SIIA Accelerating Innovation in Technology, Data & Media

1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905
www.siia.net

March 15, 2019

Chairman Mike Crapo
Ranking Member Sherrod Brown
Senate Committee on Banking, Housing, and Urban Affairs
512 Dirksen Senate Building
Washington, DC 20515

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

Dear Chairman Crapo and Ranking Member Brown:

The Software & Information Industry Association (SIIA) is pleased to provide you with a formal statement for the record on your call for information relating to the collection, use, and protection of sensitive information by financial regulators and private companies.

SIIA is the principal trade association for the software and digital information industries worldwide. Our membership includes the global industry leaders for the digital age, including software, data analytics, and information service companies. SIIA's member companies reflect the broad and diverse landscape of digital content, including both B2B and B2C services, small specialized providers, and large multinational industry leaders.

We focus our statement on two questions in your February 13, 2019 call for comments:

- Question 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?

- Question 4: 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 companies) use consumer data?

Question 1: Ensuring Consumers are Notified of Breaches in a Timely and Consistent Manner

SIIA endorses the passage of a federal data breach notification law.[1] Such a law should be effective, simple, and protect consumers. It should set notification triggers that are

[1] SIIA also supports ongoing Congressional efforts to enact a comprehensive federal privacy standard to provide strong and meaningful privacy protections, including the identification of core individual rights to notice, access, control, correction, deletion, and portability. In a recent statement filed with the Senate Committee on Commerce, Science, & Transportation, we stated our support for including a data security standard in a federal privacy law. *See* fn. 7, *infra*. Our position with combining data breach notification into a federal privacy law is different, however. Past experience shows that it will require much more time to get to yes among legislators and stakeholders if data breach notification is included in a federal privacy law. To ensure consumers quickly benefit from expanded privacy rights, and for

calibrated to the sensitivity of the personal information at issue, focus on preventing harm to consumers, and ensure flexibility to react and remedy data breaches. Importantly, any federal data breach requirement should remedy the growing patchwork of state data breach notification requirements that are complex, often conflicting, and confusing for consumers.

Preemption by an effective federal law is key to ensuring that all Americans receive equal notice and protection when there is an unauthorized breach of sensitive personal information that poses a risk of harm. A single federal standard will allow business to react more quickly and nimbly to data breaches, resulting in quicker notice to consumers if there is a breach of their sensitive information. American consumers and businesses deserve this certainty, consistency, and effectiveness.

A federal law requiring data breach notification also addresses another unintended negative consequences of a patchwork of state laws: the unavoidable bias toward "big business." Businesses, particularly those innovative businesses operating primarily online, enter a national, and even international marketplace, almost from inception. Yet most of these nascent businesses lack the resources necessary to ensure compliance with any but the most straightforward standards. A complex system of 50 or more state and local data breach notification laws is beyond the capability of all but the most sophisticated businesses. The significant penalties imposed in state laws, like the CCPA, risk that even a single data breach will bankrupt any startup, no matter how promising their technology. A well-crafted federal law can create an environment that protects consumers and promotes innovation.

When exploring a federal data breach notification law, we urge Congress to consider six additional objectives. First, the focus of the law should be on requiring notifications for breaches of sensitive personal information, the disclosure of which pose a concrete or measurable risk of consumer harm. It is important to remember that not all data is *personal* information and not all personal information is *sensitive* information. Requiring breach notifications for the disclosure of non-sensitive information or non-personal information where the disclosure poses no risk of harm creates consumer fatigue for breach notifications, reducing their effectiveness for breaches that pose a real risk of harm. Identifying the risks of harm should take into account whether the information is sensitive or unusable due to encryption, anonymization, or de-aggregation.

Second, any new law should also tailor the definition of personal information and/or sensitive personal information to carve out publicly available information. Publicly available information is information about individuals, businesses, or individuals acting in a business capacity that is in the public domain. This includes public records and information that is

---

businesses to get more regulatory certainty, SIIA suggests that Congress explore separate federal privacy and data breach notification laws.

intended by its nature to be public, such as e-mail addresses, especially business email addresses, and physical business addresses. Due to its public nature, consumers exercise no reasonable expectation of privacy over such information, even when it relates to them in their individual capacities. It is information that is open by its nature, and therefore, poses little risk of harm to consumers from its dissemination. The processing of public information reaps enormous societal benefits, including enabling the rapid extension of personal and business credit, allowing businesses to engage in risk management and comply with "know your customer" standards, and helping law enforcement combat fraud, terrorism, financial crimes, and modern slavery through the identification of suspects, witnesses, and evidence. The concept of "breach" does not make sense in the context of data that is in the public domain.

