WRITTEN TESTIMONY

BEFORE THE

SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

HEARING ON

PROTECTING PERSONAL CONSUMER INFORMATION FROM CYBER ATTACKS AND DATA BREACHES

MARCH 26, 2014

2:30 PM

TESTIMONY OF

JOHN MULLIGAN

EXECUTIVE VICE PRESIDENT AND CHIEF FINANCIAL OFFICER

TARGET

I. Introduction

Good afternoon Chairman Rockefeller, Ranking Member Thune, 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 experienced a data breach in late 2013 resulting from a criminal attack on our systems. Let me reiterate how deeply sorry we are for the impact this incident has had on our guests – your constituents. Our top priority is taking care of our guests. They should feel confident about shopping at Target. We work hard to protect their information. But the reality is we experienced a data breach. Our guests expect more and we are working hard to do better. We know this has shaken their confidence and we intend to earn it back.

We are asking hard questions about whether we could have taken different actions before the breach was discovered that would have resulted in different outcomes. In particular, we are focused on what information we had that could have alerted us to the breach earlier; whether we had the right personnel in the right positions; and ensuring that decisions related to operational and security matters were sound. We are working diligently to answer these questions.

This afternoon, I'd like to provide an update since I last testified, including actions we are taking to further strengthen our security and potential policy solutions we support. Because the government's investigation regarding the intruders remains active and ongoing, I may not be able to provide specifics on certain matters. We continue to work closely with the U.S. Secret Service and the U.S. Department of Justice – to help them bring to justice the criminals who perpetrated this wide-scale attack on Target, American business and consumers.

II. What We Know

We are further strengthening our data security based on learnings from an end-to-end review of our systems. We are not finished with that review, and additional facts may affect our findings, but we are certainly developing a clearer picture of events and want to share with you some key facts we have learned.

Like any large business, we log a significant number of technology activities in our system – more than 1 billion on average each day. These activities range from relatively insignificant, such as a team member logging onto a laptop, to more significant, such as removal of a virus from a computer. Using technology tools, those activities are narrowed to a few hundred events that are surfaced to the professionals staffing our Security Operations Center (SOC). As a result of their review of these events, dozens of cases are opened daily for additional assessment.

It appears that intruders entered our system on November 12. We now believe that some intruder activity was detected by our computer security systems, logged and surfaced to the SOC and evaluated by our security professionals. With the benefit of hindsight and new information, we are now asking hard questions regarding the judgments that were made at that time and assessing whether different judgments may have led to different outcomes.

We believe that the intruders initially obtained an HVAC vendor's credentials to access the outermost portion of our network. We are still investigating how the intruders were able to move through the system using higher-level credentials to ultimately place malware on Target's point-of-sale registers. The malware appears to have been designed to capture payment card data from the magnetic strip of credit and debit cards prior to encryption within our system.

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 Secret Service. On December 14, we engaged an outside team of experts to lead a thorough forensic investigation.

On December 15, we confirmed that criminals had infiltrated our system, installed malware on our point-of-sale network and 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 call centers and stores with the necessary information and resources to address our guests' concerns.

Our actions leading up to our public announcement on December 19 – and since – have been guided by the principle of serving our guests. We moved quickly 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.

Additionally, when we subsequently confirmed the theft of certain personal data, we used various channels of communication to notify our guests on January 10.

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 personal data included name, mailing address, phone number or email address, and in many cases, it was partial in nature.

It is difficult to develop an accurate assessment of overlap between these two types of data, due in part to the partial nature of the information related to the file of 70 million individuals. Our analysis indicates there is an overlap of at least 12 million guests in the two populations, and likely more.

III. Protecting Our Guests

From the outset, our response to the breach has been focused on supporting our guests and taking action to further protect them against constantly evolving cyber threats. We are taking a hard look at security across the network. While we don't know everything yet, we have initiated the following steps to further protect our perimeter and better secure our data:

Segmentation. We are increasing the segmentation and separation of key portions of our network by enhancing the protections provided by the firewalls we have in place to limit unauthorized traffic. This is about making it more difficult to move across our network.

Whitelisting. We continue to strengthen our anti-virus tools, and accelerated the installation of a whitelisting solution on our registers. Whitelisting protects guests by detecting malicious applications and stopping them from running on our registers and gives us another tool to prevent malware from taking root and spreading in our environment. This is about limiting what can run on our network.

Authentication. We are strengthening our network perimeter by expanding two-factor authentication for entry into the system. This is about double locking the door.

Beyond these technology responses, we need to ensure the right people, with the right experience, are in the right place. That's why we are also taking a hard look at our organization, with the intention of bolstering our information security structure and practices.

- Earlier this month, Target became the first retailer to join the Financial Services Information Sharing and Analysis Center (FS-ISAC), an initiative developed by the financial services

industry to help facilitate the detection, prevention, and response to cyber attacks and fraud activity. Target was eligible to join the organization because of its financial operations. During my testimony to Congress in February, I stressed Target's commitment to more coordinated information sharing with law enforcement and others fighting cyber threats, in order to help make our company, partners and guests more secure. Joining the FS-ISAC underscores Target's position that the retail and financial industries have a shared responsibility to collaborate and strengthen protection for American consumers.

- We are accelerating our $100 million investment in the adoption of chip technology because we believe it is critical to enhancing consumer protections. We have already installed approximately 10,000 chip-enabled payment devices in Target stores and expect to complete the installation in all Target stores by this September, six months ahead of schedule. We also expect to begin to issue chip-enabled Target REDcards and accept all chip-enabled cards by early 2015. As a founding member and steering committee member of the EMV Migration Forum, we will continue to lead the adoption of these technologies across the payment ecosystem.
- We continue to reissue new Target credit or debit cards immediately to any guest who requests one.
- We continue to offer 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 fraud resolution agent.
- We have informed our guests that they have zero liability for fraudulent charges on their cards arising from this incident. To ensure our guests are protected, we continue to

encourage them to monitor their accounts and promptly alert either Target or their issuing bank, as appropriate, of any suspicious activity.

IV. Moving Forward

For many years, Target has invested significant capital and resources in security technology, personnel and processes. Prior to the data breach, we had in place multiple layers of protection, including firewalls, malware detection software, intrusion detection and prevention capabilities, and data loss prevention tools. We performed internal and external validation and benchmarking assessments. And, in September 2013, our systems were certified compliant with the Payment Card Industry Data Security Standards, meaning that we met approximately 300 independent requirements of the assessment. Yet the reality is that our systems were breached.

To prevent this from happening again, none of us can go it alone. All businesses – and their customers – are facing frequent and increasingly sophisticated attacks by cybercriminals. Protecting American consumers is a shared responsibility and requires a collective and coordinated response. Target remains committed to being part of the solution.

V. Conclusion

I want to once again say to the Members of this Committee and our guests how sorry we are that this happened. We are determined to get things right. Thank you.