

ONE HUNDRED FIFTEENTH 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

December 5, 2017

Mr. James Norton
Adjunct Lecturer
Johns Hopkins University Zanvyl Krieger School of Arts and Sciences
1717 Massachusetts Avenue, N.W.
Washington, DC 20036

Dear Mr. Norton:

Thank you for appearing before the Subcommittee on Digital Commerce and Consumer Protection on, Wednesday, November 1, 2017, to testify at the hearing entitled "Securing Consumers' Credit Data in the Age of Digital Commerce."

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 Tuesday, December 19, 2017. Your responses should be mailed to Ali Fulling, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to ali.fulling@mail.house.gov.

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

Sincerely,



Robert E. Latta
Chairman
Subcommittee on Digital Commerce
and Consumer Protection

cc: Jan Schakowsky, Ranking Member, Subcommittee on Digital Commerce and Consumer Protection

Attachment

Additional Questions for the Record

The Honorable David McKinley

1. What is the one most important thing companies like Equifax should do to enhance our confidence in their ability to keep sensitive data secure?
2. What is the one most important thing Congress should do?
3. Is social media becoming an increasingly effective tool for cyber criminals? In September after Equifax publicly disclosed the breach, Equifax repeatedly tweeted the wrong URL for its consumer protection website. Is that an example of cyber-criminal exploiting social media for nefarious purposes?
4. What kind of new data security developments should CEOs, Chief Information Security Officers, and Chief Information Officers and indeed everyone be aware of?