June 16, 2023

Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

Re: Case No. DSE 600083

Dear Attorney General Frey:

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

A now former employee accessed Capital One credit card accounts and made unauthorized transactions between August 11, 2022 through May 22, 2023. The employee was able to see the customer's name, credit card number, date of birth, email address, other financial information (balances), address, Social Security number, telephone number and transaction history.

We are sending 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 myTrueIdentity credit monitoring service. In addition, our notice contained some fraud prevention tools and tips. A redacted copy of the notice we are sending to the impacted Maine resident 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 Malcolm Thomas, Manager Counsel at (202) 740-1678 or dse_contact@capitalone.com.

Sincerely,

Malcolm Thomas
Manager Counsel

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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

NOTICE OF DATA BREACH

Dear [redacted]

WHAT HAPPENED
We're writing to let you know that your information was compromised.

A now former employee accessed Capital One credit card accounts, including yours, and made unauthorized transactions between August 11, 2022 through May 22, 2023.

WHAT INFORMATION WAS INVOLVED
The now former employee would have had access to account information including your Name, Credit card number, Date of birth, Email address, Other financial information (balances), Address, Social Security Number, Telephone number and Transaction history.

Please be assured that the now 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.

WHAT WE ARE DOING
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 September 30, 2023. 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.

WHAT YOU CAN DO
We've included a list of tips for protecting yourself against misuse of your personal information.

FOR MORE INFORMATION
We understand how important your privacy is. If you have any questions, please don't hesitate to call us at [redacted]

Sincerely,

Joe Westcott
VP, 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 (*my*TrueIdentity) 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 *my*TrueIdentity 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 [redacted] 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 September 30, 2023. 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

Consistent with certain laws, we are providing you with the following information about steps that a consumer can take to protect against potential misuse of personal information.

You should remain vigilant for instances of fraud or identity theft over the next 12 to 24 months, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, you should report it immediately to your financial institution(s).

Federal Trade Commission. You may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Website, at www.ftc.gov/idtheft, call the FTC, at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

In addition, you may obtain information from the FTC and the nationwide credit reporting agencies listed below about fraud alerts and security freezes.

Credit Reports. You may also periodically obtain credit reports from each nationwide credit reporting agency. Under the Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.

You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com/personal/credit-report-services

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022
www.TransUnion.com/credit-help

If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

Fraud Alert. You may place a fraud alert in your credit report file by contacting one of the three nationwide credit reporting agencies listed above. A fraud alert tells creditors that you may be the victim of fraud and to follow certain procedures, such as contacting you before they open any new accounts or make certain changes to your existing accounts.

Security Freeze. You also may place a security freeze on your credit report file to restrict access to your credit report. A security freeze is designed to prevent potential creditors from accessing your credit report unless you lift the freeze. 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 will need to provide the credit reporting agency with certain identifying information, including your full name, address, date of birth, Social Security number and other personal information.

After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place. There is no charge to place, lift or remove a security freeze.

Contact Information for Certain State Attorneys General Offices.

If you are a District of Columbia resident: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and
-online-security/identity-theft

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
oag.dc.gov/

If you are a Maryland resident: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and
-online-security/identity-theft

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
oag.state.md.us

If you are a Massachusetts resident: 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.

If you are a New York resident: You may obtain information about security breach response and identity theft prevention and protection from the FTC or the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and
-online-security/identity-theft

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
dos.ny.gov

If you are a North Carolina resident: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and
-online-security/identity-theft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
ncdoj.gov

If you are a Rhode Island resident: You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
riag.ri.gov/