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.