Government Focus on Cybersecurity Elevates Data Breach Legislation

by Experian® Government Relations and Experian® Data Breach Resolution
Will Congress pass data breach legislation in 2015/2016?
Recent high-profile security breaches at nationwide retail, healthcare, entertainment, public sector and financial services organizations has brought heightened attention from lawmakers in Congress and the Obama Administration. This growing focus on cybersecurity and data breaches, coupled with a growing sense of bipartisanship on the issue, have led some to speculate that Congress could finally pass a national data breach and data security standard to replace the current patchwork of state laws. However, obstacles remain that may make consensus just beyond the grasp of policymakers.

At the same time, policymakers in the European Union and Brazil are considering new approaches to data breach notification that could impact businesses that engage in global commerce.

Navigating state laws makes compliance challenging
The current regulatory framework in the U.S. does not provide a national uniform data breach notification standard that applies to all personally sensitive information. Instead, when a breach occurs in the U.S., businesses are guided by a patchwork of 49 existing laws in nearly every state, the District of Columbia and Puerto Rico. In fact, with the enactment of a data breach standard in Kentucky this past year, Alabama, New Mexico and South Dakota are currently the only states that do not have breach notification laws on the books. While they may all be similar in some aspects, each state has its own requirements surrounding the content and timing of a notice to consumers, as well as the types of breached information that would trigger consumer notification. This patchwork, at the very least, makes compliance difficult and may confuse consumers seeking to understand their rights.

In addition to the existing body of state laws, two sector-specific laws govern breaches of a consumers’ (1) health related data and (2) financial data.

“Regardless of where you do business, there is a complicated set of state laws and regulations for organizations to follow to ensure they are in complete compliance. A best practice to navigate the complex regulatory landscape is to identify and begin working with subject matter experts ahead of time, including legal counsel, to stay on track with response to a data breach.”

Michael Bruemmer CHC CIPP/US
Vice President, Data Breach Resolution
Government Focus on Cybersecurity Elevates Data Breach Legislation

The use and protection of patients’ Protected Health Information (PHI) is regulated at the federal level under the Health Insurance Portability and Accountability Act (HIPAA). The law was modified in March 2013 when the HIPAA Omnibus Final Rule took effect. The omnibus rule broadens the definition of a healthcare breach to include more incidents, increases penalties and makes more entities liable for violations.

In addition, breaches affecting 500 or more individuals must be reported to major media outlets and the U.S. Department of Health and Human Services. States legislatures have also started looking at expanding their breach notification laws to include sensitive health information. For instance, California, Florida and North Dakota have enacted changes in their breach notice laws to require certain health providers to notify patients of a breach.

Breaches of consumer financial data are guided by the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice issued by bank regulatory agencies pursuant to the Gramm-Leach-Bliley Act. The Guidance requires that a financial institution notify affected customers “as soon as possible,” if the institution determines that misuse of “sensitive customer information” has occurred or is reasonably possible.

There is growing support for a federal standard, but obstacles remain

In previous legislative sessions, several bills were introduced and passed by Congressional committees aimed at forging a national data breach standard, but they ultimately failed to garner enough support to be signed into law. This can be attributed to a lack of consensus on specific issues related to the preemption of state laws, the types of personal information that if breached would trigger notification, as well as battles for jurisdiction among Congressional committees and the inclusion of other issues in the legislation. At this time, however, data breach legislation is once again a top priority for lawmakers and there will be increased debate on the issues during the 114th Congress.

In the House, this debate will be shaped, in part, by the Data Security and Breach Notification Act of 2015 (H.R. 1770), which was passed by the House Energy and Commerce Committee on April 15, 2015. While the bill has garnered support from the Committee there are several provisions that will need to be addressed during floor debates in the House. These include some issues related to the preemption provisions, as well as the structure of the penalties section of the bill. In particular, the bill, as drafted, would allow the Federal Trade Commission to move straight to civil monetary penalties for both violations of the security safeguards section and the data breach notification provisions with no advance guidance from the agency itself. The bill was amended at full committee to include a username or email address in combination with a password or security code in the definition of personal information that if breached would trigger notification. The bill will likely also define medical information as personal information by the time it reaches the House floor, as the Chairman of the Committee promised Democrats that he would consider including this to gain their support.
Debate in the Senate will emanate from the Senate Commerce Committee, the Senate Banking Committee and the Senate Judiciary Committee. Commerce Committee Ranking Member Bill Nelson (D-FL) has introduced the Obama Administration’s draft data breach bill and while it is unlikely to move forward, it is likely to play a role in any data breach and security legislation that moves forward in the upper chamber. Meanwhile, Senator Pat Toomey (R-PA) and Senate Commerce Committee Chairman John Thune (R-SD) have signaled that they intend to reintroduce their bill this Congress as well. The Senate Banking Committee is likely to consider the Data Security Act of 2015 (S. 961) that was reintroduced in April by Senators Tom Carper (D-Del.) and Roy Blunt (R-MO), as well as legislation introduced by Senator Mark Warner (D-VA).

