"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.