KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

October 14, 2014

Federal Bills Pursue Comprehensive Data Breach Notification

The recent string of wide-scale data breach disclosures by major retailers has led to a growing call for federal legislation to protect consumer information and establish uniform data breach notification requirements.

Existing federal laws governing data breach notification are limited to specific sectors such as financial institutions (*e.g.*, the Gramm-Leach-Bliley Act ("GLBA")) and healthcare (*e.g.*, Health Insurance Portability and Accountability Act ("HIPAA")). Almost all states have enacted and enforced laws on data breach notification, but those laws vary in terms of applicability and the requirements for notice recipients, deadlines and content. The current state-based framework has therefore made compliance difficult for companies with national operations.[1]

Attorney General Eric Holder has urged Congress to pass a national standard for data breach notification, stating that such legislation would protect Americans and aid in federal law enforcement agency investigations of criminal activity.[2] The FTC also has made its position clear that "Congress must act" to provide "a strong federal data security and breach notification law."[3] "The FTC supports federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach." The FTC acknowledges that most states have breach notification laws in place, but maintains that "a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected."

Although many state representatives support, or at least do not oppose, a uniform federal standard for data security and breach notification, they have warned against preemption of enforcement authority. Illinois Attorney General Lisa Madigan has testified before Congress with a request to "pass data security legislation that does not preempt state law."[4] Politico reports Maryland Attorney General Doug Gansler as crediting states for "heading up investigations on data breach cases" and "actually get[ing] things done."[5] Politico also quotes Connecticut Attorney General George Jepsen as calling any dismantling of state authority on data breaches a "critical mistake."[6] The National Conference of State Legislatures (NCSL) states that it "does not oppose baseline federal data security breach notification standards, provided that the requirements do not preempt state authority to adopt standards that provide affected consumers additional protection and notification." The NCSL

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Mark H. Francis
+1 212 556 2117
mfrancis@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

New York
1185 Avenue of the Americas
New York, NY 10036
Tel: +1 212 556 2100
Fax: +1 212 556 2222

www.kslaw.com

additionally "supports allowing state financial regulators and attorneys general to enforce any new federal data security breach notification standards."[7] If Congress follows these requests and enacts a federal data breach notification law that leaves heightened state standards intact, companies will still be faced with ensuring compliance on a state-by-state basis.

New proposals for federal privacy laws appear geared to preempt state laws governing data security and breach notification, although states may retain partial enforcement authority. This would be a departure from existing federal laws (such as GLBA and HIPAA) that do not preempt state authority and instead set baseline requirements that can be supplemented by state law. In 2014 alone, four data privacy bills have been introduced with data breach notification standards:

- The *Personal Data Privacy and Security Act* was introduced on January 8, 2014 by Senator Leahy (D-VT) and co-sponsored by Senators Schumer (D-NY), Franken (D-MN), and Blumenthal (D-CT), later joined by Senators Menendez (D-NJ) and Klobuchar (D-MN) (the "Leahy bill").[8] The same bill was brought to the House of Representatives by Representative Shea-Porter (D-VT) on February 4, 2014.[9]
- The *Personal Data Protection and Breach Accountability Act* was introduced by Senator Blumenthal (D-CT) on February 4, 2014 (despite his co-sponsoring the Leahy bill), and co-sponsored by Senator Markey (D-MA) (the "Blumenthal bill").[10]
- The *Data Security Act* was introduced on January 15, 2014 by Senators Carper (D-DE) and Blunt (R-MO) (the "Carper bill").[11]
- The *Data Security and Breach Notification Act* was introduced on January 30, 2014 by Senator Rockefeller (D-WV) and co-sponsored by Senators Pryor (D-AR), Nelson (D-FL) and Feinstein (D-CA) (the "Rockefeller bill").[12]

Timing of Notification

The four bills vary greatly with respect to the requirements on timing of notifications. The Leahy bill requires business entities who experience a data breach to notify individuals within 60 days or obtain approval from the FTC for a longer notification period. The Rockefeller Bill requires notification to affected individuals within 30 days. The Blumenthal bill requires notification be made "without unreasonable delay," but requires notification to a designated centralized agency within 10 days of discovering the breach, and that agency will then forward the breach report to the FTC, FBI and Secret Service. Notification of individuals must occur within 10 days of the reports to the FTC, FBI and Secret Service. Therefore, in the event of a significant breach, the deadline to meet all notice obligations under Blumenthal's bill could be as little as 12 days. The Carper Bill mandates subsequent regulations to "establish standards for when a covered entity shall provide any notice." The proposed legislation also varies in terms of federal agencies that must be contacted in the event of a breach and prescribes differing timing requirements for federal agency notification. One thing that is clear from this proposed legislation is that companies must act quickly upon the discovery of a data breach and must have an effective breach response plan in place to ensure swift investigation and response.

