Congress of the United States
Washington, DC 20515

November 18, 2014

Michael L. Corbat
Chief Executive Officer
Citigroup
399 Park Avenue
New York, NY 10043

Dear Mr. Corbat:

We are writing to request information about data breaches your company may have experienced over the past year and your company's administration of purchase and charge cards to federal agencies under a contract with the General Services Administration (GSA).

Over the past year, multiple retailers have reported significant breaches of data associated with purchase cards used at their stores.[1] In addition to compromising the purchase cards of tens of millions of American consumers, they may have compromised charge cards your company issues to federal employees under an agreement with GSA.

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.[2] 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.[3]

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 data breach not only results in hefty costs and liabilities for businesses, but puts consumers at risk of identity theft and the unauthorized use of their charge cards. Your ability to protect consumers and safeguard their personal information is central to earning and maintaining consumer confidence in our economic system.

---

[1] *See. e.g., Home Depot Data Breach Could Be the Largest Yet*, New York Times (Sept. 8, 2014) (online at http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0); *Target Cyber Breach Hits 40 Million Payment Cards at Holiday Peak*, Reuters (Dec. 19, 2013) (online at www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219).

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

[3] *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).

The increased frequency and sophistication of cyber-attacks on both public and private sector 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 financial information.

For these reasons, 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;

(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;

(9) the approximate number of fraudulent transactions, including the amounts involved, that your company has identified or become aware of to date that were connected to federal government purchase or charge cards that were exposed as part of any third-party data breach between November 2013 and the present;

(10) oversight reports your company has provided to GSA within the past two years pursuant to master contracts with that agency;

(11) investigations, assessments, or studies regarding the impact that data breaches have had on any purchase or payment cards your company has issued to federal employees under contracts with GSA; and

(12) policies, procedures, or contractual agreements that govern the liability of GSA or any other federal agency for any fraudulent activity that is found to have occurred on any government purchase or charge cards that were compromised.

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