President vocal about enacting data breach legislation
The Obama Administration has pushed for the adoption of a national uniform breach notification standard through several venues. During a speech at the Federal Trade Commission in January 2015, President Obama announced that he was putting forward draft data security and data breach legislation. The draft bill—the Personal Data Notification and Protection Act—was subsequently introduced by Senator Bill Nelson (D-FL). Meanwhile, he also used the bully pulpit of a nationally televised State of the Union address later that month to call on Congress to pass “the legislation we need to better meet the evolving threat of cyber-attacks, combat identity theft, and protect our children’s information.”

In addition to data breaches, the President has encouraged Congress to pass legislation that would support the voluntary sharing of cyber threat information. In April the House passed H.R. 1731, which emanated from the House Homeland Security Committee and is aimed at fostering greater sharing of cyber threat information by resolving liability concerns. The Senate Intelligence Committee in March passed S. 754, cyber threat information sharing legislation by a vote of 14 to 1. It has yet to be brought to the Senate floor.

FTC continues to act as enforcement body
The FTC has used its authority under Section 5 of the FTC Act, which provides the Commission with broad authority to investigate “unfair and deceptive acts and practices in or affecting commerce,” to take enforcement actions against companies that have experienced large breaches of consumer information.

Since 2001, the FTC has brought over 50 cases that accused businesses of failing to protect consumers’ personal information. Generally, in the settlements that the FTC has reached with companies in cases involving data breaches, the entities are required to implement a comprehensive information security program and undergo evaluation every two years by a certified third party.
States will continue to tinker with existing data breach laws

Even though most states already have laws on the books regarding data breach notification, State legislatures continue to consider proposals to modify them.

Legislators in several states are considering expanding existing breach notification laws by being more prescriptive about what information must be included in a notice. This may include such information as the time of the breach and the type of data affected.

As state attorneys general have gotten more involved in the oversight of breach notices, a number of states have proposed a new requirement to report breaches to the attorney general’s office. Proposals have ranged from notification in the event of any breach, no matter the size, to setting thresholds, such as the information of 500 individuals breached. State legislation also includes looking at the timing of when notices are sent out, from as soon as reasonably possible, to a more prescriptive number of days.

States legislatures are also looking at how data is secured. As the number of data breaches and the impact on consumers increase, policy makers are focused on how companies treat sensitive information. After healthcare breaches in the state, Connecticut approved a security mandate on health insurance companies, requiring organizations to implement comprehensive information security programs.

“Organizations need to stay informed about whether their state attorney general is advocating for reformed data breach notification laws, as many are pushing to expand notification to be more prescriptive and to encompass a broader definition of personal information. With ever-changing notification expectations, the bar is high for companies to stay informed and up to speed before a breach happens.”

Michael Bruemmer CHC CIPP/US
Vice President, Data Breach Resolution
Moreover, there is a growing trend to expand the types of information, which if breached, would trigger a notification to consumers. The shift in redefining what is considered sensitive information may force companies to reexamine security practices. California passed a law in 2013 that expanded the definition of the types of personal information that would trigger a breach notification to include password, user name, or security question and answer for an online account. States are also looking at notification for a breach of data that would not typically create a risk for identity theft. For example, Illinois is currently considering legislation that would take the definition of personal information beyond financial information and other key financial identifiers to less sensitive data, such as marketing information.

“...advocate for citizens by pushing for organizations to provide more protection following a data breach. While they may not be launching a cacophony of new investigations following a security incident, state regulators are using the power of the megaphone to pressure companies to take more action to protect customers.”