Third, a federal data breach law should protect consumers by imposing a flexible notification trigger subsequent to the discovery of the breach, based on the reasonable need of the breached entity to appropriately respond to any vulnerabilities. It must not arbitrarily set a prescribed time for notice, like Europe's GDPR and some state laws have done. It's a simple fact that resolving data breaches – either independently or together with law enforcement – often requires and justifies a delay in notification to individuals. When a breach occurs, it is crucial that the first response is to shut down the breach, restore the integrity of the system, assess the scope of the breach and the information impacted, and contact and work with law enforcement where appropriate. Requiring notification at a reasonable time post-discovery ensures the breached entity has the flexibility to triage its response to meet these benchmarks. Federal legislation that sets a post-occurrence and prescribed time period for notification unnecessarily interferes with these critical response stages. Moreover, it puts the breached system at further risk by requiring publication of a security vulnerability before it is fixed. This could result in more bad actors further breaching the system, causing additional consumer harm.

Fourth, the law must focus on improper, unintended, and wrongful releases of sensitive personal information that could lead to consumer harm. The purpose of a data breach notification requirement is to notify consumers of a risk of harm due to the unauthorized disclosure of their information. It is not to give notice of the routine or intended disclosure of data within the normal operations of a business. Any federal law should be drafted narrowly to avoid unintentionally capturing routine, regular, or planned releases of data.

Fifth, a data breach notification must impose appropriate trigger requirements depending on the role of the entity with respect to the information. It is common for businesses to contract with third-parties to maintain or process data, including sensitive personal information. In the event of a breach, the notification requirement is properly focused on the data controller (which typically is the consumer-facing entity that collected the data or determined its use) rather than the third-party (often referred to as a data processor). Requiring third-parties to notify consumers of a breach risks confusion because consumers generally do not know the third-party. Moreover, it may require the dissemination of even more or aggregated or unencrypted information to the third-party in order to make the notification. The proper and

most protective balance is for the law to require notification by the data controllers, and to impose obligations on third-parties to notify the data controllers if they knew the breached data contained sensitive personal information.

Finally, a data breach notification law should include an enforcement element. Currently, the FTC is the agency with primary responsibility for enforcing privacy and data security standards, generally by using Section 5 of its authorizing statute. For the consumer reporting industry, however, the FTC shares enforcement jurisdiction with the CFPB for the Fair Credit Reporting Act standards, including its provisions preventing dissemination of credit file data without a permissible purpose. To ensure enforcement consistency, SIIA supports a federal data breach notification law that places primary enforcement authority in the FTC, but recognizes the complicated stocktaking this presents.

Question 4: Ensuring the Protection and Accuracy of Consumer Credit Files

SIIA supports federal efforts to ensure a fair, accurate, and safe consumer reporting system. Consumer reports play a vital role for our society, enabling the rapid and inexpensive access to credit for consumer purchases and small business expansion. Recognizing the importance of this, Congress passed the Fair Credit Reporting Act (FCRA) in 1970 to promote the accuracy, fairness, and privacy of consumer information in consumer reports. The FCRA includes important provisions regulating the collection, dissemination, and use of consumer information; and providing consumers with a right of access to their consumer reports and the ability to dispute inaccurate information. Notably, the FCRA protects consumer reports from unreasonable disclosure, requiring consumer reporting agencies to take reasonable measures to ensure that consumer report information is only shared with those who have a statutorily prescribed permissible purpose for accessing it.

Turning first to accuracy, SIIA supports the FCRA model, which provides consumers with an open, inclusive method for accessing their consumer reports and disputing inaccurate information and requires that consumer reporting agencies investigate and resolve the dispute within 30 days. This approach strikes the right balance between empowering consumers to verify the accuracy of their own credit data with obligations for the consumer reporting agencies to investigate and resolve consumer disputes.

Consumers are aware of these rights. The FTC provides consumers with extensive education materials, including how to exercise their right to a free annual credit report,[2] and how to dispute inaccurate credit report data.[3] The CFPB dedicates an entire webpage to such

[2] *See* FTC Education Material. *Credit and Your Consumer Rights* (June 2017), https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights.

[3] *See* FTC Education Material. *Disputing Errors on Credit Reports* (February 2017), https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports.

guidance.[4] The three major consumer reporting agencies similarly provide easy-to-understand notifications, guidance, and mechanisms for consumer disputes of credit file data.[5]

The FCRA strikes an important and sensible balance between a consumer reporting agency's obligation to correct information and to accurately report information contained in public records. Take, for instance, public records, such as bankruptcies, liens, and judgments, which comprise one component of a consumer's credit file. The accuracy of information derived from a public record is based on the accuracy of the content of the public record itself. If the public record is inaccurate, the tool for resolving the inaccuracy rests with the custodian or issuing agency.

