



P.O. Box 30285
Salt Lake City, UT 84130-0285

April 22, 2021

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04111

Dear Attorney General:

We are writing to notify you of an incident that impacted personal information involving one (1) of your state's residents.

We've determined that a vendor's former employee accessed the Capital One credit card accounts of the one (1) Maine resident mentioned above during the course of what we believe was legitimate account servicing/maintenance activity, but then later used the one (1) Maine residents' account information to make unauthorized transactions or attempted transactions. The vendor's former employee would have had access to account information including the Maine residents' names, addresses, telephone numbers, email addresses, credit card account numbers, Social Security numbers, dates of birth, CVV2 codes and transaction histories. Please be assured that the former employee no longer has access to any Capital One accounts or any Capital One systems.

We sent notice of this incident to the one (1) Maine resident mentioned above, letting them know their personal information was compromised. We also offered them 24 free months of credit monitoring and identity protection with TransUnion's myTruIdentity credit monitoring service. In addition, our notice contained some fraud prevention tools and tips. A redacted copy of the notice we sent to the impacted Maine residents is attached here.

We remain committed to maintaining high standards for customer service and customer data security and want to assure you that we are taking appropriate steps to protect the personal information of our customers.

If you have any questions, comments or concerns, please contact Christina Bhirud, Senior Counsel at (702) 908-5081 or Christina.Bhirud@capitalone.com.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jonathan Olin".

Jonathan Olin
Managing Vice President, Chief Counsel
Legal, Privacy and Financial Integrity



P.O. Box 30285
Salt Lake City, UT 84130-0285

<Sysdate_Current>

<AdhocName1>
<AdhocAddress1> <AdhocAddress2>
<AdhocCity>, <AdhocState> <AdhocZip5>

Re: Account ending <AdhocAcctNumLastFour>
Case No. DSE 303212

Dear <Customer's Name>:

As you may be aware, your personal information was compromised. A former employee accessed your Capital One card account to make unauthorized transactions that were attempted between <AdhocVar1> and <AdhocVar2>. Please be assured that these attempts did not post to your account. The former employee would have had access to account information including your name, address, telephone number, email address, credit card account number, Social Security number, date of birth, CVV2 code and transaction history. Please be assured that the former employee no longer has access to your account or any Capital One systems. However, please continue to review your statements (including outside of Capital One®) for unauthorized activity and/or identity theft concerns.

We are enclosing fraud prevention tools and tips and would like to offer you two (2) years of TransUnion's credit monitoring service, at no cost to you, to help you identify any potential identity theft. You can sign up for your free two (2) years of TransUnion's credit monitoring service anytime until June 30, 2021. This service will not auto-renew, but you can choose to continue the service at your own cost after two years. Please read the enclosed instructions on how to set it up.

We understand how important your privacy is. If you have any questions, please don't hesitate to call us at 1-888-372-8305.

Sincerely,

Chanda Sperry
Managing Vice President, Operations
Capital One®





HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <AdhocVar3> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code [REDACTED] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.
- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)
- You can sign up for the online or offline credit monitoring service anytime between now and June 30, 2021. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian, or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.
- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

ADDITIONAL RESOURCES



You should remain vigilant for instances of fraud or identity theft over the next 12 to 24 months, and promptly report incidents of suspected identity theft to your financial institution(s). Further, we recommend that you review your account statements and immediately report any suspicious activity to your financial institution(s). You should closely monitor your credit reports, which are available to you free of charge

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228. You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, including your full name; Social Security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or insurance statement.

Bureau Contact Information. You may contact the three nationwide credit reporting agencies about security freezes, fraud alerts and other related topics, using the following:

Equifax:
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian:
P.O. Box 2104
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion:
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
<http://www.marylandattorneygeneral.gov/>
1-888-743-0023

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
<http://www.ncdoj.gov/>
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

Reporting identity theft and obtaining a police report.

For Iowa residents:

You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents:

You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents:

You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Rhode Island residents:

You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.



P.O. Box 30285
Salt Lake City, UT 84130-0285

April 16, 2021

[REDACTED]

Re: Account ending [REDACTED]
Case No. DSE 303212

Dear [REDACTED]:

As you may be aware, your personal information was compromised. A former employee accessed your Capital One card account to make unauthorized transactions that were conducted between 8/8/2020 and 9/21/2020. The former employee would have had access to account information including your name, address, telephone number, email address, credit card account number, Social Security number, date of birth, CVV2 code and transaction history. Please be assured that the former employee no longer has access to your account or any Capital One systems. However, please continue to review your statements (including outside of Capital One®) for unauthorized activity and/or identity theft concerns.

We are enclosing fraud prevention tools and tips and would like to offer you two (2) years of TransUnion's credit monitoring service, at no cost to you, to help you identify any potential identity theft. You can sign up for your free two (2) years of TransUnion's credit monitoring service anytime until June 30, 2021. This service will not auto-renew, but you can choose to continue the service at your own cost after two years. Please read the enclosed instructions on how to set it up.

We understand how important your privacy is. If you have any questions, please don't hesitate to call us at 1-888-372-8305.

Sincerely,

Chanda Sperry
Managing Vice President, Operations
Capital One®





HOW TO ENROLL IN CREDIT MONITORING

As noted above, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting agencies.

- To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code [REDACTED] and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code [REDACTED] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.
- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)
- You can sign up for the online or offline credit monitoring service anytime between now and June 30, 2021. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian, or Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.
- **Special note for minors affected by this incident:** The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.



ADDITIONAL RESOURCES

You should remain vigilant for instances of fraud or identity theft over the next 12 to 24 months, and promptly report incidents of suspected identity theft to your financial institution(s). Further, we recommend that you review your account statements and immediately report any suspicious activity to your financial institution(s). You should closely monitor your credit reports, which are available to you free of charge

Annual Credit Report. You may order a free annual credit report. To do so, please visit www.annualcreditreport.com or call 1-877-322-8228. You can also order your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or make certain changes to your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report. A security freeze will prevent a credit reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency certain identifying information, including your full name; Social Security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or insurance statement.

Bureau Contact Information. You may contact the three nationwide credit reporting agencies about security freezes, fraud alerts and other related topics, using the following:

Equifax:
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian:
P.O. Box 2104
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion:
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
<http://www.marylandattorneygeneral.gov/>
1-888-743-0023

North Carolina Office of the Attorney General
Mail Service Center 9001
Raleigh, NC 27699-9001
<http://www.ncdoj.gov/>
1-877-566-7226

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

Reporting identity theft and obtaining a police report.

For Iowa residents:

You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents:

You have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents:

You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Rhode Island residents:

You have the right to file or obtain a police report regarding this incident.

Federal Fair Credit Reporting Act Rights: The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.