January 28, 2026

Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, MA 02116

Re: Case No. 1132142

Dear Undersecretary:

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

We have attached a copy of the notice we sent to the resident we notified in connection with this matter which describes the facts and circumstances of the event. We have also attached a copy of the notification sent to the State of Massachusetts' Office of the Attorney General which will provide additional details of the event.

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 me at (804) 284-9977 or PERT_contact@capitalone.com.

Sincerely,

Melissa Polinsky
Assistant General Counsel
Capital One

January 28, 2026

Massachusetts Office of the Attorney General
Data Privacy and Security Division
Attn: Data Breach Notification
One Ashburton Place
Boston, MA 02108

Re: Case No. DSE 1132142

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 have determined that an integration between two systems introduced a logic change for checking existing customers, which merged customer information profiles. While we do not see any suspicious account transactions related to this, existing customers were able to see the customer's name, address, email address, phone number, and bank account numbers.

We sent notice of this incident to the one (1) Massachusetts resident mentioned above, letting them know their personal information was exposed to another customer. We also offered them 24 months of free 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 sent to the impacted Massachusetts resident is attached here.

We are providing concurrent notification to the Office of Consumer Affairs and Business Regulation. Capital One has taken action to contain and remediate the incident, including creating new customer information files and providing notice and free credit monitoring to impacted residents. We have a Written Information Security Program (WISP), and we do not believe an update to it is needed at this time.

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 me at (804) 284-9977 or PERT_contact@capitalone.com.

Sincerely,

Melissa Polinsky
Assistant General Counsel
Capital One

Capital One
P.O. Box 9033
Melville, NY 11747

800-655-BANK (2265)
capitalone.com

[redacted]

January 23, 2026

NOTICE OF DATA BREACH

Re: Case No. 1132142

Dear [redacted],

WHAT HAPPENED
We are writing to let you know about an event that impacted the privacy of your personal information at Capital One. A technical error caused some of your bank account information to be exposed to another customer. Please know that there is no indication that this data exposure was the result of any intent to target or compromise your data, and we do not see any indication of fraudulent activity on your account.

WHAT INFORMATION WAS INVOLVED
The information exposed included your name, address, email address, phone number, bank account number and transaction information. While we do not see any suspicious account activity related to this incident, and while we believe the risk of fraud is low, please keep an eye out for unauthorized transactions (including outside of Capital One).

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 April 30, 2026. This service will not auto-renew, but you can choose to continue the service at your cost after two years. Please read the enclosed instructions on how to set it up.

WHAT YOU CAN DO
We have included a list of tips for protecting yourself against potential 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] We're available 7 days a week.

Sincerely,
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 **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 **April 30, 2026**. 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 **transunion.com/credit-disputes/child-identity-theft-inquiry-form** 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 **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, D.C. 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 **annualcreditreport.com** or by calling 877-322-8228.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
800-685-1111	888-397-3742	800-680-7289
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
Equifax.com/personal/credit-report-services	**Experian.com/help**	Chester, PA 19016-2000 **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: **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, D.C. 20580
877-IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and-online-security/identity-theft

Office of the Attorney General
Office of Consumer Protection
441 4th Street, NW
Washington, D.C. 20001
202-442-9828
oag.dc.gov/consumer-protection

If you are an Iowa resident: You may report suspected incidents of identity theft to local law enforcement or you can contact the Iowa Attorney General at:

Office of the Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319-0106
888-777-4590
iowaattorneygeneral.gov/for-consumers/file-a-consumer-complaint

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, D.C. 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
marylandattorneygeneral.gov/Pages/CPD/default.aspx

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, D.C. 20580
877-IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and-online-security/identity-theft

Office of the New York
State Attorney General
The Capitol
Albany, NY 12224-0341
800-771-7755
ag.ny.gov/file-complaint/consumer

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Albany, NY 12231-0001
800-697-1220
dos.ny.gov/consumer-protection

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, D.C. 20580
877-IDTHEFT (438-4338)
consumer.ftc.gov/identity-theft-and-online-security/identity-theft

North Carolina Department of Justice
Attorney General Josh Stein
Consumer Protection
9001 Mail Service Center
Raleigh, NC 27699-9001
919-716-6000
ncdoj.gov/protecting-consumers

If you are an Oregon resident: You may report suspected incidents of identity theft to local law enforcement relating to this incident. In addition, you can contact the FTC or the Oregon Attorney General at:

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

Oregon Department of Justice
Attorney General Ellen F. Rosenblum
1162 Court St. NE
Salem, OR 97301
877-877-9392
justice.oregon.gov/consumercomplaints

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