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.