Michael Bruemmer CHC CIPP/US
Vice President, Data Breach Resolution

Data breach legislation addressed worldwide
The European Union (EU) is considering an expansive rewrite of the region’s data protection law that is currently working its way through the EU legislative process. The current draft would require 24 hour notification for all commercial sectors.

There are also signs that the Australian government will renew a push to enact a data breach notification standard. Following the recent passage of the data retention law — which requires telecommunication service providers to keep customer metadata for two years to aid in law enforcement — the Australian Government signaled that passing a mandatory data breach notification law by the end of 2015 is a top priority. The Privacy Amendment (Privacy Alerts) Bill 2014, was introduced in March 2014, but has yet to receive consideration. As drafted, the Bill would amend the Privacy Act of 1988 by introducing a requirement to notify the Australian Privacy Commissioner and ‘significantly affected individuals’ if a serious event of unauthorized access or disclosure of relevant information occurs.

A new data protection proposal in Brazil that was introduced in February 2015 also includes provisions related to data security and breach notification. In particular, the draft proposal would require data processors to adopt appropriate information security measures and immediately notify competent authorities of data breaches. The draft legislation is still in the early stages, but this legislation will likely continue to touch on issues related to data breach and data security.
Consumers and legislators demanding more protection from breached companies

In addition to meeting the breach notification requirements outlined by the current state and sectoral breach laws, policymakers have made clear that they expect for entities that experience a breach to take steps to further protect consumers from identity theft.

For example, in a November 2014 report on data breaches, the office of the California Attorney General noted that providing identity theft protection services, such as credit monitoring, could help to protect consumers who have had their sensitive information breached. The report states that “such services can be helpful in cases where Social Security numbers or driver’s license numbers are compromised, as they give early notice to individuals when criminals use their information to open new accounts in their name.”

At the federal level, a 2008 report by the President’s Identity Theft Task Force found that “any comprehensive information security program—whether in the public or private sector—must include policies for responding to a data breach…Such policies should address whether, how, and when to inform affected individuals of the loss of their data, and whether to offer services such as free credit monitoring to those individuals.”

“Unfortunately, data breaches are now a daily reality, and regulators and consumers alike have high expectations for businesses to be prepared to protect against fraud. Regardless of current regulatory requirements, businesses should recognize the need to go above and beyond to help customers following a breach. This will help limit the resulting impact to brand reputation by retaining customer trust and help them stay ahead of the curve on legal requirements, which will only get stricter over time.”

Michael Bruemmer CHC CIPP/US
Vice President, Data Breach Resolution
Government Focus on Cybersecurity Elevates Data Breach Legislation

Conclusion
High profile breaches of sensitive personal information that affect millions of American consumers will continue to draw the interest of policymakers on the issue of data breach.

Right now, it appears that Congress is poised to seriously consider legislation that would enact a national data breach notification requirement to replace the current segmented system of 49 state and sectoral laws. At the same time state legislators will continue to look for ways to innovate and modify existing statutes. Meanwhile other countries and global regions are adopting and considering data breach notification standards that could impact U.S. businesses that have operations overseas.

Congress will need to overcome a series of legislative hurdles before it adopts a national data breach standard during 2015, but it is important that organizations ensure compliance with existing breach notification laws. First and foremost, companies should implement pre-breach plans to deal with a data breach should it occur. Such plans are often viewed as a good defense in demonstrating that a company has established reasonable procedures to dealing with a data breach.

“Data breaches are inevitable, and regulators have an expectation that companies will respond quickly and with their customers' best interest in mind. Preparing a comprehensive incident response plan before a data breach strikes is crucial in helping avoid unnecessary complications and backlash from a breach.”

Michael Bruemmer CHC CIPP/US
Vice President, Data Breach Resolution
About Experian Data Breach Resolution

Experian Data Breach Resolution, powered by the nation’s largest credit reporting agency, is a leader in helping businesses plan for and mitigate consumer risk following data breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile breaches in history. The group offers swift and effective incident management, notification, call center support and reporting services while serving millions of affected consumers with proven credit and identity protection products. In 2013, Experian Data Breach Resolution received the Customer Service Team of the Year award from the American Business Awards. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, the Health Care Compliance Association, the American Health Lawyers Association, the Ponemon Institute RIM Council and InfraGuard and is a founding member of the Medical Identity Fraud Alliance. For more information, visit www.experian.com/databreach.