**"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.