<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

June 10, 2024

NOTICE OF SECURITY INCIDENT

Dear <First Name>,

We are writing regarding a cyber security incident that the Intrepid Museum Foundation, Inc. ("Intrepid") experienced that impacted some of your personal information.

Keeping personal data safe and secure is extremely important to us. Upon detecting the incident, we hired external advisors to assist in investigating and responding to the incident. After an extensive review of the impacted data, we have determined that your data was included in the impacted information. Intrepid had your data either because you are a current or former Intrepid employee, intern, or contractor; a dependent of an Intrepid employee; or in connection with your visiting the museum or attending a camp here.

Intrepid has not identified any evidence to date that data affected by this incident has been misused, as an example, for fraud or identity theft.

WHAT HAPPENED?

The Intrepid Museum detected a cybersecurity incident on December 3, 2023 in which an unauthorized third party gained access to parts of our network and downloaded a copy of some of our files. Based on our investigation, we believe that the unauthorized actor first accessed the Intrepid Museum's network on December 2, 2023.

WHAT INFORMATION WAS INVOLVED?

After an extensive analysis of the data by our outside cybersecurity consultants, we recently determined that some of your personal information was included in the files that were involved.

The impacted personal information includes your name, <exposed data elements>.

WHAT ACTIONS HAVE WE TAKEN?

We promptly took steps to address this incident after its discovery, such as launching an investigation with the assistance of external cybersecurity experts, immediately taking steps to contain the incident and ensure the ongoing security of our network, and removing the unauthorized third party from our network. We also notified law enforcement of this incident but have not delayed notification as a result of any law enforcement investigation.

We then performed an extensive analysis of our files that were affected by this incident to identify any personal information contained within those documents. We recently completed the analysis and are now notifying affected individuals accordingly.

In response to the incident, we are providing you with access to Triple Bureau Credit Monitoring services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

HOW TO ENROLL FOR THE FREE SERVICES

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/intrepidmuseum** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<unique code>**

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

WHAT CAN YOU DO?

We encourage you to take the following precautions:

- Remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing your account statements and credit history for any signs of unauthorized transactions or suspicious activity. This is a best practice for all individuals.
- If you detect any suspicious activity on an account, you should immediately change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained.
- If you ever suspect you are the victim of identity theft or fraud, you can contact your local police.

If you would like to take additional steps to protect your personal information, please consult the attached helpful resources, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

Data security is very important to us, and we are committed to making sure our security practices are strong. We have arranged a dedicated call center to respond to your questions and assist you in taking advantage of the credit monitoring identity theft protection services offered to you. Please call 1-833-566-7803 with any questions. Representatives are available for 90 days from the date of this letter from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.

Sincerely,

The Intrepid Museum

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	Experian:	TransUnion:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

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

Fraud Alert
You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze
You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 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 violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information
You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For Massachusetts residents: 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.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For 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 bureaus 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 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. We encourage you to 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.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at www.dfcs.oregon.gov/id_theft.html and click "How to get a security freeze."

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are 8 Rhode Island residents impacted by this event.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).