ELIZABETH WARREN
MASSACHUSETTS

COMMITTEES:
BANKING, HOUSING, AND URBAN AFFAIRS
HEALTH, EDUCATION, LABOR, AND PENSIONS
ARMED SERVICES
SPECIAL COMMITTEE ON AGING

United States Senate

UNITED STATES SENATE
WASHINGTON, DC 20510–2105
P: 202–224–4543

2400 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
P: 617–565–3170

1550 MAIN STREET
SUITE 406
SPRINGFIELD, MA 01103
P: 413–788–2690

www.warren.senate.gov

August 8, 2019

Richard D. Fairbank
Chairman and Chief Executive Officer
Capital One Financial Corporation
1680 Capital One Drive
McLean, VA 22102

Dear Mr. Fairbank,

I write regarding the July 29, 2019, announcement of the massive data breach that compromised sensitive personal information – including, in some cases, Social Security numbers and bank account numbers – of over 100 million Capital One customers. I am deeply troubled by this breach –"one of the largest-ever thefts of data from a bank"[1] – and I ask that you explain how the database was breached, including how the hacker was able to enter Capital One's systems and which security systems failed or were insufficient to protect consumer data, what steps Capital One has taken to fix both the specific vulnerability the hacker exploited and the systems that failed to detect the breach, and what efforts Capital One's will make to rectify the impact of the breach on the millions of people whose data were exposed.

Beginning in March 2019, Capital One's database was breached and a hacker was able to obtain the personal data of more than 100 million people, mostly related to credit card applications.[2] While some of the stolen data were encrypted or tokenized, the hacker was able to decrypt data and access names, phone numbers, and addresses, as well as over a hundred thousand Social Security numbers and tens of thousands of bank account numbers.[3]

Public reports suggest that the circumstances of the breach were not unique or unforeseeable. According to press reports, Ms. Paige Thompson has been arrested and charged with illegally

---

[1] New York Times, "Here's What You Need to Know About the Capital One Breach," David Yaffe-Bellany, July 30, 2019, https://www.nytimes.com/2019/07/30/business/capital-one-breach.html.
[2] CBS News, "What we know so far about Capital One hacker Paige Thompson," Stephen Gandel, July 31, 2019, https://www.cbsnews.com/news/paige-thompson-what-we-know-about-accused-capital-one-breach-hacker-2019-07-31/.
[3] PCWorld, "100 million Capital One credit card applications hacked: What you need to know (and do next)," Michael Simon, July 30, 2019, https://www.pcworld.com/article/3428616/capital-one-credit-card-application-hack-faq.html. In some cases, Social Security numbers and bank account numbers were not tokenized or encrypted such as when small businesses substituted Social Security numbers for Employer Identification Numbers.

obtaining the data.[4] Capital One indicated in a statement that Thompson is a "highly sophisticated individual" [5] who previously worked at Amazon Web Services, which hosts the Capital One database, as recently as September 2016.[6] But Thompson's knowledge may not be unique – tens of thousands of employees work or have worked at Amazon Web Services and thousands more work at Capital One. [7] [8] Equally troubling, "some researchers have noted that the techniques allegedly used and the security weaknesses allegedly exploited are commonly known."[9]

It is also disturbing that Capital One did not detect the breach until nearly four months after the incident. According to a briefing delivered to staff for the Senate Committee on Banking, Housing, and Urban Affairs on July 31, 2019, Thompson first breached Capital One's systems in March and"[t]he configuration vulnerability was reported to us by an external security researcher through our Responsible Disclosure Program on July 17, 2019."[10] It does not appear that Capital One's internal controls and audit ever detected the breach. While white hat operations are a crucial part of any fulsome cybersecurity program, they are not a substitute for robust internal controls. Capital One must also explain in detail the steps that the company has taken to ensure that this specific vulnerability is no longer present and describe the steps the bank will take to fortify its defenses to ensure that its databases are not further exposed to similar breaches and other vulnerabilities that put additional consumer data at risk.