As an illustration: Jane Doe's consumer report reflects that a county court ordered Jane to pay her neighbor $10,000 in a civil land dispute. If the consumer reporting agency reported that fact inaccurately and the court's docket shows that Jane Doe was not in fact a party, then the consumer reporting agency must correct the report. In contrast, however, if the public record (in this instance, the court docket) mistakenly reflects that the court imposed the monetary judgment against Jane, the consumer reporting agency has no standing to compel the court (or any other government entity) to correct this information.

To require otherwise would essentially make a compiler of public records the entity responsible for the content and correction of government records. Moreover, it would subject public records to the potential for abuse. Take, for instance, the abuse perpetrated on consumers and the consumer reporting agencies by fraudulent credit repair companies that promise to delete even accurate consumer data by inundating the system with dispute requests to exhaust the capacity for reasonable investigation procedures.[6]

Turning next to the data security issues, SIIA also supports the FCRA model. As noted above, FCRA requires covered entities to employ reasonable measures to ensure the information in consumer reports is only shared with those who have a permissible purpose to access it. The permissible purposes are set forth in the statute. The permissible purpose

---

[4] *See* CFPB Education Materials. *Credit Reports and Scores*, https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/.

[5] *See* TransUnion Website. *Credit Dispute*, https://www.transunion.com/credit-disputes/dispute-your-credit; Experian Website. *Dispute Online: How to correct inaccuracies in your Credit Report for free*, https://www.experian.com/disputes/main.html; Equifax Website. *How to dispute information on your Equifax credit report,* https://www.equifax.com/personal/disputes/.

[6] *See* FTC Report on Credit Education and the Credit Repair Organizations Act, ("Credit repair scams often demand that [consumer reporting agencyies] delete not only adverse information on credit reports that is inaccurate or obsolete but also delete adverse information that is accurate and not obsolete, i.e., information that is highly relevant to prospective lenders in making decisions whether to extend credit."), p. 5. , https://www.ftc.gov/system/files/documents/reports/report-credit-education-credit-repair-organizations-act-federal-trade-commission-report-congress/p054815_ftc_report_to_congress_re_credit_education_and_the_croa.pdf;

approach, the parameters of which are decided by Congress, is the right approach to ensuring that those who compile important credit file information only share that information in a manner that advances the principles of fair credit.

With respect to data security more generally, SIIA has endorsed federal data security legislation, either standing alone, in combination with data breach notification law, or included in a federal privacy law. As we noted in a recent statement to the Senate,[7] data security is integral to protecting the privacy of consumers' personal data. The current landscape, like the data breach notification system, involves a number of overlapping, inconsistent, and confusing data security laws across the states. We support a federal law that harmonizes data security standards to create equal protections for consumers and regulatory predictability for businesses. As with data breach notification, preemption is imperative.

What should a national data security standard look like? The NIST Cybersecurity Framework is a good resource for how a standard might be configured. Much like the standard employed by the FTC, a new federal standard should require reasonable and appropriate security measures, the exact nature of which will depend on the sensitivity of the data, the risk of tangible harm from an unauthorized disclosure, the size and complexity of the business, and the availability and costs of the security features. The reasonable data security standards for a consumer reporting agency that handles hundreds of millions of records containing sensitive personal information should not be the same as a small consumer reporting agency that produces specialized consumer reports for local businesses. Under this approach, the obligations scale up with the increased sensitivity and/or volume of personal information and with the resources available to the consumer reporting agency. This balances strong consumer protection without deploying an unworkable one-size-fits all approach.

In conclusion, SIIA appreciates the opportunity to provide you with our comments regarding these important issues. Our members take their obligations to safeguard the data they are entrusted with seriously. We support Congressional efforts to provide national, preemptive standards regarding privacy, data security, and data breach notification that aim to prevent and remedy consumer harms. SIIA and our member companies look forward to working with you and the Senate Committee on Banking, Housing and Urban Affairs, as you move forward with legislation to provide important consumer protections for financial information.

Respectfully submitted,

Sara DePaul, Senior Director, Technology Policy
Software & Information Industry Association

[7] *See* SIIA Stmt. to Senate Comm. on Commerce, Sci., & Transp. (Mar. 12, 2019), http://www.siia.net/Portals/0/pdf/Policy/SIIA%20Comments%20to%20Senate%20Committee%20on%20Commerce%20-%20Federal%20Privacy%20Legislation.pdf?ver=2019-03-12-160058-343.