NYDIA M. VELAZQUEZ, NEW YORK
CHAIRWOMAN

STEVE CHABOT, OHIO
RANKING MEMBER

Congress of the United States

U.S. House of Representatives

Committee on Small Business

2361 Rayburn House Office Building
Washington, DC 20515-6315

July 31, 2019

Richard D. Fairbank
Chief Executive Officer
Capital One Financial Corp.
1680 Capital One Drive
McLean, VA 22102-3491

Dear Mr. Fairbank:

As Chairwoman of the House Committee on Small Business, I am concerned about the data security breach at Capital One and the potential impact on the nation's nearly 30 million small businesses. According to your press release, the data breach affected approximately 100 million individuals in the United States. Particularly concerning is that the largest category of information accessed was that of small business owners from 2005 through early 2019 who applied for one of your credit card products. The data breach compromised the names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, self-reported income, along with credit scores, credit limits, balances, and payment history. The misuse of this personal information can have a devastating effect on small business owners. Identity theft will not only damage their personal finances but can jeopardize business operations and possibly their livelihood.

Capital One is a leading provider of credit cards for small businesses through the SPARK business card. Therefore, this breach is alarming because it could inflict financial losses to millions of small business owners in a variety of industries across the country. Additionally, Capital One, as a provider of Small Business Administration 504 loans and 7(a) loans, has a duty to protect the interests of its small businesses customers who not only rely on access to affordable credit but expect that their personally identifiable information will be kept secure. Finally, I am concerned that the data breach could harm small business owners who used the SPARK 401(K) plan to start a retirement plan. In particular, the data breach could compromise the retirement security of small business owners and their employees.

Most small businesses simply do not have the staff or financial resources to become experts in cybersecurity and identify theft protections, or otherwise retain an employee dedicated to such issues. Given the significant potential exposure of small businesses as a result of this breach, I urge you to provide greater assistance for small business owners who may be impacted. Accordingly, I request the following information:

1. How many Capital One Spark Credit Card holders were impacted by the data breach?

2. If a small business owner has a Capital One Spark Credit Card and it is linked to other accounts, are these accounts impacted?
3. Do you have reason to believe any other such information was comprised, such as loan applications? Why or why not?
    a. Were small businesses that have taken out 504 loans with Capital One impacted? If so, how many?
    b. Were any small businesses that took out 7(a) loans have been affected? If so, how many?
4. It is my understanding that the former management team of Capital One's Spark 401(k) team purchased the 401(k) business from Capital One, and now operates it as Sharebuilder 401(k). Does Capital One still have the personally identifiable information of small business owners and their employees that are enrolled in a Share builder 401(k) and was it included in the breach?
5. While Capital One has already stated its intention to offer free credit monitoring services, how long will such monitoring last and how are you working with customers to bolster account security?
6. What steps are being taken to educate small business owners about the breach and what the potential consequences are for their businesses?
7. Does Capital One plan to have dedicated lines of communication and agents to respond to the questions from small business owners?
8. How will Capital One ensure that assistance is provided to small business owners and individuals in areas with little or no Internet access?
9. Has Capital One conducted a thorough analysis of its cybersecurity systems to ensure this does not happen again?
10. Have you been working with Amazon to take corrective measures to close the "misconfiguration" of the firewall and strengthen the web applications?
11. How does cybersecurity risk factor into Capital One's corporate governance?
12. What steps has Capital One taken to ensure its employees are properly trained on cyber security protocol?

I look forward to your prompt response.

Sincerely,

Nydia M. Velázquez
Chairwoman
House Committee on Small Business