



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 215.656.3301

December 14, 2023

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 are writing to provide notice on behalf of Plug Power Inc. (“Plug Power”) pursuant to Md. Code Ann. Comm. Law § 14-3504, regarding an incident involving 41 Maryland residents. By providing this notice, Plug Power does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of Maryland’s security incident notification statute, or personal jurisdiction.

On March 22, 2023, Plug Power became aware of a ransomware event on certain company systems. Upon discovery, Plug Power immediately took action to contain the event and engaged third-party cyber experts to determine the nature and scope of the incident. Power also notified law enforcement.

Plug Power’s in-depth investigation of the incident determined that an unauthorized user gained access to, and may have taken information from, certain systems between March 13, 2023, and March 23, 2023. With the assistance of cybersecurity experts, Plug Power worked diligently to recover and restore impacted systems so it could analyze the data potentially accessed and taken by the unauthorized user. On November 30, 2023, after a comprehensive review of the data involved, the investigation revealed that a limited amount of personal information of Maryland residents was contained in the affected data set.

Since this event, Plug Power has enhanced its monitoring, reset passwords throughout the organization, and implemented additional security technologies and processes to bolster overall security.

The information involved varies by individual but includes one or more of the following types of personal information: name, social security number, driver’s license number, passport number, financial account information in combination with any required security code, access code or password that would permit access to a resident’s financial account, account login credentials, medical information and health insurance information. The notification letter sent to affected Maryland residents will identify the specific data elements involved for each individual receiving notice.

On December 15, 2023, Plug Power will mail written notice to Maryland residents, offering a complimentary 24-month subscription for credit monitoring services through IDX identity protection services. Residents who receive notice 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 Maryland residents affected by this incident, please contact me at (215) 656-2453 or Ron.Plesco@us.dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

A handwritten signature in blue ink, appearing to read "Ron Plesco", is centered on the page. The signature is written in a cursive, flowing style.

Ron Plesco



P. O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 15, 2023

NOTICE OF SECURITY INCIDENT

Dear <<First Name>> <<Last Name>>,

Plug Power Inc. ("Plug Power") writes to inform you of an incident that may have involved 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 incident, our response, and details related to what you may do to better protect your personal information. Plug Power 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 March 22, 2023, Plug Power became aware of a ransomware event on certain company systems. Upon discovery, Plug Power immediately took action to contain and engaged third-party cyber experts to determine the nature and scope of the incident. Plug Power also notified law enforcement.

Plug Power's in-depth investigation determined that an unauthorized user gained access to, and may have taken information from, certain systems between March 13, 2023, and March 23, 2023. With the assistance of cybersecurity experts, Plug Power worked diligently to recover and restore impacted systems so it could analyze the data potentially accessed and taken by the unauthorized user. On November 30, 2023, after a comprehensive review of the data impacted, we discovered some of your personal information may have been involved.

What Information Was Involved

The investigation determined the following types of your personal information may have been involved: <<Variable Data>>.

What We Are Doing

Please know that protecting your personal information is something we take very seriously. We conducted a diligent investigation to confirm the nature and scope of this incident. We also took steps to reduce the likelihood of a similar incident from occurring in the future, and we continue to make additional improvements that strengthen our cybersecurity protections. Although we have no evidence to suggest your personal information has been fraudulently used, we are nevertheless offering you complimentary credit monitoring services through IDX, A ZeroFox Company, as detailed below.

IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

You can review the enclosed *Additional Steps to Help Protect Your Information*. You can also enroll to receive the complimentary credit monitoring services being offered to you. 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 also be on guard for schemes where malicious actors may pretend to represent Plug Power or reference this incident.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-817-5781, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 15, 2024.

For More Information

Please call 1-888-817-5781 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. We sincerely regret any inconvenience this incident may cause.

Sincerely,

A handwritten signature in black ink that reads "Paul B. Middleton". The signature is written in a cursive, flowing style.

Paul Middleton
Chief Financial Officer
Plug Power Inc.

(Enclosure)



Additional Steps to Help Protect Your Information

1. Website and enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. For more information. Contact IDX at 1-888-817-5781 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports and monitor your accounts. We recommend that you remain vigilant by regularly reviewing account statements and monitoring credit reports. 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 discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. You 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

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
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

6. 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;
- 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.

7. Additional Information. You can further educate yourself regarding identity theft and the steps you can take to protect yourself, including placing fraud alerts and security freezes, by contacting your state Attorney General or the Federal Trade Commission (FTC). Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You may contact the FTC at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.

8. State-Specific Information. If you are a resident of the following states, the following information applies to you:

District of Columbia: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: (202) 727-3400, <https://oag.dc.gov>, Office of the Attorney General for the District of Columbia, 441 4th St. NW, Washington, DC 20001.

Kentucky Residents: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the

consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: For information on how to avoid identity theft or to contact the attorney general, please use the following contact information: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. Under Rhode Island law, you have the right to obtain a police report filed in regard to this breach. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Based on our investigation to date, we believe this breach affected 8,323 individuals.