Capital One's response to potentially affected customers also raises questions. In its press statement, Capital One promised to, "notify affected individuals through a variety of channels,"[11] but did not specify who it considers "affected individuals" and how and when they will be notified. And in the July 31, 2019, staff briefing, representatives from Capital One, led by the Executive Vice President and Chief External Affairs Officer Andres Navarrete, stated that the company is still working to identify ways to proactively contact individuals and businesses affected by the breach.[12] This is especially concerning because the 100 million stolen credit card applications include current customers, former customers, and individuals and businesses that

---

[4] New York Times, "'I'm Never Coming Back,' the Woman at the Center of the Capital One Heist Warned Friends," Mike Baker, July 30, 2019, https://www.nytimes.com/2019/07/30/us/capital-one-hacker-paige-thompson.html.

[5] Capital One, "Capital One Announces Data Security Incident," press release, July 29, 2019, http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle.

[6] New York Times, "Capital One Data Breach Compromises Data of Over 100 Million," Emily Flitter and Karen Weise, July 29, 2019, https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

[7] LinkedIn, "Amazon Web Services," Accessed August 5, 2019, https://www.linkedin.com/company/amazon-web-services.

[8] Forbes, "Capital One Financial," Accessed August 5, 2019, https://www.forbes.com/companies/capital-one-financial/.

[9] Washington Post, "The Capital One hack couldn't have come at a worse time for Amazon's most profitable business," Jay Greene and Drew Harwell, August 1, 2019, https://www.washingtonpost.com/technology/2019/08/01/capital-one-hack-couldnt-have-come-worse-time-amazons-most-profitable-business/.

[10] Senate Committee on Banking, Housing, and Urban Affairs, staff briefing with representatives from Capital One, July 31, 2019.

[11] *Id.*

[12] Senate Committee on Banking, Housing, and Urban Affairs, staff briefing with representatives from Capital One, July 31, 2019.

submitted applications but ultimately did not receive credit cards.[13] It is critical that individuals or businesses whose data were exposed due to Capital One's security failures receive adequate and timely notifications.

The public deserves to know exactly what the company plans to do to ensure that consumers' accounts and application information are protected from the consequences of Capital One's security failures.

In the aftermath of the massive Equifax breach in 2017, I opened an investigation of the causes of the breach and the company's response.[14] That investigation revealed that Equifax set up a failed system to prevent and mitigate the impact of data breaches, ignored numerous warnings of risks to sensitive data, failed to notify consumers and regulators of the breach in a timely fashion, and provided inadequate information and assistance to consumers in the wake of the breach. I hope that this investigation does not reveal similar failures by Capital One.

To address these concerns and provide the public with clarity on the causes of, extent of, and ramifications of the breach, as well as actions that Capital One will take to rectify the consequences, I ask that you answer the following questions no later than August 19th. I understand that some of my questions concern matters that may be confidential, and my staff and I are happy to discuss this matter with you to address any concerns and ensure that private business information and law enforcement-sensitive information are not made public.

1. Please provide a detailed timeline of all matters related to the breach, including:
    a. Key milestones or decisions by Capital One prior to the breach.
    b. The data breach.
    c. Capital One's discovery of the breach.
    d. Capital One's actions immediately following discovery of the breach.
    e. Capital One's initial efforts to inform the public of the breach.
    f. Actions taken by Capital One after July 29, 2019.
    g. Ongoing actions taken by Capital One.

2. How did Capital One discover the breach, and what information did the company receive that resulted in the discovery?
    a. If the company did not receive a tip through the Responsible Disclosure Program, what existing security measures could have identified this security vulnerability? Why were these measures insufficient without external assistance?

---

[13] CNBC, "Jamie Dimon's worst fears for the banking industry realized with Capital One data hack," Hugh Son, July 30, 2019, https://www.cnbc.com/2019/07/30/jamie-dimons-worst-fears-for-banks-realized-with-capital-one-hack.html.

