could conflict with existing federal regulatory requirements applicable to financial institutions. For example, Rules 17a-3 and 17a-4 promulgated under the Securities and Exchange Act of 1934 require broker-dealers to retain most client information for up to six years following account closing. As a result, firms could not comply with requests by consumers "to be forgotten" or for data erasure because such data may be required to be retained under another regulatory requirements. Congress should remain aware of the need to harmonize any future privacy obligations, including new consumer rights, with existing legal obligations for financial institutions.

2. Disclosure to Consumers About Information Being Collected

Consumers should have a clear view of how their personal financial information is being collected and shared. Consumers currently receive a privacy notice from their financial institution when opening an account and under certain circumstances annually thereafter that outlines how consumers' non-public personal information is shared with third parties. The content of these notices sent by our member firms is dictated by GLBA, SEC Regulation S-P, and other regulatory requirements depending on the firms'

regulatory structure. Consumers may also receive other types of notices depending on their relationships with an organization, including notices for consumers, employees, and businesses to name a few. A single short form notice across all types of financial relationships with individual consumers would help to reduce consumer confusion and streamline the notification process for financial institutions and other organizations that hold, store, or use consumer financial data. Financial institutions should not be required to provide such notices to institutional clients or their representatives in the normal course of business because institutional clients are covered by contractual rights and other business-to-business disclosures.

On a related point, SIFMA and others continue to raise significant concerns with the SEC about consumer personally identifiable information ("PII") in the Consolidated Audit Trail ("CAT"). SIFMA has repeatedly expressed concern about the risks of including consumer PII in the CAT outweighing the regulatory benefit.[7] It seems only a matter of "when" the CAT's database is breached, not "if" a breach will happen. At a minimum, the SEC should take steps to assure that affected firms and consumers are provided adequate notice of any CAT data breach under the standards described above. In addition, affected firms and consumers should have a means for reimbursement for reasonable fees and damages incurred in connection with a CAT data breach.

3. Control Over the Use of Consumer Financial Data

Consumers should continue to have the right to opt out of the sharing of personal financial data for third-party marketing purposes. Currently, Reg S-P gives consumers the right to opt out of having their financial institution share their personal information with third parties for the third party's own marketing purposes. This right should be expanded to allow consumers to opt out of allowing any organization, regardless of whether it is a regulated financial institution, to share financial information with third parties for that third party's marketing purposes.

Further, any federal privacy legislation should make clear that consumers cannot opt out of the sharing of personal financial information for anti-money laundering, fraud monitoring, and financial crime prevention or other law enforcement purposes, as well any activities necessary to service the consumer in the ordinary course of business. Although currently consumers cannot opt out of this type of information sharing under Reg S-P, CCPA does not expressly allow for this type of information sharing which, unless fixed, will cause significant issues for financial institutions and law enforcement when the law comes into effect.

[7] For more detailed information on CAT security concerns, see Letter to Brett Redfearn, SEC, from SIFMA (October 2018).

4. Consumer Control Over Information Collected and Shared by Data Brokers and Other Third Parties

Consumer financial data is a valuable resource in today's global economy. The flow of consumer financial data helps improve the products and services available to all consumers, and therefore should only be restricted based on actual risks to consumers. The data brokerage industry has been maligned in the media and by some consumer rights advocates, but some data brokers provide valuable information to financial institutions that can be used to help validate consumer identities, determine eligibility for loans, combat fraud, and make underwriting decisions. Restricting the flow and use of this information would be detrimental to the economy but some parameters should be set to ensure that personal financial data is not mishandled or misused in this context.

Data brokers, data aggregators, and any other unregulated entities that hold non-public personal financial information should be governed by the same privacy and cybersecurity standards imposed on financial institutions by GLBA, whether by legislation or by regulation. Financial institutions should only share consumer financial information with data brokers that have contracted to keep such data secure and to use the data only for purposes for which it was shared.

Data aggregation services raise similar questions and concerns. Data aggregation serves many valuable functions that consumers demand, but such activities are not without risk. At the forefront, the secure transfer of information between financial institutions, data aggregators, and permissioned parties is critical to ensure that customer financial information is not compromised. Currently data aggregators collect personal financial information from consumers either through a technology protocol such as an application programming interface ("API") or by screen-scraping the account information from financial institutions' websites. The latter method raises more privacy and security risks for consumers and financial institutions. SIFMA believes that the industry will be able to develop a common standard to move toward more secure information sharing and therefore reduce the risks associated with screen-scraping. In 2018, SIFMA issued Data Aggregation Principles that guide SIFMA members and data aggregators on the collection, retention, and use of personal financial data.[8] Further, SIFMA along with several financial institutions, technology companies, and permissioned parties, as well as The Clearing House and FS-ISAC, have founded the Financial Data Exchange, LLC, a non-profit group dedicated to developing technical standards for the authorized sharing of consumer financial information for the purposes of data aggregation.[9] Such technology will provide consumers with greater flexibility and control over what data is

[8] SIFMA Data Aggregation Principles available at https://www.sifma.org/resources/general/data-aggregation-principles/

[9] For a list of Financial Data Exchange members see http://www.financialdataexchange.org/

provided to non-financial institutions for the purposes of credit, insurance, employment, and other purposes.

* * *

Thank you for considering these comments in response to your request for information. SIFMA takes consumer privacy and data protection very seriously and would like to serve as a resource for the Committee if needed. If you have any additional questions or concerns, please contact me at 202-962-7300 or at mmacgregor@sifma.org.

Sincerely,

/Melissa MacGregor/

Melissa MacGregor
Managing Director & Associate General Counsel