

# CONGRESS EDGES CLOSER TO FEDERAL PROTECTION OF SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

Shortly after the November 2006 elections that put the Democrats in control of Congress, Senator Patrick Leahy (D-VT) vowed that as Chairman of the Senate Judiciary Committee he would make protecting the privacy rights of Americans a top priority. On February 6, 2007, he and Senator Arlen Specter (R-PA) introduced legislation aimed at preventing and mitigating identity theft. If passed, the “Personal Privacy and Data Security Act” (S. 495) could affect most businesses in the United States with regard to how they maintain “sensitive personally identifiable information” and how they respond to unauthorized breaches of that information.

Prior efforts by Congress created protections for personal information in certain areas. For example, the Gramm-Leach-Bliley Act became law in 1999 affecting certain nonpublic consumer information held by financial institutions, securities firms and insurance companies. The Health Insurance Portability and Accountability Act of 1996 led to regulations in 2000 affecting health information maintained by covered health plans, health care providers and health care clearinghouses. The Americans with Disabilities Act, Family Medical Leave Act, Fair Credit and Reporting Act, Occupational Safety and Health Administration also contain privacy provisions specific to the substantive issues addressed by those statutes – medical inquiries related to a disability, requests for family medical leave, privacy of consumer reports obtained by employers on employees and applicants for employment, and medical records related to certain work-related injuries or illnesses. The Personal Privacy and Data Security Act (“Act”), if passed, would fill many of the gaps left by prior legislation in protecting personal information maintained by businesses.

This article discusses two goals of the Act – (i) require certain businesses to establish data privacy and security programs; and (ii) following the lead taken by 35 States to date[[Link to prior posting on website re state data breach notification statutes.](#)], provide a national standard for notifying U.S. persons when there has been an unauthorized breach to their sensitive personally identifiable information. The breach notification requirements under the Act would preempt all similar Federal and State laws. Perhaps even more far reaching, however, data privacy and security program requirement would include implementing safeguards such as conducting risk assessments, training employees and monitoring vulnerability of protected information. Before expanding more on these two goals, the section below defines “sensitive personally identifiable information,” the information targeted by the goals.

## **Sensitive Personally Identifiable Information**

Sensitive personally identifiable information is information in electronic or digital form that includes

- An individual first and last name or first initial and last name in combination with any one of the following:
  - Non-truncated Social Security Number, driver’s license number, passport number, or alien registration number.

- Any 2 of the following: (I) home address or telephone number; (II) mother's maiden name; (III) month, day and year of birth.
- Unique biometric data such as finger print or retina image.
- Unique account identifier, electronic identification number, user name or routing number in combination with any associated pass code, access code or security code required to obtain money, goods, services or anything of value, **or**
- A financial account number or credit card number in combination with any password, access code or security code required to obtain credit, withdraw funds or engage in a financial transaction.

## **Goal One: Creation of Data Privacy and Security Programs**

The Act's data privacy and security program requirement would ensure standards for developing and implementing *administrative, physical and technological* safeguards to protect sensitive personally identifiable information.

### *Who Would Be Covered?*

- Business entities engaged in interstate commerce that collect, access, transmit, use, store or dispose of sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons.
- But not (i) financial institutions subject to the Gramm-Leach-Bliley Act, and (ii) covered entities and business associates under the HIPAA privacy regulations.

The requirement that to be covered the entity must have sensitive personally identifiable information on 10,000 or more U.S. persons would seem to have the effect of excluding most businesses. However, the increasing ability to hold greater amounts of data coupled with record retention policies (even those that are short-lived) applying to employee and customer records, could cause smaller companies to find themselves covered by the Act.

Significantly, the Act also would affect many entities that do not meet the requirements above. This is because the Act would require covered entities to require their service providers with responsibilities to sensitive personally identifiable information to agree by contract to have appropriate measures in place that in essence constitute data privacy and security programs similar to those of entities covered under the Act.

