Information Technology Industry Council

Data Breach Notification Principles

The Information Technology Industry Council (ITI) strongly supports efforts to establish a commonsense, uniform national breach notification regime to help consumers when there is a significant risk of identity theft or financial harm. We are committed to working with Congress to enact meaningful legislation that establishes a national data breach notification process that is simple and consumer-driven. As the committees of jurisdiction in the House and Senate work to develop their respective bills, we urge Members to include the following key elements:

1. Federal Preemption. ITI supports the creation of a strong federal breach notification law. Effective federal preemption of the multitude of state notification laws will allow businesses to notify consumers more quickly when a breach of sensitive personal data occurs by easing the confusion and duplication that results from the current patchwork of competing, and often conflicting, state requirements. With almost every state now having enacted data breach notification laws, it is important that the role of the states be carefully defined in federal legislation.

2. Inaccessible, Unusable, Unreadable, or Indecipherable Data. Data may be unusable due to the absence of critical pieces, obfuscation, encryption, redaction, anonymization, or expiration by its own terms. Effective security practices and methods change over time and new technologies continue to evolve which enable data to be rendered unusable. An effective "unusable data" provision would make clear that notification is not required when there is a reasonable determination that data is rendered inaccessible, unusable, unreadable, or indecipherable. It is important that federal legislation not single out or give preference to one method of rendering data unusable as a means to avoid notification. Such action could create a false sense of security and create a compliance basement which may reduce the development and use of diverse and innovative security tools. ITI supports legislation that recognizes such technologies with technology-neutral and method-neutral language and that allows businesses to determine whether or not data may be used for the purposes of committing identity theft or financial harm.

3. Effective Harm-Based Trigger. Federal breach notification legislation must recognize the delicate balance between over- and under-notification with respect to when notices should be sent to consumers. ITI strongly believes notification should only be required after organizations determine the unauthorized acquisition of sensitive personal data could result in a significant risk of identity theft or financial harm. Expanding the types of harm to vague or subjective concepts such as "other unlawful conduct" creates confusion and will result in over-notification. Additionally, efforts to lower the threshold to a reasonable risk of identifity theft or financial harm will expose consumers and businesses to the numerous costs associated with over-notification. Further, the definition of a data breach should clearly tie an "unauthorized acquisition of sensitive personal information" to the risk of identity theft or financial harm. Not all data breaches are nefarious nor do they create a risk to consumers. Failing to recognize this in the definition of a data breach would expose organizations to possible enforcement action by government entities, including state attorneys general, for unauthorized breaches, regardless of the risk of identity theft or financial harm.

Information Technology Industry Council
1101 K St, NW Suite 610, Washington, D.C. 20005
T +1 (202) 737-8888, www.itic.org

4. Reasonable Scope of Legislation. The protection of consumer information across industries is a complex statutory and regulatory puzzle. It is important that federal breach notification legislation does not create unworkable and overlapping regulatory regimes for commercial and financial services industries. Entities that are already subject to any existing federal data breach requirements in a sector-specific law should continue to be required to comply with those laws and should not be subject to additional regimes.

5. Flexible Manner of Notification. Federal data breach notification requirements must accommodate both traditional companies that communicate with customers by mail, telephone, or fax and online companies that communicate predominantly through electronic communication (e.g., electronic mail). Consumers trust that companies will notify them in a manner that is consistent with previous communications and expect that will be done in an expedient and timely manner. A consumer receiving a telephone call from their email provider outlining a breach and urging action would be justifiably suspicious.

6. Third Party Requirements. Many organizations contract with third parties to maintain or process data containing personal information. Consumers may be unaware of these third-party relationships and requiring a notification from the third party to the consumer may create unnecessary confusion. In the event of a data breach of any third party system, the third party should be required to notify the consumer-facing company of the breach. The consumer-facing company and the third party should then have the flexibility to determine which entity should notify consumers. Additionally, legislation should not require notification of a broad range of third parties other than the consumer and credit reporting bureaus in the event of an actual or likely breach.

7. No Private Right of Action. An effective breach notification requirement and an efficient enforcement framework provides the best protection for consumers and will avoid unnecessary and frivolous litigation. Legislation should also prohibit the use of government regulatory enforcement action in private litigation asserting non-preempted state or other causes of action.

8. No Criminal Penalties. Most data breaches are the result of criminal acts, and therefore, breached entities are the victims of a crime. Organizations can and should do their part to protect consumer data from unauthorized access, but they should not be subject to criminal sanctions for being victimized by criminal hackers.

9. Discovery, Assessment, Mitigation, and Notice. Federal legislation must allow organizations to redress the vulnerability and conduct thorough investigations of suspected data breaches before notifying customers or government agencies. Unless the vulnerability is addressed prior to making the incident public, the organization and its customers are susceptible to further harm. Notifying customers will be counterproductive should the alleged breach prove false or if the breach does not create a risk of identity theft. A tremendous amount of forensics, decision-making, and legal work is required before ascertaining the nature and scope of a breach, assessing the risk of harm, and determining the appropriate form of notification. Recognizing the sophistications of today's hackers, and the challenging nature of a post-data breach forensic investigation, federal legislation must provide realistic, flexible, and workable time requirements, as well as recognize the need to cooperate with law enforcement in their criminal investigations.