A flurry of federal data security and data breach notification bills introduced into Congress

Proposed legislation would preempt 46 state statutes

Recent high profile data breaches and increased attention to the protection of consumers' personal information has intensified the momentum towards enactment of a federal data security and data breach notification law. Currently 46 states and the District of Columbia have enacted data breach notifications with drastically different requirements and policies. Within the last few months, Congress has been inundated with national data security bills outlining an organization's obligations when it suffers a data breach. Unfortunately, the proposed federal bills would, in many instances, further complicate an entity's obligations upon a breach.

Among the numerous federal data security bills introduced, the following four are most recent and significant:

1. Data Breach Notification Act of 2011 – S. 1408 (introduced by Senator Dianne Feinstein)
2. SAFE Data Act – H.R. 2577 (introduced by Representative Mary Bono Mack)
3. Data Accountability and Trust Act – H.R. 1707 (introduced by Representative Bobby L. Rush)
4. Cybersecurity Legislative Proposal (introduced by the White House)

The proposed bills are structured in a similar nature to the state breach notification laws, but contain drastically different requirements. All four proposals would preempt the current state breach notification laws in the 46 states and the District of Columbia. The main similarities and differences are as follows:

Scope

The bills cover persons engaged in or affecting "interstate commerce" that own, transmit, store, use, access or dispose of Personal Information (PI). The Mack and Rush bills define PI as a person's name in combination with a Social Security number, driver's license number, or financial account or credit card number, along with the appropriate security code. The Feinstein and White House proposals refer to a broader definition of PI to include:

1. Name with any two of the following – address, telephone number, mother's maiden name or date of birth;
2. Social Security number;
3. Driver's license number;
4. Account number or credit card number; or
5. Unique biometric data (i.e., fingerprint).

Breach notifications

After discovery of unauthorized acquisition or access to data containing PI, the Mack and Rush bills require organizations to notify the Federal Trade Commission (FTC) and any resident of the U.S. whose PI was compromised. The other proposals do not mandate notification to FTC, unless certain exceptions apply.

Timing of notifications: The Feinstein bill requires affected individuals be notified "without unreasonable delay" whereas the Mack bill requires notification not later than 48 hours after identifying the affected individuals and not later than 45 days after discovery of the breach. The Rush bill and White House proposal allow for up to 60 days after

discovery of the breach.

Content of notifications: All of the bills require a description of the PI that was breached, telephone numbers to call for more information about the incident and the toll-free contact numbers and addresses for the major credit reporting agencies and the FTC.

Credit reports and monitoring: The Mack and Rush bills obligate organizations to provide or arrange for the provision of free consumer credit reports on a quarterly basis for two years or offer free credit monitoring for two years to the affected individuals.

Safe Harbor: All four proposals exempt an organization from providing notice if it determines that there is no reasonable risk of identity theft, harm, or fraud. The bills also create a presumption that no reasonable risk of harm exists if the PI was encrypted.

Enforcement

The Mack, Rush and White House proposals authorize the FTC to enforce violations as unfair or deceptive acts or practices, whereas the Feinstein bill authorizes the U.S. Attorney General to bring a civil action against a violating entity. All four proposals allow for state attorneys general to enforce violations through civil actions to recover penalties, and all preclude a private right of action by individuals.

Fines

The Feinstein and White House proposals limit civil fines to no more than $1,000 per day and a maximum amount of $1 million. The Mack and Rush bills allow for $11,000 per day and a maximum of $5 million.

Data security programs

The Mack and Rush bills, in addition to breach notification obligations, mandate that organizations implement data security policies and programs with respect to the collection, use, sale, other dissemination and maintenance of PI. The bills would require companies to appoint an internal contact to manage the information security. In addition, organizations would be required to implement a process and standard method for disposing of data in electronic form containing PI and destruction of paper documents containing PI.

Preemption

All proposals would preempt state laws that require information security practices for PI and would preempt state breach notification laws.

Previous attempts to pass federal data security and breach notification legislation have consistently failed. With data breaches increasingly in the news headlines, it will be interesting to see if Congress is more motivated to pass such legislation this time around. For now, the 46 various state statutes govern an organization's notification requirements at the time of a data breach. When a data breach occurs, the impacted organization must comply with the state statute relative to the state of residence of each affected individual. Thus, a one-size-fits-all notification letter cannot be used as it would violate several of the state statutes.

If you have any questions, contact:

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com

or any of our Data Privacy and Network Security attorneys by clicking on the link below:

Data Privacy and Network Security

McDonald Hopkins counsels businesses and organizations regarding all aspects of data privacy and network security, including proactive compliance with the numerous state, federal and private data security regulations (including PCI DSS and HITECH) relative to personal information and protected health information, training of employees and preventative measures to decrease the risk of data theft. We also counsel businesses and organizations through the data breach response process and coordinate notifications to affected individuals and state attorneys general, as well as advising on media related issues. Our attorneys can help you properly assess your risks to ensure compliance. After you complete the brief McDonald Hopkins Data Privacy and Network Security Review, your company will be provided with an assessment of the required areas of compliance which have the greatest need of attention and improvement.