Sony and Epsilon on the 'Hot Seat': House Commerce Subcommittee Investigates 'Historic' Data Breaches

Dana B. Rosenfeld, Alysa Z. Hutnik

June 3, 2011

On June 2, 2011, the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade held a hearing examining threats to data security and historic data breaches at Sony and Epsilon. The hearing, "Sony and Epsilon: Lessons for Data Security Legislation" focused on the recent Epsilon and Sony data breaches and the need for comprehensive federal data security and data breach notification legislation. The representatives and witnesses discussed the delays in Sony's notification, the extent of the breaches and the prospect for federal legislation.

In attendance at the hearing were Subcommittee Chairwoman Rep. Mary Bono Mack (R-CA), Ranking Member Rep. G.K. Butterfield (D-NC), Rep. Cliff Stearns (R-FL), Rep. Brett Guthrie (R-KY), Rep. Gregg Harper (R-MS), and Rep. Pete Olson (R-TX). Tim Schaaff, President of Sony Network Entertainment International, and Jeanette Fitzgerald, General Counsel for Epsilon Data Management LLC, each testified.

Sony and Epsilon Data Breaches

By way of background, on April 1, 2011, Epsilon Data Management, an email marketing company, announced on its website unauthorized access to their servers, exposing consumer names and email addresses to hackers. The breach affected 75 of Epsilon's business customers, including Best Buy, Capital One, Kroger, Target and Verizon, and ultimately affected more than 60 million consumers. A few weeks later, on April 22, 2011, Sony's PlayStation Network announced that a data breach occurred on April 19, 2011, exposing names, email addresses, passwords, physical addresses, and birthdates of over 77 million consumers. A little over a week later, on May 2, 2011, Sony announced that on May 1, 2011 its Online Entertainment network was breached, exposing personal information on over 25 million consumers. These high-profile data breaches prompted an ongoing Congressional inquiry in the form of a series of letters from Chairwoman Bono Mack and Ranking Member Butterfield to Sony and Epsilon leading up to the June 2nd hearing. In the immediate wake of their data breaches, Sony and Epsilon declined to testify at a May 4, 2011 Subcommittee hearing on data theft and data security.

Lessons Learned for Federal Data Breach Legislation

On June 2, 2011, the Subcommittee had the opportunity to question Sony and Epsilon under oath. Rep. Bono Mack opened by noting that for her the "most troubling" aspect of the Sony data breach was the time it took for Sony to notify consumers and the way that Sony initially notified consumers through a blog posting. Representatives Bono Mack, Butterfield and Harper pressed Sony on why it

took so long to notify consumers of the breach. Sony initially notified PlayStation users on April 22 via blog post, and subsequently on April 26 notified users by direct email notice (which took several days to complete). Mr. Schaaff testified that it took Sony time to identify that a breach occurred, noting that Sony thought it would be "irresponsible" to notify consumers with inaccurate information as Sony investigated the full extent of the breach. Rep. Bono Mack was concerned that Sony's initial notice via blog post placed the burden on consumers to learn that a breach occurred. Mr. Schaaff defended this action because its blog was a popular source of information for PlayStation users and that Sony followed up by notifying users with more detailed information by direct email and public announcements, once it had more complete information. Further, Sony responded by providing its customers with free credit monitoring.

The representatives also inquired on the extent of the damage caused by the data breaches. Rep. Butterfield pressed Mr. Schaaff on whether credit card information for PlayStation users was breached. Mr. Schaaff testified that there is no evidence in its database logs to suggest that that credit card information was accessed and, further, that credit card information was encrypted in line with industry practices. In response to a question from Rep. Stearns, Ms. Fitzgerald indicated that Epsilon's breach exposed information on millions of Verizon's customers, a client of Epsilon's. Epsilon only notified its business customers such as Verizon, not the consumers whose information was jeopardized. In response to a question from Rep. Guthrie, Mr. Schaaff estimated that the data breach would cost Sony around $170 million.

The representatives asked Sony and Epsilon representatives about their thoughts on federal data breach legislation. In response to a question from Rep. Guthrie, Mr. Schaaff noted the burdens imposed on companies to comply with often conflicting state notification requirements. Mr. Schaaff and Ms. Fitzgerald supported a federal data breach notification law that would preempt state laws, including specifications on who companies need to notify and when they need to notify.

At the hearing, Rep. Bono Mack called for a "uniform national standard" for data security and data breach notification, announcing her intent to introduce legislation based on "three guiding principles," including:

1. Companies that maintain personal information must have security policies in place to prevent unauthorized access to sensitive data;

2. Especially sensitive data, such as credit card numbers, must have more robust safeguards; and

3. Consumers must be promptly notified of data breaches.

Congressional Data Security and Privacy Initiative

The hearing is part of a comprehensive review of data security and electronic privacy initiated by the House Energy and Commerce Committee that was announced on June 1, 2011. According to the Committee press release, the first phase of the Committee's review will focus on online data security and data theft prevention, followed later in the year by a focus on broader electronic privacy concerns. Data security and data privacy legislation has been gaining traction in Congress. Most recently, Rep. Bobby Rush (D-IL) introduced the Data Accountability and Trust Act, which would require data security policies and mandate national consumer data breach notification. There also has been a flurry of activity on the data privacy front with a number of bills circulating on Capitol Hill, including Rep. Stearns' and Rep. Jim Matheson's (D-UT) Consumer Privacy Protection Act of 2011, Rep. Rush's BEST PRACTICES Act, Rep. Jackie Speier's (D-CA) Do Not Track Me Online Act and

Senators John Kerry's (D-MA) and John McCain's (R-AZ) Commercial Privacy Bill of Rights Act of 2011.

Conclusion

In the wake of the much publicized data breaches at Sony and Epsilon, companies are reminded of the increasing need to exercise the utmost due diligence in the collection and retention, and security of sensitive data. On June 2, 2011, the same day Sony testified at the hearing, hackers claimed responsibility for yet another data breach at Sony, purportedly accessing personal information on some 52,000 Sony customers. These security issues however extend beyond Sony and Epsilon. Mr. Schaaff asserted that data breach issues discussed at the hearing apply to everyone because all networks are built out of the same basic components. The hearing built on the growing record in Congress supporting data security and data breach notification legislation that could ultimately supersede the current patchwork of state laws.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

Kelley Drye's Government Relations and Public Policy Practice Group helps clients interpret and shape governing laws, enabling them to achieve and maintain market leadership. The varied backgrounds of its government relations lawyers and professionals enable the team to handle a variety of clients needs including representation and strategic planning.

For more information about this advisory, contact:

Dana B. Rosenfeld
(202) 342-8588
drosenfeld@kelleydrye.com

Alysa Zeltzer Hutnik
(202) 342-8603
ahutnik@kelleydrye.com