



December 8, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Via email: IDTheft@oag.state.md.us

SUBJECT: Notification of Data Security Incident

To Whom It May Concern:

This letter shall serve as Idaho National Laboratory's (INL) notice to the State of Maryland of a data security incident impacting 228 residents of Maryland. Battelle Energy Alliance, LLC (BEA) manages and operates the U.S. Department of Energy (DOE) INL site under a government contract. This contract requires that BEA follow DOE O. 206.1 data breach notification requirements. Pertinent incident information is as follows:

Incident Summary: On November 20, 2023, INL was informed that a cyber data breach occurred on November 19, 2023, at an off-site data center that housed information on INL employees, former employees, spouses, and dependents. The event did not impact INL's own network, or other networks or databases used by employees, lab customers or other contractors.

Remediation Efforts: In the immediate aftermath of the event, INL worked to restrict access to the server that was involved in the breach, alerted federal law enforcement agencies, and began the process of confirming the individuals and the types of information that were compromised. INL also worked to notify impacted individuals and lab stakeholders through internal and external means and provided steps impacted individuals can take to protect themselves. Further steps are being taken and evaluated to prevent a similar occurrence.

Notification to Impacted Individuals: Our anticipated date to notify Maryland residents is December 13, 2023 by way of correspondence through the United States Postal Service or email if an individual's address is not available. Our notification extends an offer of free credit monitoring for 12 months.

Please feel free to contact me with any questions.

Sincerely,

Andre' Duffin
Assistant Privacy Officer
(208) 526-6161

Enclosure



[Return Address Line 1]

[Return Address Line 2]

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

[Date]

RE: Important Security Notification Concerning Notice of Data Breach. Please read this entire letter.

Dear [First Name] [Last Name]:

As you may be aware, Idaho National Laboratory (INL) recently suffered a cyber data breach that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On November 20, 2023, INL was informed that a cyber data breach occurred on November 19, 2023, at an off-site data center that housed information on INL employees, former employees, spouses, and dependents. The event did not impact INL's own network, or other networks or databases used by employees, lab customers or other contractors. The event continues to be investigated by federal agencies including the Department of Energy, Federal Bureau of Investigation, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Though the matter is currently under investigation, this notice was not delayed as a result of law enforcement investigations.

What Information Was Involved? We can confirm that multiple forms of sensitive personally identifiable information (PII) including names, social security numbers, salary information and banking details were exposed for many individuals. Some individuals only had their names and dates of birth compromised. The compromised information contained payroll data for employees, former employees, and retirees that was current as of June 1, 2023. PII that may have been included within that data set includes the following: [PII Data Set]

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. In the immediate aftermath of the event, we worked to restrict access to the server that was involved in the breach, alerted federal law enforcement agencies, and began the process of confirming the individuals and the types of information that were compromised. We also worked to notify impacted individuals and lab stakeholders through internal and external means and provided steps impacted individuals can take to protect themselves.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Length of Credit Monitoring] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit

bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Length of Credit Monitoring] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Length of Credit Monitoring]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** March 10, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Length of Credit Monitoring]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$5 Million Identity Theft Insurance*:** Provides coverage for certain costs and \$500k coverage of unauthorized electronic fund transfers.

Listed below are additional steps that you may take to minimize the potential for identify theft:

1. Since your personal information was involved in this incident, it can be used by identity thieves to open fraudulent accounts in your name, so watch for signs that your personal information has been misused. For example, bills that do not arrive on time; receiving credit cards you did not apply for; unexpected offers of credit or an increase in the number of offers; being denied credit; or being contacted by debt collectors or businesses about merchandise or services you did not buy.
2. Consider placing a fraud alert on your credit file. Fraud alerts tell potential creditors that they should take special precautions to verify the identity of the applicant. Remember that you may find it more difficult to get new credit while there is a fraud alert on your credit file. You may place a 90-day "initial fraud alert" on your file by calling any one of the three nationwide consumer reporting companies at their designated toll-free numbers (listed below). The company you call will inform the other two companies. This alert can help stop someone from opening new credit accounts in your name. If you are an identity theft victim and submit an identity theft report like a police report, you can place an "extended" seven-year alert on your file.

Equifax: 1-800-525-6285 or equifax.com
Experian: 1-888-397-3742 or experian.com
TransUnion: 1-800-680-7289 or transunion.com

If an initial alert is on a credit file, creditors must use reasonable policies and procedures to verify the identity of the person requesting credit, including calling the consumer at a telephone number designated on the fraud alert. If an

extended alert is on a credit file, the creditor must contact the consumer at the telephone number designated on the extended alert.

