No consensus on how to notify data breach victims

March 9 2014, by Eric Tucker

In this Feb. 4, 2014, file photo, Peter Swire, of the Review Group on Intelligence and Communications Technology, testifies before the House Judiciary Committee's hearing on Recommendations to Reform FISA Authorities, on Capitol Hill in Washington. A massive data breach at Target Corp. that exposed tens of millions of credit card numbers has focused attention on a patchwork of state consumer notification laws and renewed a push for a single national standard. "We're stuck with the state-by-state approach unless some compromise gets done at the federal level," said Swire, a privacy expert at Georgia Tech and a former White House privacy official.(AP Photo/Cliff Owen, File)

(AP)—The data breach at Target Corp. that exposed millions of credit card numbers has focused attention on the patchwork of state consumer notification laws in the U.S. and renewed a push for a single national standard.

Most U.S. states have laws that require retailers to disclose data breaches, but the laws vary wildly. Consumers in one state might learn immediately that their personal information had been exposed, but that might not happen in another state, and notification requirements for businesses depend on where their customers are located. Attorney General Eric Holder has joined the call for a nationwide notification standard, but divisions persist, making a consensus questionable this year.

"We're stuck with the state-by-state approach unless some compromise gets done at the federal level," said Peter Swire, a privacy expert at Georgia Tech and a former White House privacy official.

Despite general agreement on the value of a national standard, there are obstacles to a straightforward compromise:

—Consumer groups don't want to weaken existing protections in states with the strongest laws.

—Retailers want laws that are less burdensome to comply with and say too much notification could cause consumers to tune out the problem.

—Congress is looking at different proposals for how any federal standard should be enforced and what the threshold should be before notification requirements kick in.

The issue gained fresh urgency as part of a larger security debate after data breaches involving retailers Neiman Marcus and Target. Target, the second-largest U.S. retail discounter, has said 40 million credit and debit card accounts were exposed between Nov. 27 and Dec. 15.

The company went public with the breach on Dec. 19, several days after it said it learned of the problem and soon after the news began leaking online. Since then, sales, profit and stock prices have dropped, the company's chief information officer has resigned and banks and retailers are facing continued scrutiny about what more can be done to protect consumer data.

This Dec. 19, 2013, file photo shows a Target retail chain logo on the exterior of a Target store in Watertown, Mass. A massive data breach at Target Corp. that exposed tens of millions of credit card numbers has focused attention on a patchwork of state consumer notification laws and renewed a push for a single

national standard. (AP Photo/Steven Senne, File)

The Justice Department is investigating the data theft, and Holder urged Congress in a video statement last month to adopt a national notification standard that would include exemptions for harmless breaches.

"This would empower the American people to protect themselves if they are at risk of identity theft. It would enable law enforcement to better investigate these crimes and to hold compromised entities accountable when they fail to keep sensitive information safe," he said in the statement.

Such proposals have been around for years.

An Obama administration plan from 2011 would have required businesses that collect personal information on more than 10,000 people in any 12-month period to disclose potentially harmful breaches and for breaches that affect more than 5,000 people to be reported to consumer credit reporting agencies and the federal government.

Past congressional efforts to agree on a standard have failed. Currently, 46 states and the District of Columbia have their own breach notification laws, according to the National Conference of State Legislatures.

Proposals now before Congress would require notification. But there are differences in what information the notification would provide, the threshold for notifying regulators and law enforcement, and the proposed enforcement. Some bills seek criminal penalties for deliberately concealing a breach; others do not.

Consumer groups fear that any national standard could turn out to be

weaker than the strongest state laws, such as one in California that requires a business or state agency to notify any state resident whose data was improperly obtained. Other state laws are more lenient, requiring notice only in cases where a risk analysis determines that the breach is likely to have actually harmed consumers.

"From industry's perspective, whether you're a bank or a merchant, you don't want to have to notify consumers," said Ed Mierzwinski, consumer program director at the U.S. Public Interest Research Group. "They want to pre-empt, or override, the best state laws."

Retailers say they do support a federal notification standard but one that would be triggered when sensitive material has been exposed—as opposed to, say, customers' shoe sizes—and when there's a risk that it will be used for theft or fraud.

"There are different kinds of data. There's data that can lead to an identity theft (or) financial fraud, and there's data that probably doesn't have much utility to the criminals," said David French, senior vice president for government relations at the National Retail Federation. "If you get 20 notices a month, at some point you just turn it off."

Meanwhile, retailers remain at odds with financial institutions over how best to protect consumer data. Retailers say banks need to upgrade security technology on the credit cards they issue. Banks say retailers need to do more to enhance their own security.

"There's no agreement in the private sector among the major players about what their responsibilities are, and that makes it more difficult for us in the Congress to end up on the same page," said Sen. Tom Carper, chairman of the Senate Homeland Security and Governmental Affairs committee, in an interview.

He is sponsoring legislation that provides for notification in cases where there is "substantial risk" of identity theft or account fraud.

Carper said he's hoping for a solution, because the "alternative is a patchwork quilt that is a nightmare."