U.S. House of Representatives
Committee on Science, Space, and Technology

HEARING CHARTER

Healthcare.gov: Consequences of Stolen Identity

Thursday, January 16, 2014
9:00 a.m. – 11:00 a.m.
2318 Rayburn House Office Building

Purpose

On Thursday, January 16, 2014, the Committee on Science, Space, and Technology will hold a hearing titled, *Healthcare.gov: Consequences of Stolen Identity.* This hearing will be a follow-up from the Committee's November 19, 2013 hearing on the security concerns of the Healthcare.gov website.[1] At that hearing, expert witnesses raised concerns about the vulnerabilities and risks to the privacy and security of Americans' personal information. Today's hearing will provide the Committee with an updated security assessment to determine the likelihood of personal information being accessed or compromised because of an attack on Healthcare.gov. It will also examine the consequences of identity theft to Americans if hackers with malicious intent gained personal information through the Healthcare.gov website, which is one of the largest collections of personal information ever assembled, linking social security numbers, birth dates, and tax and other financial information of its users.

Witnesses

- **Mr. David Kennedy**, Chief Executive Officer, TrustedSEC, LLC
- **Mr. Waylon Krush**, Co-Founder and CEO, Lunarline, Inc.
- **Mr. Michael Gregg**, Chief Executive Officer, Superior Solutions, Inc.
- **Dr. Lawrence Ponemon**, Chairman and Founder, Ponemon Institute

Overview

On November 19, 2013, the Committee held a hearing to assess the security of data on Healthcare.gov where witnesses raised numerous concerns about the lack of security and privacy standards for personal information passing through the website. When asked whether Healthcare.gov had been compromised by hackers, one witness testified that he believed the website already has been hacked or soon will be. In addition, all of the witnesses agreed that Healthcare.gov is not secure. When the witnesses were asked if they would have launched the website, the unanimous answer was "No." Further, when the witnesses were asked if they would require front-end personal data disclosure on the site, again, all four responded "No." Lastly, each of the experts said taking down Healthcare.gov should be seriously considered to address the security concerns raised.

[1] House Committee on Science, Space and Technology hearing, "*Is My Data on Healthcare.gov Secure*," November 19, 2013, available at: http://science.house.gov/hearing/full-committee-hearing-my-data-healthcaregov-secure.

Congressional investigations into the flawed website have identified varying degrees of concern among those involved in developing the website prior to its launch last October. A Centers for Medicare and Medicaid Services (CMS) memo on the Federally Facilitated Marketplaces (FFM) System from September 3, 2013 noted that "[t]here is the possibility that the FFM security controls are ineffective,"[2] and that "[i]neffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise."[3] Later that month, a memo addressed to CMS Administrator Marilyn Tavenner stated, "From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM."[4] Further, a former senior security expert at CMS stated last month that she recommended against launching the Healthcare.gov website on October 1, 2013 because of "high risk security concerns."[5]

Despite an improved ability for Americans to log on and create accounts in their search for healthcare plans since the flawed October 1st launch, it is unclear how much has been done to address the types of privacy and security concerns raised over the past few months. Since the data on Healthcare.gov is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies[6] along with state agencies and government contractors, a security breach would be devastating to the millions of Americans forced by Administration regulations to enroll in health insurance plans through the website. Without proper security measures in place, participants are vulnerable to hackers who might be able to access such personal information, leaving them to deal with the consequences that come along with identity theft.

Issues

Target…and others

To understand what a potential data breach of the Healthcare.gov website could mean to the American public, it is useful to review the recent hacking of Target department stores' online billing information. Initially, Target reported that "payment data was stolen from about 40 million customers"[7] who shopped in its U.S. stores over the holiday season. But upon further review of the exposure, last week Target "revised the number of customers whose personal information was stolen…now reporting a range of 70 million to 110 million people."[8]

---

[2] CMS Memo, "Authorization Decision for the Federal Facilitated Marketplaces (FFM) System," available at: http://oversight.house.gov/wp-content/uploads/2013/11/9.3.13-Trenkle.pdf.

[3] Ibid.

[4] Memo to Marilyn Tavenner from James Kerr and Henry Chao, "Federally Facilitated Marketplace – DECISION," September 27, 2013, available at: http://www.scribd.com/doc/180332001/CMS-Memo-on-Marketplace-Security.

[5] House Oversight and Government Reform Committee press release, "CMS Officials Launched Healthcare.gov Against Warning Agency's Top Cybersecurity Official," December 20, 2013, available at: http://oversight.house.gov/release/cms-officials-launched-healthcare-gov-warning-agencys-top-cybersecurity-official.

[6] The seven agencies are: Internal Revenue Service, Social Security Administration, Department of Homeland Security, Department of Defense, Department of Veterans Affairs, Office of Personnel Management and Peace Corps; See Stacy Cowley, "How Obamacare's 'privacy nightmare' database really works," CNN.com, July 24, 2013, available at http://money.cnn.com/2013/07/23/technology/security/obamacare-privacy.

