Target data breach pits US banks against retailers

February 4 2014, by Marcy Gordon

In this Monday, Feb. 3, 2014 photo, Sen. Mark Warner, D-Va., chairman of the Senate Banking Subcommittee on National Security and International Trade and Finance, displays his personal bank card as he leads a hearing on the recent incidents of mass credit card fraud in Washington. The hearing comes following the theft of consumers' data at retailers such as Target Corp and Neiman Marcus during the holiday shopping season. (AP Photo/J. Scott Applewhite)

Banks and America's big retailers are locked in a debate over the massive breach of millions of consumers' data that gripped Target Corp. during the holiday season. At issue: Which industry bears more responsibility for protecting consumers' personal information?

The retailers' argument: Banks must upgrade the security technology for the credit and debit cards they issue. The banks' counterargument: Newer electronic-chip technology wouldn't have prevented the Target breach. And retailers must tighten their own security systems for processing card payments.

An estimated 40 million credit and debit card accounts were affected by the Target breach, which occurred between Nov. 27 and Dec. 15. Stolen were customers' names, credit and debit card numbers, card expiration dates, debit-card personal identification numbers and the embedded codes on the cards' magnetic strips.

Also stolen was non-card personal information—names, phone numbers and email and mailing addresses—for up to 70 million Target customers who could have shopped before or after the Nov. 27-Dec. 15 period.

The Target theft could prove to be the biggest data breach on record for a U.S. retailer. Minneapolis-based Target, the No. 2 U.S. discounter, has acknowledged that news of the breach has scared some shoppers away. The company last month cut its earnings outlook for its fourth quarter, which covers the crucial holiday season. It warned that sales would be down for the period.

The two industries are pointing fingers at each other. Each has considerable lobbying might. Their trade groups have been bombarding lawmakers with letters arguing why the other industry must do more—and spend more—to protect consumers.

"Nearly every retailer security breach in recent memory has revealed some violation of industry security agreements," the Independent Community Bankers argued last month. "In some cases, retailers haven't even had technology in place to alert them to the breach intrusion, and third parties like banks have had to notify the retailers that their information has been compromised."

The National Retail Federation has fired back:

Retailers must accept "fraud-prone cards" issued by banks that are attractive to thieves, the federation's general counsel testified at a Senate subcommittee hearing Monday. "Unlike the rest of the world, the U.S. cards still use a signature and magnetic stripe for authentication."

Their antagonism aside, the two sides agree on one point: That Congress should create a national standard for notifying consumers of any data breaches. A uniform standard would replace the current hodgepodge of state guidelines.

In the middle are American consumers, many of whom say they're alarmed about the safety of their personal information since the Target breach. In an Associated Press-GfK poll conducted Jan. 17-21, nearly half of those surveyed said they've become extremely concerned about the vulnerability of their personal data when shopping in stores since the incident.

This week, Congress is examining data security breaches and what to do about them. Four committees have scheduled hearings.

At a Senate Judiciary Committee hearing Tuesday, the head of the Federal Trade Commission and officials from the Secret Service and the Justice Department are set to testify. So are executives of Target and luxury retailer Neiman Marcus.

Still unknown is how the malicious software that was used to carry out the theft got into Target's computer system and how the hackers stole credentials from a Target vendor to enter the system. The identity of the vendor isn't known, either. The Secret Service has been investigating, and Attorney General Eric Holder has said the Justice Department is conducting a criminal probe to find those responsible.

Retailers are trying to shore up consumers' confidence by upgrading and testing their systems for accepting payments. But their trade association says the billions that merchants are spending won't prevent breaches unless the banks adopt more secure card technology.

The banks plan to put digital chips for storing account information on debit and credit cards by the fall of 2015. Compared with the current magnetic strips, it's a system that typically makes data theft harder and is common in other countries. This would be a step forward but hardly a guarantee against cyber attacks, the banks caution.

Retailers want the chips, but they also want each debit or credit card transaction to require a personal identification number instead of a signature. Experts say it's harder for criminals to steal personal identification numbers than to forge signatures.

The magnetic strips use the same technology as cassette tapes to store account information and are easy to copy. By contrast, a digital chip generates a unique code each time it's used. Criminals can steal and sell data from cards with chips, but they can't create fraudulent cards.

© 2014 The Associated Press. All rights reserved.

Citation: Target data breach pits US banks against retailers (2014, February 4) retrieved 7 May 2024 from https://phys.org/news/2014-02-breach-pits-banks-retailers.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.