January 20, 2015

Practice Groups:

Public Policy and Law;

Cyber Law and Cybersecurity;

Investment Management, Hedge Funds and Alternative Investments;

Global Government Solutions

Cybersecurity: The Obama Administration Proposes Legislation

Proposals Would Standardize Breach Notification Requirements, Enhance Cybersecurity-Related Information Sharing, and Toughen Cybercrime Prosecution

By: R. Paul Stimers, András P. Teleki, Bruce J. Heiman, and Michael J. O'Neil

On January 13, 2015, in response to the continuing onslaught of cyber attacks, including the recent cybersecurity attack and data loss at Sony Pictures Entertainment, the Obama Administration sent to Congress three legislative proposals to improve cybersecurity. The proposals would:

- Establish a single federal breach notification standard preempting a patchwork of state notification laws;
- Encourage cyber threat information sharing within the private sector and between the private sector and the federal government; and
- Enhance law enforcement's ability to investigate and prosecute cyber crimes.

The President has been highlighting the cybersecurity proposals in a series of speeches leading up to the State of the Union Address today.

New Federal Breach Notification Requirements

The Administration's breach notification bill would attempt to provide a single federal breach notification standard, preempting the patchwork of state laws that businesses currently must navigate when they suffer an electronic data breach. It also would make FTC enforcement, rather than state Attorney General enforcement, preeminent. The bill also would give the FTC broad rulemaking authority and clarify that the FTC can enforce the bill using its FTC Act enforcement powers. Although preemption to establish a single national standard for data breach notifications has long been a goal of many in industry, the additional federal powers and broad requirements in the bill are likely to be less well-received by the business community. Significantly, the bill would not preclude a private right of action, which has been an industry goal. Finally, the bill would not address what role the federal functional regulators such as the Federal Reserve, OCC, SEC, and CFTC will have with respect to their constituents regarding compliance and enforcement in this area.

The Breach Notification Framework. The notification requirement would apply broadly to businesses that access, transmit, store, dispose of, or collect "sensitive personally identifiable information" about more than 10,000 individuals during any 12-month period. "Sensitive Personally Identifiable Information" is defined very broadly and exceeds the definition of "personally identifiable information" that currently appears in a number of federal and state regulations.

Under the bill, following the discovery of a security breach of sensitive personally identifiable information, the business would be required to notify any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual and certain conditions have been met by the business (i.e., the business has conducted a risk assessment that concludes that there is no reasonable risk of harm, and the business notifies the FTC in writing of the results of the risk assessment and its decision to invoke the exemption).

The burden of proof will be on the affected company to conduct a risk assessment to determine whether that conclusion is supportable and to report that conclusion to the FTC. The bill also includes a rebuttable presumption that there is no such risk if the data was encrypted or otherwise unusable. A second exemption would apply if the business used a security program that "effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual and provides notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions."

With few exceptions, all notifications must be made without "unreasonable delay" following the discovery by the business of a security breach - generally no later than 30 days regardless of the size of the breach or the information at risk – a provision that industry will undoubtedly seek to tighten to prevent over-reporting. For larger breaches or in special circumstances, companies would also have to notify credit reporting agencies and various law enforcement agencies. Federal law enforcement agencies may, subject to certain conditions, require businesses to delay notifications in cases where such notification would impede a criminal investigation or national security activity.

Other Requirements. The bill sets forth the methods of notice, as well as the content of the notice, and contemplates e-mail notice, if the individual has "consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of [E-Sign]." The bill also contemplates companies entering into contractual arrangements that specify which entity would provide the requisite notice in the event of a breach.

The bill provides one exception to its data breach notification standards. They would not supersede the data breach notification requirements for breaches involving protected health information governed by the Health Information Technology for Economic and Clinical Health Act, which would remain in effect for covered entities, business associates and vendors of personal health records, and third-party service providers, which themselves are strict and provide for detailed notifications.

Information Sharing

The Administration's information sharing bill would offer companies civil and criminal liability protection in an effort to encourage them to share information about cyber threats and vulnerabilities. The proposal designates the newly authorized National Cybersecurity and Communications Information Center as a clearinghouse for this information. In an attempt to address privacy concerns, it would require companies to make reasonable efforts to redact sensitive personally identifiable information before sharing, but privacy advocates have expressed concerns that this provision is too vague. They also are concerned about excessive sharing of information among government agencies.

Cybersecurity: The Obama Administration Proposes Legislation

Proposals Would Standardize Breach Notification Requirements, Enhance Cybersecurity-Related Information Sharing, and Toughen Cybercrime Prosecution

Law Enforcement

The Administration's law enforcement proposals include expanding federal powers to prosecute the sale of botnets and to shut down criminal botnets; criminalizing the overseas sale of stolen financial sensitive personally identifiable information; updating the Racketeering Influenced and Corrupt Organizations (RICO) Act to apply to cybercrime; and updating the Computer Fraud and Abuse Act to apply to insider hacking, while limiting criminal prosecutions based on violations of terms of service. The last law to update cybercrime enforcement was enacted several years ago.

Congressional Reaction and Prospects

President Obama has stated that cybersecurity is an area in which he and the Republican-controlled House and Senate can work together (in addition to trade and tax). Speaker Boehner has responded that House and Senate Republicans would work with the President and their Democratic counterparts to address the issue. He noted that the House has passed a number of cybersecurity bills that have failed to pass the Senate in recent years.

Senator John Thune (R-SD), who has just assumed the Chairmanship of the Senate Commerce Committee, suggested that the President was late to the discussion but welcomed his participation on the issue. Breach notification bills were considered but not passed in the 113th Congress. Senate Commerce Committee Ranking Member Bill Nelson (D-FL) followed the Administration's announcement with word that he would introduce a data breach notification bill that would complement the Administration's proposal while meeting the Administration's goals. His bill would be a modified version of the Data Security and Breach Notification Act that he and several Democratic colleagues introduced in the 113th Congress. Senator Chuck Grassley (R-IA), who now chairs the Senate Judiciary Committee, also announced plans to introduce data breach legislation. An information sharing bill passed the House in the 113th Congress. A Senate version was reported out of the Intelligence Committee but did not pass the Senate due to privacy concerns.

Conclusion

Although this bill is not likely to be the last salvo in the cybersecurity and data protection fight, it offers a view into the current Administration's thinking on the questions of what constitutes sensitive personally identifiable information, how a federal breach notification regime may look, and the circumstances under which reporting would not be required at the federal level. It also adds fuel to the fire for congressional action in this area.

Cybersecurity: The Obama Administration Proposes Legislation

Proposals Would Standardize Breach Notification Requirements, Enhance Cybersecurity-Related Information Sharing, and Toughen Cybercrime Prosecution

Authors:

R. Paul Stimers
paul.stimers@klgates.com
+1.202.661.3883

András P. Teleki
andras.teleki@klgates.com
+1.202.778.9477

Bruce J. Heiman
bruce.heiman@klgates.com
+1.202.661.3935

Michael J. O'Neil
mike.oneil@klgates.com
+1.202.661.6226

Additional Contacts:

Holly K. Towle
holly.towle@klgates.com
+1.206.370.8334

Robert E. Feyder
robert.feyder@klgates.com
+1.310.552.5023

Roberta D. Anderson
roberta.anderson@klgates.com
+1.412.355.6222