FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

March 4, 2015

Ms. Elizabeth Hyman
Executive Vice President
Public Advocacy
CompTIA
515 2nd Street, N.E.
Washington, D.C. 20002

Dear Ms. Hyman,

Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Tuesday, January 27, 2015 to testify at the hearing entitled "What are the Elements of Sound Data Breach Legislation?"

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Wednesday, March 18, 2015. Your responses should be e-mailed to the Legislative Clerk in Word format at **Kirby.Howard@mail.house.gov** and mailed to Kirby Howard, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Michael C. Burgess
Chairman
Subcommittee on Commerce,
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

Additional Questions for the Record

The Honorable Michael C. Burgess

1. The President recently called for a single, national standard for breach notification legislation. Do you have a response to the language he proposed? Please discuss.

2. The President recently called for a single, national standard for breach notification legislation. Do you have a response to the language he proposed? Please discuss.

3. Given the activity of States regulating data security in the last few years, is there a benefit for industry if Congress sets a national standard for reasonable data security? Would you support a preemptive reasonable data security standard? Please explain.

4. Would your members support data security and breach notification legislation that does not contain preemption of State law?

5. How do you define preemption that would effectively eliminate the existing patchwork of State laws?

6. How do you believe state common law should be treated in federal data security and breach notification legislation? Should it be preempted?

7. Please explain the issues that could develop in the marketplace if a federal data security and breach notification bill does not preempt State law.

8. Do you support allowing State Attorneys General to enforce a federal data security and breach notification law if the law preempts current State law? Are there other factors that should be considered in extending this enforcement authority?

9. There was testimony during the hearing that companies undertake investigations after a breach is discovered. Please explain the steps of a data breach investigation and what information companies learn during this process.

10. The dangers of over notification for consumers in the long term have been outlined by States, companies, and the Federal Trade Commission. Taking this issue into consideration, what should the risk trigger be for a company to notify individuals after a breach?

11. If there is a deadline for notification following a breach, should the clock start after the breached entity has been able to secure and restore the breached system? How do the States approach this in their breach notification statutes?

12. What are cyber attackers typically looking for when they attempt to breach your members' networks? Do you know if the purpose is typically to embarrass the consumer or to steal his or her information for financial gain?