Congress of the United States
Washington, DC 20515

November 18, 2014

Abigail P. Johnson
Chief Executive Officer
Fidelity Investments
82 Devonshire Street
Boston, MA 02109

Dear Ms. Johnson:

USA Today recently ran a front-page story reporting that 500 million records have been stolen from various financial institutions as a result of cyber-attacks over the past year, according to federal law enforcement officials. The report stated:

> Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building.[1]

The report explained that law enforcement officials believe the "U.S. financial sector is one of the most targeted in the world." They warned that nearly "439 million records have been stolen in the past six months," and that approximately "80% of hacking victims in the business community didn't even realize they had been hacked until they were told by investigators." If a business is hacked, law enforcement officials urged companies to work closely with government entities "rather than trying to keep the attack quiet and deal with it internally."[2]

According to filings with the Securities and Exchange Commission, JPMorgan Chase recently reported that it was the victim of a data security breach that compromised account holder names, addresses, and phone numbers, but not necessarily passwords.[3] Multiple press accounts reported that the hackers who breached JPMorgan Chase's data security systems may also have attempted to breach security protections at other financial institutions.[4]

The increasing number of cyber-attacks and data breaches is unprecedented and poses a clear and present danger to our nation's economic security. Each successive cyber-attack and

---

[1] *Officials Warn 500 Million Financial Records Hacked*, USA Today (Oct. 21, 2014) (online at www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029/).

[2] *Id.*

[3] JPMorgan Chase & Co., *Form 8-K Current Report* (Oct. 2, 2014) (online at www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm).

[4] *See, e.g., JPMorgan Hackers Said to Probe 13 Financial Firms*, Bloomberg (Oct. 9, 2014) (online at www.bloomberg.com/news/2014-10-09/jpmorgan-hackers-said-to-probe-13-financial-firms.html).

data breach not only results in hefty costs and liabilities for businesses, but exposes consumers to identity theft and other fraud, as well as a host of other cyber-crimes. Your ability to protect consumers and safeguard their personal information is central to earning and maintaining consumer confidence in our economic system.

The increased frequency and sophistication of cyber-attacks on both public and private entities highlights the need for greater collaboration to improve data security. Your company's knowledge, information, and experience will be helpful as Congress examines federal cybersecurity laws and any necessary improvements to protect sensitive consumer and government information.

To aid in this oversight, we are writing to inquire whether your company was the subject of a cyber-attack over the past year. If so, we request that you provide the following information:

(1) a description of all data breaches your company has experienced over the past year, including the date and the manner and method by which your company first discovered the breaches, the dates the breaches are believed to have begun and ended, and the types of data breached;

(2) the approximate number of customers that may have been affected by the breaches, and the manner in which customers were notified of the breaches;

(3) the findings from forensic investigative analyses or reports concerning the breaches, including findings about vulnerabilities to malware, the use of data segmentation to protect personally identifiable information, and why the breaches went undetected for the length of time they did;

(4) the individuals or entities suspected or believed to have caused the data breaches, and whether they have been reported to the appropriate law enforcement agencies;

(5) a description of data protection improvement measures your company has undertaken since discovering the breaches;

(6) an estimate of the number and value of fraudulent transactions that were connected to the data breaches, including the approximate number of federal, state, and local government customers whose information was exposed during the data breaches at issue, as well as the number and value of fraudulent transactions that were connected to federal, state, and local government customers exposed in the data breaches;

(7) a description of the data security policies and procedures that govern your relationships with vendors, third-party service providers, and subcontractors, including the manner by which your company ensures that entities performing work on your behalf have reasonable data security controls in place to thwart cyber-attacks; and

(8) any recommendations for improvements in cybersecurity laws or the coordination of efforts to identify and respond to emerging trends in cybersecurity risks to help prevent future data breaches.

Please provide the requested information by December 19, 2014. We also request a briefing from your Chief Information Security Officer or similar chief IT security professional by December 8, 2014. If you have any questions about this request, please contact Timothy D. Lynch at (202) 225-0312. Thank you for your cooperation with this matter.

Sincerely,

Elijah E. Cummings
Member of Congress

Elizabeth Warren
United States Senator