[7] Elizabeth Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow," The New York Times, January 10, 2014, available at: http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0.

[8] Ibid.

While original reports noted the theft of credit and debit cards as well as PIN data from bank ATM cards, the recent disclosure includes more personal information such as "mailing and email addresses, phone numbers or names, the kind of data routinely collected from customers during interactions like shopping online or volunteering a phone number when using a call center."[9]

In a December 22nd letter to the Federal Trade Commission calling for an investigation of the Target breach, Senator Richard Blumenthal (D-Conn.) stated, "Those Target customers who have their data misused by hackers or thieves could lose their good credit and in turn their ability to purchase the goods and services they need for their wellbeing and the wellbeing of their families. Even customers whose stolen data will never ultimately be misused must live with the fear and uncertainty of knowing that it could be."[10]

It is important to note that besides the Target data breach, media reports from this past weekend identified retailer Neiman Marcus as also experiencing network breaches over the holiday season.[11] Additionally, smaller "breaches on at least three other well-known U.S. retailers took place and were conducted using similar techniques as the one on Target."[12]

Experian

The credit bureau and consumer data tracking service Experian provides "the identity verification component of the Health Insurance Marketplace enrollment process."[13]

Experian also offers data breach services to companies through its Experian Data Breach Resolution arm. According to a recent Experian report, data breach incidents in the healthcare industry will rise in 2014 with the addition of the insurance exchange:

> *"With the addition of the Healthcare Insurance Exchanges, millions of individuals will be introduced into the healthcare system and in return increase the vulnerability of the already susceptible healthcare industry. When combined with new HIPAA data breach compliance rules taking shape, the healthcare industry is likely to make the most breach headlines in 2014."*[14]

---

[9] Ibid.

[10] Senator Richard Blumenthal press release, "In Response To Massive Data Breach, Blumenthal Calls For FTC Investigation Into Target Security Practices," December 22, 2013, available at: http://www.blumenthal.senate.gov/newsroom/press/release/in-response-to-massive-data-breach-blumenthal-calls-for-ftc-investigation-into-target-security-practices-.

[11] Jim Finkle and Mark Hosenball, "Exclusive: More Well-Known U.S. Retailers Victims of Cyber Attacks – Sources," Reuters, January 12, 2014, available at: http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112.

[12] Ibid.

[13] Experian website, "Information about Experian's role in the Health Insurance Marketplace," available at: http://www.experian.com/help/health-insurance-marketplace-verification.html?intcmp=hcinfo_hp.

[14] Experian Data Breach Resolution, "2014 Data Breach Industry Forecast", available at: http://www.experian.com/assets/p/data-breach/experian-2014-data-breach-industry-forecast.pdf.

GAO Report

Last month, the U.S. Government Accountability Office (GAO) released a report in which it reviewed issues related to personally identifiable information (PII) data breaches in the government.[15] GAO reviewed the policies and procedures of eight federal agencies, including CMS, and determined that the agencies "inconsistently implemented"[16] policies for "responding to a data breach involving PII that addressed key practices specified by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology."[17]

Further, according to the report, a "data breach can leave individuals vulnerable to identity theft or other fraudulent activity. Although federal agencies have taken steps to protect PII, breaches continue to occur on a regular basis. In fiscal year 2012, agencies reported 22,156 data breaches - an increase of 111 percent from incidents reported in 2009,"[18] with 4,172 incidents reported at CMS.

Consequences of Stolen Identity

When a data breach occurs and an individual's identity is stolen, then that information can be used to make purchases, obtain medical care, or for some other nefarious purpose. In 2013, 1.84 million Americans became victims of medical identity theft, with the total out-of-pocket cost incurred at $12.3 billion.[19] This cost included identity protection, legal counsel, and reimbursements to healthcare providers for fraudulent medical services. There is also a significant amount of time and effort spent on remedying the situation. In addition to the financial and time burden, in cases of medical identity theft, there is the risk that medical record inaccuracies created by an imposter may be unknown or may become permanent, potentially putting victims' lives at risk.

One example of medical identity theft in the U.S. involves a woman named Anndorie Sachs. After receiving a phone call one day stating that her newborn baby had tested positive for drugs, authorities arrived at her house the next day threatening to take her other children away from her for being an unfit mother. In reality, Ms. Sachs had not given birth in years, but someone stole her information and had a baby under her name. Ms. Sachs had to take a DNA test to prove that it was not she who gave birth at the hospital, deal with the $10,000 hospital bill, and live in fear over "the long-term damage that may have been done to her medical records."[20]

---

[15] GAO report, "Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent," December 9, 2013, available at: http://www.gao.gov/products/GAO-14-34.
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Ponemon Institute, "2013 Survey on Medical Identity Theft," available at: http://medidfraud.org/2013-survey-on-medical-identity-theft.
[20] Caitlin Johnson, "Protect Against Medical ID Theft," CBSNews.com, October 9, 2006, available at: http://www.cbsnews.com/news/protect-against-medical-id-theft.