Required Content

The bills provide slightly different requirements for the content of breach notifications. The Leahy bill generally requires that notifications (1) describe the personally identifiable information that was breached, (2) provide a toll-free number to contact the business regarding the personally identifiable information it maintains, and (3) provide a toll-free number and address for the major credit reporting agencies. The Blumenthal bill adopts these requirements and adds disclosures of (4) the telephone numbers and website addresses for "relevant federal agencies that provide information regarding identity theft prevention and protection," (5) notice regarding rights to obtain free consumer credit reports, (6) notice regarding rights to placing a security freeze and (7) "notice that any costs or damages incurred by an individual as a result of a security breach will be paid by the business entity or agency that experienced the security breach." The Rockefeller bill

also starts with the Leahy bill requirements, but includes disclosure of the right to obtain consumer credit reports and the FTC telephone number and website address for information about identity theft. The Carper bill requires that notices describe the information at risk, the actions taken to address the breach, and the consumers' rights under the FCRA to place a security freeze on their accounts.

Exemptions

The bills permit exemptions or delays at the behest of federal agencies if necessary for law enforcement investigations or authorized intelligence activity. All of the bills exclude entities that comply with the breach notification requirements of the GLBA and HIPAA.

The Leahy and Blumenthal Bills both include a "safe harbor" exemption for providing notice when the business provides the FTC with a risk assessment concluding that the breach will not harm affected individuals and the FTC does not object (*e.g.*, if the risk assessment shows that the data was encrypted and not accessible). The bills also include a "financial fraud prevention" exemption where a business implements procedures to prevent unauthorized financial transactions. Likewise, the Rockefeller bill does not require notice if "there is no reasonable risk of identity theft, fraud, or other unlawful conduct," which may be presumed if the data was encrypted or otherwise protected from disclosure. The Carper Bill does not contain any safe harbors but only requires notification if personal information is likely to be misused in a manner that will cause substantial harm or inconvenience to the consumer.

Preemption of State Authority

The Leahy and Rockefeller Bills preempt state laws on the protection of personal information and data breach notification. The FTC and Attorney General are tasked with enforcement, but state attorneys general may bring enforcement actions as well. The Blumenthal Bill goes one step further and adds a private right of action for individuals harmed by violations of the bill. By contrast, the Carper bill preempts all state authority, including enforcement.

It remains to be seen whether sufficient bipartisan support exists to bring such laws to fruition, and what balance of federal and state enforcement will result. Given the level of national concern and press coverage of this issue, however, the support for federal legislation is growing and will likely lead to a federal data breach law. Even without federally-mandated breach notification requirements, companies should expect state attorneys general and the FTC to remain active in monitoring company response in the wake of a data breach.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property

rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

---

[1] *See* National Conference of State Legislatures, "Security Breach Notification Laws," *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[2] *See* Press Release, *Attorney General Holder Urges Congress to Create National Standard for Reporting Cyberattacks*¸ Department of Justice (Feb. 24, 2014), http://www.justice.gov/opa/pr/attorney-general-holder-urges-congress-create-national-standard-reporting-cyberattacks; *see also* http://www.justice.gov/agwa.php (video).
[3] Prepared Statement of the Federal Trade Commission, *Data Breach on the Rise: Protecting Personal Information From Harm*, Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate (Apr. 2, 2014), http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.
[4] Prepared Statement of Illinois Attorney General Lisa Madigan, *Protecting Consumer Information: Can Data Breaches Be Prevented?* To the Subcommittee on Commerce, Manufacturing, and Trade Committee on Energy & Commerce, U.S. House of Representatives (Feb. 5, 2014), http://docs.house.gov/meetings/IF/IF17/20140205/101714/HMTG-113-IF17-Wstate-MadiganL-20140205.pdf.
[5] Jessica Meyers, *States defend turf from feds on data breach rules*, Politico (Feb. 19, 2014), http://www.politico.com/story/2014/02/states-defend-turf-from-feds-on-data-breach-rules-103647.html.
[6] *Id*.
[7] National Conference of State Legislatures, *Policies for the Jurisdiction of the Communications, Financial Services & Interstate Commerce Committee*, as of the annual business meeting of the NCSL Standing Committee on Communications, Financial Services & Interstate Commerce (Aug. 22, 2014), http://www.ncsl.org/ncsl-in-dc/task-forces/policies-communication.aspx.
[8] *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014), *available at* https://beta.congress.gov/bill/113th-congress/senate-bill/1897/text.
[9] *See* Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2014), *available at* https://beta.congress.gov/bill/113th-congress/house-bill/3990/text. (This is the fifth iteration of a bill that has been introduced by Senator Leahy each term since 2005).
[10] *See* Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014), *available at* https://beta.congress.gov/bill/113th-congress/senate-bill/1995/text.
[11] *See* Data Security Act of 2014, S. 1927, 113th Cong. (2014), *available at* https://beta.congress.gov/bill/113th-congress/senate-bill/1927/text.
[12] *See* Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014), *available at* https://beta.congress.gov/bill/113th-congress/senate-bill/1976/text.