Written Questions for the Record of Chairman Leahy
for Fran Rosch
Senior Vice President
Security Products and Services, Endpoint and Mobility
Symantec Corporation
February 11, 2014

1. During the February 4, 2014 hearing, you testified about steps that American retailers could take to better protect customer data from data breaches and cyber attacks.

    a. In your view, what are the key steps that retailers should take to safeguard consumer data during the payment process for point of sale transactions?

    There are a number of key steps that companies can take to secure consumer data during point of sale (PoS) transactions. First, it is critical that retailers implement Payment Card Industry (PCI) Data Security Standards (DSS). This includes installing a firewall to facilitate network segmentation, changing default system passwords, encrypting cardholder data as it passes through the company's systems, regularly updating security software, and using strong authentication including two-factor authentication for remote systems. We also recommend the use of file integrity and monitoring software to monitor all network and data access points. Finally, companies should lock down the PoS devices themselves by restricting their operations to only those required to perform their functions, and by restricting what software can be installed on them.

    Second, we recommend the adoption of point to point encryption (P2PE) technology which will protect consumer credit card data from "RAM scraping" attacks. Most systems today encrypt consumer data as that data move across the network; however sensitive information still sits in plain text within the memory banks of the PoS system making it highly vulnerable. By implementing P2PE, retailers can ensure that all consumer data is encrypted from the moment a customer swipes their card until the moment that information is received by the payment card processing company.

    Finally, good security is not just about the technology. Threats are always evolving, so it is important that companies view security as a continuing responsibility that integrates people, processes and technology.

    b. What about during the payment process for online purchases?

    Retailers need to ensure that they are using secure, encrypted communications channels, and should provide assurances to their customers that they are doing so. Encryption is enabled by "SSL digital certificates" which are issued by "Certificate Authorities," – a trusted third party that "vouches" for the identity of the business. There are different classes of certificates, however, and the most

secure is called Extended Validation (EV) certificate. EV certificates are only issued to the website after the business has undergone an extensive validation process by the Certificate Authority. EV certificates cause the address bar in popular browsers to turn green, a visual cue to consumers that they are dealing with a trusted vendor.

Once a retailer has obtained payment information, it should be treated like any other highly sensitive personal information – kept on highly secure servers and encrypted whether the data is at rest or in transit.

2. In your experience, where are data breaches involving payment card data most likely to occur today -- during "point of sale" transactions, or during online transactions?

   Although many of the recent data breaches in the news involved point of sale systems that does not mean either environment is more or less susceptible to attack. Criminals will continue to adapt to our every move and will try to exploit all users and systems to get what they want – when PoS systems are made more secure, they will look to other avenues to steal information. The best we can do is to make it harder for them to access sensitive data by ensuring that it is protected and secured to the highest degree possible. This means using encryption, stronger passwords, employing company-wide cybersecurity policies, patching systems, and using the latest generation computer security software.

3. Do you anticipate the trend of data breaches involving point of sale transactions will continue, given the recent data breaches involving American retailers?

   Yes, for a time. Cyber criminals have a business model – that is, they are in it to make money. These criminals will continue to develop new and adaptive ways to breach systems and steal sensitive financial information from consumers. Right now, they've been effective at compromising some PoS systems, and they will continue to do that until we make it too difficult – and costly – to do so. Once that happens, they will shift their methods.

"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. Fran Rosch

1. In your written testimony, you stated that it is important for a federal breach notification law to minimize "false positives," i.e., issuing notice to individuals who are later shown not to have been impacted by a breach. I share this concern because over-notification can also be harmful as it might lead to consumer apathy. Could you please share your thoughts and advice for the following:

    a. Discuss what we should consider when drafting legislation that minimizes the risk of "false positives"?

    Data breaches are complex events, and it can take a significant amount of forensic work to determine what data was stolen. In determining whether an individual has indeed been meaningfully impacted, there are two essential considerations: first, what data was stolen, and second was that data encrypted or otherwise rendered unusable. As to the first point, companies hold a variety of information about people, and while all of it should be protected, only some of it can be used to commit financial crimes or identity theft. Notification may be necessary if the information that was taken can individually or in the aggregate lead to a financial loss, identity theft, or fraud. As to the second point, an organization must determine if the information stolen is in fact usable. If it was properly encrypted or otherwise rendered unusable it should not be necessary for a company to notify users because they are not at risk for fraud or identity theft.

    b. How can we strike the right balance for notification so that companies understand when to issue notice, and consumers are armed with the information they need to monitor the potential for harm?

    We believe that while companies should produce information about a breach in a timely manner, they should have time to engage law enforcement, investigate the breach and repair the vulnerability. Every breach is different and it is important that companies are given the time to analyze what happened so that they provide the public the most accurate information and minimize the risks of "false positives." Notification should be made as expeditiously as possible, but as long as companies are acting in good faith to assess the extent of the data breach and determine how to repair the vulnerability, a company should not be required to notify individual customers until it verifies that those customers were impacted and that the vulnerability has been patched, so as not to further expose other data or systems.

2. In your written testimony, you noted that data breach notification legislation should apply equally to all. Do you also support the position that a federal breach notification standard should preempt the current patchwork of state breach notification laws? If so, explain why preemption is so important?

    Today there are at least 48 state-specific data breach notification laws. This creates an enormous compliance burden, particularly for smaller companies that have to try to

comply with myriad and often conflicting standards. This current situation does nothing to offer additional protection to consumers, and in fact can create confusion when residents of different states receive different information about the same breach. A federal standard should create uniformity for consumers and businesses alike, and avoid confusing, even contradictory consumer notices.

3. 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.

   Symantec appreciates the opportunity to testify on this important issue, and looks forward to assisting the Committee in any way possible in the future.