



DLA Piper LLP (US)
One Liberty Place
1650 Market Street
Suite 5000
Philadelphia, Pennsylvania 19103-7300
www.dlapiper.com

Ron Plesco
ron.plesco@us.dlapiper.com
T 215.656.2453
F 215.606.2053

December 3, 2024

VIA EMAIL

Idtheft@oag.state.md.us
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Security Incident Notification

Dear Sir or Madam:

We represent Chemonics International, Inc. (“Chemonics”) and are writing to notify your Office of a compromise that affected the security of certain personal information relating to 1,107 Maryland residents. By providing this notice, Chemonics does not waive any rights or defenses, including but not limited to rights or defenses regarding the applicability of Maryland law, the applicability of Maryland data event notification statute, or personal jurisdiction.

On December 15, 2023, Chemonics became aware of suspicious activity related to certain user accounts (the “Incident”). Upon discovery, the internal security team took steps to remediate, including by conducting password resets and disabling impacted accounts. Please note that the Incident has since been contained and remediated. Chemonics launched a comprehensive investigation with the assistance of cybersecurity experts to determine the nature and scope of the Incident. Chemonics also engaged and continues to work with appropriate law enforcement authorities.

The in-depth cyber forensic investigation identified evidence indicating the unauthorized access occurred beginning on May 30, 2023, and continued through the last date of detection on January 9, 2024. Through the investigation, it was also determined that data was subject to unauthorized access. With the assistance of third-party eDiscovery experts retained through outside counsel, Chemonics conducted a thorough and time-intensive review of the data at issue to identify the personal information subject to unauthorized access and determine to whom the personal information relates. This process took time to complete, and on October 31, 2024, the eDiscovery process confirmed which individuals’ personal information was subject to unauthorized access.

The information affected varies by individual but includes one or more of the following types of personal information: name, address, social security number, passport number, financial account number and access code, payment card number, health information, user credentials, and biometric data. The notification letter sent to residents will identify the specific data elements impacted for each individual receiving notice.



December 3, 2024

Page Two

Since this Incident, Chemonics has implemented additional security technologies and processes to bolster overall security including strengthening its multi-factor authentication processes, enhancing email security, deploying additional endpoint monitoring and detection tools, and blocking suspicious Internet traffic.

On December 3, 2024, Chemonics will mail notice to the affected residents, offering a 24-month subscription for credit monitoring and identity protection through Equifax Credit Watch Gold. Affected residents may enroll in the services at no cost by using a promotional code and instructions provided to them in the notification letter.

A sample notification letter is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the residents affected by this Incident, please contact me at (215) 656-2453 or Ron.plesco@dlapiper.com.

Respectfully submitted,

A handwritten signature in blue ink that reads 'Ron Plesco'.

DLA Piper LLP (US)

Ron Plesco

Counsel for Chemonics International, Inc.

Enclosure(s):

Sample Notification Letter



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Re: NOTICE OF DATA BREACH

Dear <<Full Name>>:

Chemonics International, Inc. (“Chemonics,” “we,” “us,” or “our”) writes to inform you of an incident that involved some of your personal information. While we are unaware of any attempted or actual misuse of your personal information, we are providing you with information about the event, our response, and steps you can take to protect your personal information, should you feel it necessary to do so. Chemonics takes this incident and the security of your personal information very seriously and we sincerely regret any concern this incident may cause.

WHAT HAPPENED? On December 15, 2023, Chemonics became aware of suspicious activity related to certain user accounts (the “Incident”). Upon discovery, the internal security team took steps to remediate, including by conducting password resets and disabling impacted accounts. Please note that the Incident has since been contained and remediated. Chemonics launched a comprehensive investigation with the assistance of cybersecurity experts to determine the nature and scope of the Incident. Chemonics also engaged and continues to work with appropriate law enforcement authorities.

The in-depth cyber forensic investigation identified evidence indicating that the unauthorized access occurred beginning on May 30, 2023, and continued through the last date of detection on January 9, 2024. Through the investigation, it was also determined that data was subject to unauthorized access. With the assistance of third-party eDiscovery experts retained through outside counsel, Chemonics conducted a thorough and time-intensive review of the data at issue to identify the personal information subject to unauthorized access and determine to whom the personal information relates. This process took time to complete, and on October 31, 2024, the eDiscovery process confirmed which individuals’ personal information was subject to unauthorized access.

WHAT INFORMATION WAS INVOLVED? The investigation determined that the following types of your personal information were included in the impacted data: <<Breached Elements>>.

WHAT WE ARE DOING. Please know that protecting your personal information is something that Chemonics takes very seriously. We conducted a diligent investigation to confirm the nature and scope of the Incident, and we have taken steps to bolster overall security including strengthening multi-factor authentication processes, enhancing email security, deploying additional endpoint monitoring and detection tools, and blocking suspicious Internet traffic. We are providing notice and offering credit monitoring services to individuals based on the personal information that was potentially impacted.

WHAT YOU CAN DO. You can review the enclosed document titled *Additional Steps to Protect Your Personal Information* for more information. We encourage you to remain vigilant by reviewing account statements and monitoring free credit reports. You may want to temporarily freeze your credit. You should be on guard for schemes where malicious actors may pretend to represent Chemonics or reference this incident. If you have questions, please contact us at the number described below.

To help protect your identity, we are offering complimentary access to Equifax Credit Watch Gold for 24 months. This helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

To enroll in this credit monitoring service, please visit the website listed below. You will need the Activation Code provided below to complete your enrollment.

Enrollment URL: **www.equifax.com/activate**

Your Activation Code: <<**Activation Code**>>

Enrollment Deadline: <<**Expiration Date**>>

Go to **www.equifax.com/activate**

Enter your unique Activation Code of <<**Activation Code**>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, Equifax will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

FOR MORE INFORMATION. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call 1-888-658-8864, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time (excluding major U.S. holidays).

Sincerely,



Catherine Kannam
Chief Operating Officer
Chemonics International, Inc.

Additional Steps to Protect Your Personal Information

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill; and
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take

steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
[www.transunion.com/fraud-
victim-resource/place-fraud-
alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

State Specific Information

California Residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street, NW
Washington, D.C. 20001
(202) 727-3400
Email: oag@dc.gov
<https://oag.dc.gov/Consumer>

Maryland Residents: You may obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office at:

Attorney General of Maryland
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023
www.oag.state.md.us

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include: the right to access information in your consumer file at a consumer reporting agency; to dispute incomplete or inaccurate information in your consumer file at a consumer reporting agency; to have consumer reporting agencies correct or delete inaccurate information in your consumer file; the right to block information in your consumer file that is the result of identity theft; and the right to have a fraud alert placed on your consumer file (as described above). For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
The Capitol
Albany, NY 12224-0341
(800) 771-7755
<https://ag.ny.gov/consumer-frauds-bureau>

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

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
114 West Edenton Street
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

Oregon Residents: You may obtain information about reporting suspected identity theft from the following Oregon agencies:

Office of the Attorney General
Oregon Department of Justice
1162 Court St. NE
Salem, OR 97301-4096
Email: AttorneyGeneral@doj.state.or.us

Office of Attorney General
Consumer Protection
Toll-Free: 1-877-877-9392
<https://justice.oregon.gov/consumercomplaints/>

Rhode Island Residents: The total number of Rhode Island residents impacted in this incident is <<RI#>>. Under Rhode Island law, you have the right to obtain a police report filed in regard to 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. You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov