

Sent: Friday, July 14, 2023 12:22 AM
To: DOJ: Consumer Protection Bureau <DOJ-CPB@doj.nh.gov>
Subject: Data Security Incident Notification

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

Consumer Protection and Antitrust Bureau:

I am writing to notify you of a data security incident impacting 8 residents of New Hampshire. Pertinent incident information is detailed as follows:

Incident Summary: Three Blu-ray compact discs containing recent changes to Idaho National Laboratory's (INL) Electronic Data Management System database were lost within the INL internal physical mail system while being sent for off-line storage. The discs were unencrypted and contain some personally identifiable information (PII) that was listed on dosimeter request questionnaires from visitors, contractors, and employees. The PII includes

. Upon discovery that the discs had not been received by the intended recipient, a comprehensive search began for recovery of the discs. To date, the discs have not been recovered; however, there is an extensive search that remains ongoing. Currently, we are not aware of any indicators of unauthorized access of this information.

Remediation Efforts: INL put an immediate stop to this backup process and is developing a more secure approach that complies with information security requirements.

Notification to Impacted Individuals: Written notification was distributed to New Hampshire residents via U.S. Mail on today's date (July 13, 2023). To help defend against identity theft, the notification extends an offer of free credit monitoring for .

Let me know if you have any questions.

Regards,

Mandi

Mandi Hong
Privacy Officer
FOIA Officer
Office of Risk, Assurance & Compliance
Idaho National Laboratory

CONFIDENTIALITY NOTICE: This message, together with any attachments, may be legally privileged and is confidential information intended only for the use of the individual or entity to which it is addressed. It is exempt from disclosure under applicable law including court orders. If you are not the intended recipient, you are notified that any use, dissemination, distribution or copying of this message or any attachment is strictly prohibited. If you have received this message in error, please notify the sender and delete this message and any attachments.



July __ 2023

«AddressBlock»

SUBJECT: NOTIFICATION OF DATA SECURITY INCIDENT

«GreetingLine»

The privacy and security of the personal information we maintain is of the utmost importance to Idaho National Laboratory (INL). We are writing to inform you of a data security incident at INL involving some of your information. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

Recently, records saved to a Blu-ray disc as part of a routine file backup process were lost in transit after being sent internally between two onsite locations. No evidence has been found that your records have been accessed without authorization. In an effort to promote transparency, we are notifying you of the loss of records and outlining additional steps we are currently taking to protect your privacy.

Our review of the incident has established that your personal information was among the data believed to be on the disc. The personal information was part of a _____ that included «PII_CATEGORY», generated as a result of the radiological monitoring that took place while you participated in training and/or visited the facility.

This means that, although not confirmed, your PII may have been compromised in this incident. If compromised, this type of PII may be misused to target you with phishing emails, identity theft, or for other fraudulent purposes. To help defend against identity theft, BEA is offering you free credit monitoring for one year. To apply for this credit monitoring offer or if you have any questions, please contact INL's Privacy Officer via mail at P.O. Box 1625, Idaho Falls, ID 83415-3899, via email at _____, or via fax at _____. You must request credit monitoring by _____, to be eligible for this offer. Also, in order to be able to receive credit monitoring you must have a credit history. Listed below are additional steps that you may take to minimize the potential for identity theft.

First, 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.

Second, 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

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289

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.

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.

Third, 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 _____ 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.

Fourth, 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. Note that 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.

Fifth, 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> or 1-877-438-4338. 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. You should also notify INL’s Privacy Officer at _____ so that we can try to determine any linkage between this event and the misuse of your identity.

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

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

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

Should you have any personal concerns or would like to learn additional information about this incident, please contact INL's Privacy Officer via mail at P.O. Box 1625, Idaho Falls, ID 83415-3899, via email at .

BEA is committed to ensuring that you are informed of any potential risk resulting from this matter. We regret the inconvenience this situation may cause you.

Sincerely,

Mandi Hong
Privacy Officer

