BSA | The Software Alliance has for more than a decade supported the establishment of a federal data breach notification standard. In our view, the value of such legislation should be measured against three goals:

(1) Ensuring that consumers receive timely and meaningful notification in the aftermath of a breach;
(2) Encouraging enterprises to maintain reasonable data security practices; and
(3) Creating a consistent national framework to replace the patchwork of state standards.

A federal standard should ensure that consumers receive **timely and meaningful notification** about data breaches that create risks of financial fraud or identity theft.

- The notification standard should be risk-based so that consumers can take steps to mitigate the potential impact of data breaches that create significant risks of material harm. The standard should promote good data storage practices by clarifying that data rendered indecipherable to unauthorized entities through use of encryption or other obfuscation technologies does not create such risks.
- In the immediate aftermath of a data breach, companies should be encouraged (and afforded adequate time) to focus their resources on performing a thorough investigation and restoring the integrity of potentially compromised systems.
- Consumers should generally expect to receive notification from the organization with whom they have a direct relationship. Such a principle promotes good data stewardship, ensuring that entities who collect confidential personal information take a life cycle approach to managing the associated privacy and security risks. Contracts between a covered entity and its third-party data processors should remain enforceable, allowing an efficient allocation of risks.

To help prevent the occurrence of data breaches, Congress should enact a **federal standard for reasonable data security safeguards**.

- A risk-based, technology neutral approach should require companies to maintain data security practices that are reasonably scoped to the size and complexity of an organization, the sensitivity and volume of confidential information on its systems, and the cost of available tools to improve security and reduce vulnerabilities
- To provide consumers and enterprises with greater certainty, a federal standard should identify key data security practices that are entitled to a presumption of reasonableness.

Advancing these goals requires **full preemption** of the maze of existing state standards.

- Companies currently encounter a patchwork of requirements arising from 52 state and territory data breach notification statutes and additional state-specific data security requirements. Complying with the varying (and at times contradictory) standards diverts resources from efforts to secure networks. A national standard should replace the current patchwork, thus providing clarity for consumers and easing the compliance burden on businesses.
- To promote consistent enforcement, legislation should confer exclusive jurisdiction for enforcement to the Federal Trade Commission and state Attorneys General.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org