The high price of data breaches

November 26 2011, By James Cole

As consumers, we transmit valuable personal information to the companies with which we do business. In doing so, we trust that information will remain secure. Over the past year, however, we have learned of a number of instances in which vast quantities of personal data have been compromised. Last spring, for instance, breaches at Sony Corp. affected more than 100 million customers, putting their credit card numbers, email addresses and passwords at risk. Another recent breach exposed email addresses of customers of companies such as Best Buy, Citibank, Disney, JPMorgan Chase, the Home Shopping Network, Hilton, Marriott and the College Board.

Although we often think of credit card numbers as being among the most sensitive personal information, disclosure of email addresses and passwords can in some cases allow identity thieves to do us more harm. Because many people use the same passwords for different accounts - an inadvisable but common practice - knowledge of an email address and password for one account may give an identity thief access to other accounts, to social network profiles, or even to the contents of email accounts. With one breach, identity thieves may gain access to nearly all sensitive information that a person stores electronically.

When companies disclose breaches of personal data, as Sony did, consumers can take steps to reduce the damage caused by the breach. They can strengthen passwords, change credit card numbers, put fraud alerts on their credit reports, and keep a close watch on their bank accounts. A 2006 study commissioned by the Federal Trade Commission found that the earlier consumers discovered the identity theft, the less

time it took to resolve the crime, and the less money thieves were able to steal. Early notification can mean the difference between a few hours of effort or months of stress and worry for identity theft victims.

Prompt notification also enables law enforcement officials to more swiftly and effectively investigate and prosecute the perpetrators of the identity theft. Last year, law enforcement officials successfully prosecuted an individual who stole more than 90 million credit and debit card numbers by hacking the payment systems of several U.S. retailers. He was sentenced to 20 years in prison - the lengthiest sentence imposed in the United States for identity theft. Such successful prosecutions not only provide justice to victims, but also may deter would-be identity thieves from stealing personal data in the future.

Forty-seven states have laws that require companies to notify consumers in the event of a breach of their personal information. These laws have helped consumers mitigate the risks of identity theft and have created incentives for companies to improve their cybersecurity. But this patchwork of state laws is not enough. Not all states require data breach notification, and the existence of multiple standards makes compliance unnecessarily difficult and more costly for companies.

In May, the administration proposed a broad-ranging cybersecurity bill that would address this problem by imposing a single notification standard for companies nationwide. The bill would require companies to provide timely notice to their customers when their personal information is compromised. The bill also would require companies to report data breaches to the federal government to help law enforcement go after identity thieves before the digital evidence disappears. And the bill would authorize enforcement by the Federal Trade Commission and state attorneys general, giving companies real incentive to comply.

There is strong bipartisan consensus in Congress for cybersecurity

reform. A Republican task force in the House published a report last month on the pressing need to improve cybersecurity. The Senate also has been working hard to move forward with cybersecurity reform. During a mid-October meeting with leaders from the administration, a bipartisan group of senators agreed to work together to pass a cybersecurity bill as quickly as possible.

We need Congress to act promptly. The Privacy Rights Clearinghouse has been tracking data breaches since 2005 and now lists more than 540 million records of personal information breached. Congress should require companies to comply with a national data breach notification requirement and hold them accountable to consumers and the marketplace. When breaches occur that put personal information at risk, notification helps protect consumers and punish identity thieves who undermine society's trust in cyberspace and put our economic prosperity at risk.

More information: James Cole is U.S. deputy attorney general. Readers may write to him at: U.S. Department of Justice, 950 Pennsylvania Avenue NW, Washington, D.C. 20530.