

The Data Security Act

Rep. Randy Neugebauer (R-TX) and Rep. John Carney (D-DE)

BACKGROUND:

Over the past decade data security has emerged as a critical issue for financial institutions, businesses, and the customers they serve. The patchwork of state laws that currently exist around data security and breach notification have caused confusion and a lack of accountability as cyber criminals continue to steal valuable personal information from consumers. Many times, consumers are unaware of the data breach until long after the breach occurs. This is unacceptable. A comprehensive data security program which applies to all actors within the chain of commerce is essential in order to adequately protect consumers and withstand future attempts to undermine confidence in the safety of sensitive customer data.

In 1999, a Republican Congress passed, and a Democratic President signed into law, the Gramm-Leach-Bliley Act (GLBA). Among its provisions was a requirement that financial institutions develop an information security plan to address their protection of consumer account information and non-public sensitive personal information.

This system has proven to be effective but needs to be expanded so that all businesses, retailers, and financial institutions abide by the same rules of the road when it comes to data security.

THE PROBLEM:

Although the government requires financial institutions to have information security programs, there are others within the chain of commerce that store or handle the same account information and non-public sensitive information. These actors have no equivalent requirements to protect such data.

Without a set of standard requirements to follow, repeated breaches at non-financial institutions have resulted in significant costs for consumers and society. Congress' failure to act has led to a byzantine patchwork of state laws for both data security and breach notification. This is confusing for consumers and a compliance nightmare for companies.

THE SOLUTION:

A national problem requires a national solution. The Data Security Act establishes a single, consistent minimum standard for both data security and breach notification. A single standard for security and breach notification provides better protection for consumers and provides greater clarity for businesses.

The Data Security Act provides flexible and scalable standards. This permits each business to have a data security program that is technology neutral and process specific. Small businesses may tailor their data security requirements to fit with the size, nature, and scope of their business in order to avoid any unnecessary burdens and costs.

SPECIFIC PROVISIONS:

The legislation is modeled on aspects of GLBA to provide a process-driven framework scalable to the size, nature, and scope of an organization, and includes flexibility to keep pace with changes in technology.

Specifically, the bill directs covered entities to develop an information security plan that requires them to:

- Designate at least one employee to manage safeguards
- Conduct risk analyses
- Regularly assess the plan in light of risks
- Update the program on a rolling basis as technology evolves.

The bill also lays out clear requirements for consumer and law enforcement notification after a breach.

The trigger for notification occurs only after a company confirms that hackers acquired sensitive account or sensitive personal information that can be used for identity theft or financial fraud.