### *Data Privacy and Security Program Specifics*

Data privacy and security programs would be required to include the following measures to protect sensitive personally identifiable information:

- Risk assessments
- Policies and procedures that control identified risks

- Training and supervision of employees on the requirements of the program
- Data security vulnerability testing
- Exercise of appropriate due diligence in selecting service providers and requiring such service providers by contract to have appropriate data security measures in place
- Periodically assessing and adjusting the program over time in response to relevant changes in such things as technology and business arrangements.

### *Enforcement and Preemption*

While the Act would expressly preclude private lawsuits, entities violating these requirements would be subject to penalties of up to \$5,000 per violation, per day, with a maximum of \$500,000. Greater penalties would apply for willful violations.

The Act would prohibit States from requiring covered entities to implement administrative, physical and technological safeguards to protect sensitive personally identifiable information.

### **Goal Two: Create a Federal Data Breach Notification Requirement**

The breach notification requirements proposed under the Act are very similar to those enacted by most States.

#### *Who Would Be Covered?*

- Business entities engaged in interstate commerce that collect, access, transmit, use, store or dispose of sensitive personally identifiable information.

#### *Key Features of the Notification Requirement*

- Covered entities would be permitted to contract with third parties to provide the required notice.
- Notice would be required to be provided without unreasonable delay. Reasonable delays would include time necessary to determine the scope of the breach, restore integrity to the system or notify law enforcement.
- Covered entities would be permitted to delay notification upon receipt of written notice from a Federal law enforcement agency. However, covered entities would be required to give notice 30 days later unless they received an additional notice of further delay from law enforcement.
- The notification requirement would not apply if the covered entity certifies that notification could cause damage to national security or impair a law enforcement investigation. This certification would need to immediately be provided to the U.S. Secret Service. The

certification could not be used to (i) conceal violations of law, inefficiency, or administrative error; (ii) prevent embarrassment; or (iii) restrain competition.

- Covered entities would be exempt from the notification requirement if, after conducting a risk assessment, the entity (i) concluded that there is no significant risk that the security breach resulted in or will result in harm to affected individuals; (ii) notifies the U.S. Secret Service of the risk assessment within 45 days after the discovery of the breach; and (iii) does not receive notice from the Secret Service within 10 days to provide the breach notification.
- Permissible methods of notice would include regular mail, telephone notice and electronic notice. Notification through major media outlets also would be required where there are more than 5,000 individual affected.
- Notices would be required to include (i) the categories of sensitive personally identifiable information acquired or reasonably believed to have been acquired; (ii) a toll-free number (or email address) an individual may use to contact the covered entity; (iii) toll-free numbers and addresses for credit reporting agencies; and (iv) information regarding victim protection assistance provided by a State if notice of such assistance is required by that State.
- If the Act would require a covered entity to provide notice to more than 1,000 individuals, the entity would be required to notify the credit reporting agencies. If the number of affected individuals is, or is reasonably believed to be, more than 10,000, and in certain other cases, the covered entity also would be required to notify the Secret Service.

#### *Enforcement and Preemption*

- The Act would expressly preclude private lawsuits. However, entities violating the notification requirement would be subject to penalties of up to \$1,000 per individual, per day, with a maximum of \$1,000,000. Greater penalties would apply for willful violations.
- The breach notification provisions of the Act would supersede and other provision of Federal or State law relating to similar notification requirements.

The Act certainly is not the only privacy and data security measure Congress is considering. (See, for example, bills introduced by Sen. Feinstein (D-CA) (S. 238 and S. 239) on January 10, 2007). However, S.495 seems to be one of the more comprehensive measures proposed. While it is unknowable which proposal, if any, will become law, momentum appears to be building for some action in this area during the 110<sup>th</sup> Congress.

Jackson Lewis will continue to monitor the progress of this proposed legislation, as well as other developments in federal and state law in this area. If you have any questions regarding this legislation or any other workplace privacy or employee benefits questions, please contact the Jackson Lewis attorney with whom you regularly work, or Joseph Lazzarotti with the HIPAA and Workplace Privacy Practice Group, at (914) 514-6107, [lazzarottij@jacksonlewis.com](mailto:lazzarottij@jacksonlewis.com).