

1. What happened?

On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products.

Capital One immediately fixed the issue and promptly began working with federal law enforcement. The person responsible was arrested. Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.

2. How did you discover the incident?

Like many companies, we have a responsible disclosure program which provides an avenue for ethical security researchers to report vulnerabilities directly to us. The configuration vulnerability was reported to us by an external security researcher through our Responsible Disclosure Program on July 17, 2019. We then began our own internal investigation, leading to the July 19, 2019, discovery of the incident.

3. When did this occur?

On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information about Capital One credit card customers and individuals who had applied for our credit card products. This occurred on March 22 and 23, 2019.

4. Has my information been accessed?

Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.

We will directly notify by mail the U.S. individuals whose Social Security numbers or linked bank account numbers were accessed. We will directly notify all Canadian customers affected.

Free credit monitoring and identity protection is available to everyone affected.

We are also encouraging customers to enroll in account alerts to help them keep track of activity on their accounts. Customers can sign in to online banking and set up text or email alerts, based on their preferences.

We also encourage customers to monitor their credit card accounts for unusual or suspicious activity that they do not recognize, and to call the phone number on the back of their Capital One card or on their statement as soon as possible, if they see unusual activity.

We do not call customers asking for personal information and customers should be mindful of the possibility of phishing emails and calls due to this incident. Tips on how to spot fraudulent emails / messages are on the Capital One website at [Protect Yourself Against Card Fraud](#).

Phishing is an attempt to acquire personal information, sometimes to compromise online banking accounts by posing as a legitimate company in an electronic communication. These emails are not from Capital One. If you believe you have received a fraudulent email that claims to be from Capital One:

- Do not reply to the email.
- Do not click on any of the links embedded in the email.
- Forward the email to abuse@capitalone.com.
- After forwarding the email to Capital One for investigation, delete it.
- Be sure to monitor your credit card account and call us if you notice any unusual activity.

5. Who is responsible for this cyber incident?

The FBI has arrested the person responsible for this cyber incident. Based on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual.

6. Does this incident impact customers from your other businesses?

This incident primarily impacted people who have applied for one of our credit card products as well as credit card customers. Our Auto Finance, Commercial Bank, and customers from our UK card businesses were not impacted.

7. What is Capital One doing to protect me after this incident? How can I sign up for credit monitoring / identity protection services?

We have sophisticated fraud systems in place to detect any unusual activity and protect our customers from unauthorized actions.

We will directly notify by mail the U.S. individuals whose Social Security numbers or linked bank account numbers were accessed. We will directly notify all Canadian customers affected. Free credit monitoring and identity protection is available to everyone affected.

Customers are encouraged to enroll in credit card account alerts to help them keep track of activity on their accounts. Customers can sign in to online banking and set up text or email alerts, based on their preferences.

Additionally, we encourage customers to monitor their credit card accounts for unusual or suspicious activity and, if they notice any activity that they do not recognize, to call the number on the back of their Capital One card or on their statement as soon as possible.

We do not call customers asking for personal information and customers should be mindful of phishing emails and calls due to this incident. Tips on how to spot fraudulent emails / messages are on the Capital One website at [Protect Yourself Against Card Fraud](#).

Phishing is an attempt to acquire personal information, sometimes to compromise online banking accounts by posing as a legitimate company in an electronic communication. These emails are not from Capital One. If you believe you have received a fraudulent email that claims to be from Capital One:

- Do not reply to the email.
- Do not click on any of the links embedded in the email.
- Forward the email to abuse@capitalone.com.
- After forwarding the email to Capital One for investigation, delete it.
- Be sure to monitor your account and call us if you notice any unusual activity.

8. Was the data encrypted or tokenized?

We encrypt our data as a standard. Due to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of data.

However, it is also our practice to tokenize select data fields, most notably Social Security numbers and account numbers. Tokenization involves the substitution of the sensitive field with a cryptographically generated replacement. The method and keys to unlock the tokenized fields are different from those used to encrypt the data. Tokenized data remained protected.

9. I think I received a scam email related to Capital One's cyber incident?

Customers should be mindful of phishing emails due to this incident. Tips on how to spot fraudulent emails / messages are on the Capital One website at [Protect Yourself Against Card Fraud](#).

Phishing is an attempt to acquire personal information, sometimes to compromise online banking accounts by posing as a legitimate company in an electronic communication. These emails are not from Capital One. If you believe you have received a fraudulent email that claims to be from Capital One:

- Do not reply to the email.
- Do not click on any of the links embedded in the email.
- Forward the email to abuse@capitalone.com.
- After forwarding the email to Capital One for investigation, delete it.
- Be sure to monitor your account and call us if you notice any unusual activity.

10. I received a call or text from Capital One related to this cyber incident asking for my information. What should I do?

Capital One is not calling or texting customers to ask for credit card or account information, or Social Security numbers over the phone or via email.

If you have provided personal information over the phone or clicked on links in a fraudulent email, follow these additional steps:

1. Call us immediately to report that your account information may have been compromised.
2. Sign in to Capital One Online Banking and change your password and security questions.
3. Check your accounts for suspicious activity.
4. Update and run anti-virus software on your computer.

11. Are there any additional steps that I can take to protect myself against fraud and identity theft?

You can request a free copy of your credit report once every 12 months from each of the three national credit reporting agencies: Equifax, Experian and TransUnion.

- Once you receive your reports, review them for suspicious activity, such as inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you did not authorize.
- Verify the accuracy of your Social Security number, address(es), complete name and employer(s).
- Notify the credit bureaus if any information is incorrect in order to have it corrected or deleted.

To obtain free credit reports, simply visit www.annualcreditreport.com, call 1-877-322-8228, or complete the Annual Credit Report Request Form, which can be found [here](#), and mail it to: *Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.*

Additionally, you can call the toll-free fraud number of any one of the three nationwide credit bureaus and place an initial or extended fraud alert on your credit report.

- [Equifax](#): 1-800-525-6285; Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348-5069
- [Experian](#): 1-888-EXPERIAN (397-3742); P.O. Box 9532, Allen, TX 75013
- [TransUnion](#): 1-800-680-7289; Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016

An initial fraud alert stays on your credit report for 90 days and acts as an alert to potential lenders. An extended fraud alert is intended for victims of identity theft and stays on your credit report for seven years.

12. How may I contact Capital One?

We'll continue to update this site with developments as new information becomes available. If you'd like to speak with an agent, call 1-800-227-4825.