[14] Office of Senator Elizabeth Warren, "Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information," February 2018, https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf.

b. Without a tip through the Responsible Disclosure Program, how would the company have identified the security vulnerability and how would the company have identified that an unauthorized person had access to the database?

3. Please explain precisely the extent of the breach.
    a. How many U.S. individuals' Social Security numbers were accessed?
        a. Please provide a breakdown of how many of these individuals are current customers, former customers, or other applicants whom Capital One does not have accurate and up-to-date contact information?
    b. How many U.S. individuals' birth dates were accessed?
        a. Please provide a breakdown of how many of these individuals are current customers, former customers, or other applicants whom Capital One does not have accurate and up-to-date contact information?
    c. How many U.S. individuals' addresses were accessed?
        a. Please provide a breakdown of how many of these individuals are current customers, former customers, or other applicants whom Capital One does not have accurate and up-to-date contact information?
    d. Your press release indicates that the accessed information included "personal information Capital One routinely collects at the time it receives credit card applications."[15] Exactly what personal information was accessed?
    e. Were any other kinds of document or information accessed besides names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, self-reported income, and customer status data? If yes, what type of documents, and how many U.S. consumers were affected?
        a. How many of these individuals are current customers, former customers, or other applicants whom Capital One does not have accurate and up-to-date contact information?

4. How does Capital One plan to contact credit card applicants who did not ultimately become Capital One customers and were included in the data breach?
    a. If Capital One does not have up-to-date or accurate contact information for every individual, what steps will Capital One take to ensure that these individuals are still notified in a timely manner?

5. Please explain how, if at all, any executives at Capital One or Amazon Web Services, the company hosting the breached database, are being held accountable for the security failures.
    a. Has any Capital One executive been fired or otherwise penalized as a result of the breach? If so, please provide details on these executives and their punishment.
    b. To your knowledge, has any executive at Amazon Web Services been fired or otherwise penalized as a result of the breach? If so, please provide details.

---

[15] Capital One, "Capital One Announces Data Security Incident," press release, July 29, 2019, http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle.

i. Has Capital One sought to find more information about the breach from Amazon Web Services? If so, please provide information regarding your communications with Amazon Web Services.
ii. Has Capital One sought to hold Amazon Web Services accountable for the breach? If so, please provide information regarding your communications with Amazon Web Services.

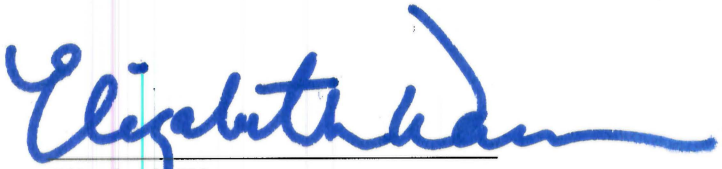
6. In addition to contacting law enforcement, did Capital One inform any of its regulators of the breach before informing the public? If so, please describe the communications and the timeline of communications.

7. Please describe all actions taken by Capital One to identify the root cause of the breach. What conclusions has Capital One reached with regards to the root cause of the breach, and what specific actions has the company taken in response to these findings?

8. Prior to July 19, 2019, did Capital One have a plan in place to respond to a large-scale security breach?
   a. If so, please provide a copy of this plan.
   b. If so, was this plan followed in its entirely following the July 2019 discovery of the breach? If not, where did the Capital One response deviate from this plan, and why?

9. Beyond providing free credit monitoring and identity protection services, how will Capital One ensure that consumers are minimally affected by the data breach and the identified security vulnerabilities?
   a. Please provide specific details on the credit monitoring and identity protection services that Capital One will provide to affected consumers, including the length of free services, whether consumers will need to opt-out of services before being required to pay for these services, and the terms and conditions to which consumers receiving these services must agree.
   b. What additional actions will Capital One take in addition to providing credit monitoring and identity protection?

Sincerely,



Elizabeth Warren
United States Senator