3. If you do not want to place a fraud alert on your credit file, you can still order your free annual credit report. You can order online at annualcreditreport.com, or by calling toll free 1-877-322-8228, or by writing Annual Credit Report Request Service, Box 105281, Atlanta GA 30384-5281.

Once you receive your credit report, review it for suspicious activity such as inquiries from companies you did not contact, accounts you did not open, and unexplained charges on accounts. Check that other information such as your address, date of birth or employer, is correct.

When you place a fraud alert with one of the three credit reporting companies, you will receive information about ordering one free credit report from each of the three companies.

4. All credit bureaus allow consumers to "freeze" their credit file. Credit freezes restrict access to a consumer's credit file, so the file cannot be used in credit granting decisions. If a credit freeze is in place, it is unlikely that creditors would open a new account because they can't determine the credit-worthiness of the applicant. Neither an identity thief nor the actual consumer would be able to get credit while a freeze is in effect. While there is no charge to place a credit freeze, there may be a fee associated with unfreezing a credit file, and that laws governing this may vary by state.

If you choose to put a credit freeze in place, you will have to contact each of the three consumer reporting companies.

5. If you learn that your information has been misused, file a complaint with the police and with the Federal Trade Commission (FTC) at <http://ftc.gov>, 1-877-438-4338, or Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580. The FTC website also has step-by-step instructions on other measures to take, including an ID Theft Affidavit that consumers can use when disputing unauthorized accounts. Subject to applicable state law, you have the right to receive a police incident report in response to any complaint you make with police.

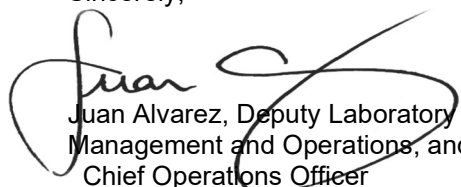
For further valuable information regarding protecting yourself from identity theft, and resolving identity theft if it should occur, refer to these websites:

<http://www.ftc.gov/idtheft/>

http://www.treasury.gov/services/report-fwa/Pages/id_theft.aspx.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call [Experian TFN] toll-free 24 hours a day, 7 days a week (excluding major U.S. holidays). Be prepared to provide your engagement number [B#####]. If you are a current employee and require further assistance or information, please send electronic communications to info@inl.gov. For all other individuals that require further assistance or information, please contact databreach@inl.gov. Alternatively, written communication may be forwarded to Idaho National Laboratory, P.O. Box 1625, 2525 North Fremont Ave., Idaho Falls, ID 83415.

Sincerely,



Juan Alvarez, Deputy Laboratory Director
Management and Operations, and
Chief Operations Officer

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Residents of Washington D.C. have the additional option to contact the following agency for further steps to avoid identify theft at:

Office of the Attorney General
Office of Consumer Protection
441 4th Street, NW
Washington, DC 20001
Phone: 202-727-3400
Website: <https://oag.dc.gov>

Residents of Iowa have the additional option to contact the following agency to report suspected incidents of identity theft at:

Office of the Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319-0106
Phone: 515-281-5926
Website: <http://www.iowaattorneygeneral.gov>

Residents of Maryland have the additional option to contact their attorney general's office at:

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Phone: 410-576-6574
Website: <https://www.marylandattorneygeneral.gov/>

Residents of North Carolina have the additional option to contact the following agency for further steps to prevent identity theft at:

Attorney General's Office
Consumer Protection Division
9001 Mail Service center
Raleigh, NC 27699-9001
Phone: 919-716-6400
Website: <http://www.ncdoj.gov>

Residents of Oregon have the additional option to contact the following agency to report suspected incidents of identity theft at:

Office of the Attorney General
Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
Phone: 503-378-4400
Website: <http://www.doj.state.or.us/pages/index.aspx>

Residents of Rhode Island have the additional option to contact their attorney general's office at:

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

Residents of New Mexico may visit the following link to review a summary of your rights under the federal Fair Credit Reporting Act (FCRA):
https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Residents of New York can receive additional information regarding security breach response and identity theft prevention and protection information at:

Office of the New York State Attorney General
Consumer Frauds Bureau
Albany: The Capitol, Albany NY 12224
New York City: 28 Liberty Street, New York, NY 10005
Identity Theft Help Line: 1:800-771-7755
Website: <https://ag.ny.gov/publications/identity-theft>