Hughes Hubbard & Reed

Recent Data Breaches May Spur Congressional Action on Data Regulations

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

In the wake of the recently publicized data breach involving Sony's PlayStation and Online Entertainment networks, Congress appears ready to accelerate its efforts to enact legislation to implement regulations intended to prevent future breaches and provide a framework for enforcement in the event of a breach. The data breaches at Sony, which occurred on two separate occasions (at the end of April and then again at the beginning of May), involved more than 100 million accounts. The data that was leaked included information about PlayStation subscribers such as names, addresses, emails, passwords, usernames, birthdays, phone numbers and purchase histories. Sony is not the first, and unfortunately will likely not be the last, to be subject to such attacks. To date, the largest data breaches include up to 130 million credit card numbers stolen from Heartland Payment System in 2009, up to 100 million accounts from retailer TJX in 2005 and 2006, and more than 4.2 million credit and debit card numbers from the grocery chain Hannaford Bros. in 2008. Recently, at e-mail marketing firm Epsilon, there was asignificant data breach which affected about 50 of its business customers. And just this week it was revealed that a software flaw may have enabled third party applications operating within Facebook to leak user account information. These incidents have renewed concerns on Capitol Hill about how companies are responding to data breaches, especially in connection with notifying customers that their information may have leaked. Both Sony and Epsilon sent written responses to questions posed by a House subcommittee on their handling of the breaches. Lawmakers appear to recognize that, although security measures may be in place, they are not always fully implemented. House Energy and Commerce Committee members have questioned whether U.S. businesses are taking the necessary steps to protect their data. According to Pablo Martinez, a deputy special agent in charge of the Criminal Investigative Division at the U.S. Secret Service, in nearly all data breaches, the subject company had not taken reasonable precautions. A 2010 report found that 96% of breaches were, in fact, avoidable through simple or intermediate controls". In determining how to begin drafting a comprehensive and effective bill to regulate data breaches, several lawmakers said they planned to use the Data Accountability and Trust Act (2009) (DATA Act), as their starting point. Although introduced and passed by the House, the DATA Act was put to a vote in the Senate. If passed, the Act would have required organizations holding personal data to maintain security policies and to notify affected consumers after a data breach. It addressed the following three major concerns:

information security requirements for personal information in general; information security requirements for personal information for 'information brokers'; and breach notice obligations. Although the majority of states have enacted data breach laws, the DATA Act proposed an allowance for civil penalties of up to $11,000 per violation (up to $5 million) and each failure to send the required notification to an affected individual would be treated, under the Act, as a separate violation. The risk of such considerable penalties set forth in the Act would surely encourage compliance. On the other hand, there seemed to appear to be certain clauses within the DATA Act that could have led to even less breach reporting. With regard to breach notice obligations, the bill required that potential victims of identity theft be notified whenever their electronically stored personal information was exposed. Had it been passed, the law would preempt all state laws (not just state laws that are less stringent or contrary to the Act) and would be the first of its kind. All competing state law standards would therefore be eliminated, ultimately leading to less forum shopping. Furthermore, the standard ("risk of harm") set forth in the DATA Act falls on the higher end of the spectrum as compared to the standards set forth in some state laws which would most likely lead to less frivolous lawsuits. A major concern with the DATA Act was that it could only be implemented by the FTC. This was problematic as there are numerous companies and organizations that the FTC does not have jurisdiction over including banks, common carries and nonprofits. In order to be effective and worthwhile, the new bill will have to be drafted so that it is not only enforceable by the FTC but by other governmental entities as well. Other apprehension stemmed from the fact that the bill provided that breaches would not have to be reported if the organization in question determined that "there is no reasonable risk of identity theft, fraud, or other unlawful conduct". The bill also granted an exemption if the breached information was encrypted or protected by any other technologies that, according to the FTC, renders data unreadable. As expected, lawsuits over the Japanese electronics giant's breach have started to come out of the woodworks. The first suit came a day after Sony acknowledged the breach. The complaint, filed in the Northern District Court of California, alleges that Sony failed to take "reasonable care to protect, encrypt and secure the private and sensitive data of its users" which prevented PlayStation Network users from being able to "to make an informed decision as to whether to change credit card numbers, close the exposed accounts, check their credit reports, or take other mitigating actions". The suit seeks monetary compensation and free credit card monitoring. A second suit, which claims damages in excess of $1 billion (Canadian dollars), was filed by a Toronto-based law firm on behalf of a 21-year-old plaintiff and names Sony Japan, Sony USA, Sony Canada and other Sony entities as defendants. The aftermath of these recent incidents may prove to be a useful lesson and may expedite the development of better security technology and practices in the private sector and perhaps even force Congress and the FTC to finally pass a bill that will afford sufficient protection to consumers' personal data. We will continue to monitor the ongoing developments in privacy and security legislation and its potential impact on our clients.

Related Areas of Focus

Media, Technology & Commercial Transactions