WRITTEN TESTIMONY

BEFORE THE

SENATE COMMITTEE ON THE JUDICIARY

HEARING ON

PRIVACY IN THE DIGITAL AGE:

PREVENTING DATA BREACHES AND COMBATING CYBERCRIME

FEBRUARY 4, 2014

TESTIMONY OF

JOHN MULLIGAN

EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER

TARGET

I. Introduction

Good morning Chairman Leahy, Ranking Member Grassley, and Members of the Committee. My name is John Mulligan and I am the Executive Vice President and Chief Financial Officer of Target. I appreciate the opportunity to be here today to discuss important issues surrounding data breaches and cybercrime.

As you know, Target recently experienced a data breach resulting from a criminal attack on our systems. To begin, I want to say how deeply sorry we are for the impact this incident has had on our guests – your constituents. We know this breach has shaken their confidence in Target, and we are determined to work very hard to earn it back.

At Target we take our responsibility to our guests very seriously, and this attack has only strengthened our resolve. We will learn from this incident and as a result, we hope to make Target, and our industry, more secure for consumers in the future.

I'd now like to explain the events of the breach as I currently understand them. Please recognize that I may not be able to provide specifics on certain matters because the criminal and forensic investigations remain active and ongoing. We are working closely with the U.S. Secret Service and the U.S. Department of Justice on the investigation – to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.

II. What We Know

On the evening of December 12, we were notified by the Justice Department of suspicious activity involving payment cards used at Target stores. We immediately started our internal investigation.

On December 13, we met with the Justice Department and the Secret Service. On December 14, we hired an independent team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, had installed malware on our point-of-sale network and had potentially stolen guest payment card data. That same day, we removed the malware from virtually all registers in our U.S. stores.

Over the next two days, we began notifying the payment processors and card networks, preparing to publicly notify our guests and equipping our call centers and stores with the necessary information and resources to address the concerns of our guests.

On December 18 we disabled malware on about 25 additional registers which were disconnected from our system when we completed the initial malware removal on December 15. As a result, we determined that fewer than 150 additional guest accounts were affected.

Our actions leading up to our public announcement on December 19 – and since – have been guided by the principle of serving our guests, and we have been moving as quickly as possible to share accurate and actionable information with the public. When we announced the intrusion on December 19 we used multiple forms of communication, including a mass-scale public announcement, email, prominent notices on our website, and social media channels.

What we know today is that the breach affected two types of data: payment card data which affected approximately 40 million guests and certain personal data which affected up to 70 million guests. The theft of the payment card data affected guests who shopped at our U.S. stores

from November 27 through December 18. The theft of partial personal data included name, mailing address, phone number or email address.

We now know that the intruder stole a vendor's credentials to access our system and place malware on our point-of-sale registers. The malware was designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

As the forensic investigation continued, we learned that the malware also captured some strongly encrypted PIN data. We publicly shared this information on December 27, reassuring our guests that they would not be responsible for any fraudulent charges that may occur as a result of the breach.

When we subsequently confirmed the theft of partial personal data on January 9, we used various channels of communication to notify our guests on January 10 and provide them with tips to guard against possible scams.

III. Protecting Our Guests

From the outset, our response to the breach has been focused on supporting our guests and strengthening our security. In addition to the immediate actions I already described, we are taking the following concrete actions:

- First, we are undertaking an end-to-end review of our entire network and will make security enhancements, as appropriate.
- Second, we increased fraud detection for our Target REDcard guests. To date, we have not seen any fraud on our Target proprietary credit and debit cards due to this breach. And we have seen only a very low amount of additional fraud on our Target Visa card.

- Third, we are reissuing new Target credit or debit cards immediately to any guest who requests one.
- Fourth, we are offering one year of free credit monitoring and identity theft protection to anyone who has ever shopped at our U.S. Target stores. This protection includes a free credit report, daily credit monitoring, identity theft insurance and unlimited access to personalized assistance from a highly trained fraud resolution agent.
- Fifth, we informed our guests that they have zero liability for any fraudulent charges on their cards arising from this incident. We encouraged them to monitor their accounts and promptly alert either Target or their issuing bank of any suspicious activity.
- Sixth, Target is accelerating our investment in chip technology for our Target REDcards and stores' point-of-sale terminals. We believe that chip-enabled technologies are critical to providing enhanced protection for consumers, which is why we are a founding, and steering committee, member of the EMV Migration Forum at the SmartCard Alliance.
- Seventh, Target initiated the creation of, and is investing $5 million in, a campaign with Better Business Bureau, the National Cyber Security Alliance and the National Cyber-Forensics & Training Alliance to advance public education around cybersecurity and the dangers of consumer scams.
- And, eighth, last week Target helped launch a retail industry Cybersecurity and Data Privacy Initiative that will be focused on informing public dialogue and enhancing practices related to cybersecurity, improved payment security and consumer privacy. Target will be an active leader in this effort.

For many years, Target has invested significant capital and resources in security technology, personnel and processes. We had in place multiple layers of protection, including

firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools. We perform internal and external validation and benchmarking assessments. And, as recently as September 2013, our systems were certified as compliant with the Payment Card Industry Data Security Standards.

But, the unfortunate reality is that we suffered a breach, and all businesses – and their customers -- are facing increasingly sophisticated threats from cyber criminals. In fact, recent news reports have indicated that several other companies have been subjected to similar attacks.

IV. Moving Forward

To prevent this from happening again, none of us can go it alone. We need to work together.

Updating payment card technology and strengthening protections for American consumers is a shared responsibility and requires a collective and coordinated response. On behalf of Target, I am committing that we will be an active part of that solution.

Senators -- to each of you, and to all of your constituents and our guests, I want to say once again how sorry we are that this has happened. We will work with you, the business community, and other thought leaders to find effective solutions to this ongoing and pervasive challenge. Thank you very much for your time today.