Written Questions for the Record of Chairman Leahy
for John J. Mulligan
Executive Vice President and Chief Financial Officer
Target Corporation
February 11, 2014

1. At the February 4, 2014 hearing, you testified that Target suffered two data breaches: The first affected the payment information of approximately 40 million customers. A second data breach affected the sensitive personal information of approximately 70 million customers.

    a. Did both of these data breaches involve the same malware and the same perpetrator(s)? Please explain.

    Chairman Leahy, I appreciate the opportunity to clarify the details surrounding the breach and the impacted data. We have consistently stated that the breach affected two types of data: payment card data which affected approximately 40 million guests and partial 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. The intruder also accessed partial personal data for up to 70 million guests. This partial personal data included name, address, email address and telephone number.

    While the investigation is still active and ongoing, we believe the same attacker is responsible for the theft of both sets of data.

    b. Vast amounts of stored consumer data can become an attractive target for cyber thieves. Does Target store its customers' personally identifiable information on its computer systems? If so, what steps does Target take to protect this sensitive data from data breaches or other cyber attacks?

    Target stores its guests' data on its computer systems. For many years, Target has invested significant capital and resources in security technology, personnel and processes, including firewalls, malware detection software, intrusion detection and prevention capabilities and data loss prevention tools. We perform internal and external validation and benchmarking assessments. Target's last assessment for compliance with the Payment Card Industry Data Security Standards ("PCI DSS") was completed on

September 20, 2013 by Trustwave. On that date, Trustwave certified Target as compliant with PCI DSS.

c. Does Target notify its customers about the company's policy on the collection and retention of customer data?

At Target, we want our guests to know how we collect, use, share, and protect information about them. By interacting with Target, our guests consent to use of information that is collected or submitted as described in our privacy policy (link to our privacy policy included below).

http://www.target.com/spot/privacy-policy#?lnk=fnav_t_spc_2_2&intc=28074|null

d. Do Target customers have the ability to opt out of any program involving the collection or retention of their personal information?

We provide our guests with choices about receiving marketing from Target and sharing of personal information with other companies for their marketing purposes. Our privacy policy provides our guests with information related to the collection, use, sharing and protection of information about them.

http://www.target.com/spot/privacy-policy#?lnk=fnav_t_spc_2_2&intc=28074|null

2. During the hearing, you discussed your support for so-called "Chip and Pin" technology for point of sale transactions.

a. When do you anticipate that Target will adopt Chip and Pin technology at its stores?

At Target, we've been working for years towards adoption of this technology. Since the breach, we are accelerating our own $100 million investment to put chip-enabled technology in place. Our goal is to implement this technology in our stores and on our proprietary REDcards by early 2015, more than six months ahead of our previous plan.

b. Do you have any concerns about this technology?

For consumers, this technology differs in important ways from what is widely used in the United States today. The standard credit and debit cards we use now have a magnetic stripe containing account information. When first introduced, that stripe was an innovation. But in today's world, more is needed. The latest "smart cards" have tiny microprocessor chips that encrypt the personal data shared with the sales terminals used by merchants. This change is important because even if a thief manages to steal a smart

card number, it's useless without the chip.

In addition, requiring the use of a four-digit personal identification number (PIN) to complete a sales transaction would provide even greater safety. While there is no consensus across the business community on the use of PINs in conjunction with chip-enabled cards, Target supports the goal and will work toward adoption of the practice in our own stores and more widely.

In the United Kingdom, where smart card technology is widely used, financial losses associated with lost or stolen cards are at their lowest levels since 1999 and have fallen by 67 percent since 2004, according to industry estimates. In Canada, where Target and others have adopted smart cards, losses from card skimming were reduced by 72 percent from 2008 to 2012, according to industry estimates.

c. Has Target explored any other payment processing methods to help protect the privacy of sensitive financial and consumer data during the payment process?

Target is investing in solutions that will make mobile transactions more secure. We know work is needed to strengthen protections for e-commerce, an important long-term goal. In the meantime, adopting chip-enabled cards would be a clear step in the right direction.

3. Has the investigation into the data breach at Target prompted any changes in Target's security of online transactions or stored customer data? If so, please explain.

In addition to the active and ongoing criminal investigation, we are in the midst of a comprehensive, end-to-end review of our entire network. It is our expectation that the findings from the internal review will provide us with opportunities to make security enhancements as appropriate.

"Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime."
Questions for the Record Submitted by
Ranking Member Charles E. Grassley of Iowa,
February 11, 2014.

Questions for Mr. John Mulligan and Mr. Michael Kingston

1. The recent attack your company suffered highlights the problem with the current patchwork of state notification laws. There are differing views whether a federal breach notification standard should serve as a "floor" or preempt the current breach notification laws. Given your recent experience with issuing notification, please discuss the following:

    a. How would a federal notification standard that permits states to include additional requirements have affected the company during the wake of the breach?

    There is much debate surrounding a federal breach notification standard and while I do not want to speculate about the appropriate path Congress should take, I can speak to our actions. We provided substitute notice, including by (1) posting notice on our website; (2) providing notice by e-mail to each relevant guest for whom we had an e-mail address; and (3) providing notice to nationwide and state media. Of the various aspects of our substitute notice, only e-mail was provided directly to specific guests. In this regard, we provided notice by e-mail to each relevant guest for whom we had an e-mail address.

    In general, Target's efforts to provide substitute notice were the same with respect to guests residing in all States. For example, Target posted notice on its website for all guests, not just guests residing in certain States. In addition, Target sent information to news media in every State. In Massachusetts and Texas, however, Target took out paid notices in statewide newspapers, as provided for by relevant State law.

    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. 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 email, prominent notices on our website, and social media channels.

    b. What would the approach have been if a federal uniform notification standard was in place that fully preempted current notification laws?

Target's priority was to provide accurate and actionable notification to our guests.

c. What impact would the two different approaches have on a company's resources as compared to the other, i.e., full preemption versus a federal standard that serves as a "floor"?

We have not determined the impact on our resources if a federal standard were in place.

d. Is current law preferable to either of the approaches discussed above?

There is much debate surrounding a federal breach notification standard, and I would defer to Congress on the appropriate policy in this area.

2. In the Congress there are several data breach notification proposals, all of which differ from the other. One important consideration is that of timing for issuing notification. Some legislation requires notice of a breach be issued as soon as possible; another says within 48 hours of discovery. Please describe the general process involved in issuing notice to consumers, including a consideration whether statutory time frames for issuing notifications would be helpful or harmful.

I understand that Congress is considering various legislative proposals. Regardless of the outcome, Target will continue to comply with applicable notification laws. As for the process involved as we prepared to notify our guests, I can share the following:

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.

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 email, prominent notices on our website, and social media channels.

3. Another significant issue concerns the penalties associated with a company's failure to comply with any notification requirements. Do you believe that providing criminal – as opposed to civil – penalties for failing to notify consumers would be helpful or harmful? Why?

Target's priority was on providing accurate and actionable information to our guests. We are not in a position to speculate on the impact of criminal penalties for failing to notify consumers.

4. Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses and/or anything else that came up at the hearing, which you did not have a chance to respond to.

Thank you for the opportunity to appear before your Committee.