

Asia Pacific

Bangkok
Beijing
Brisbane
Hanoi
Ho Chi Minh City
Hong Kong
Jakarta
Kuala Lumpur*
Manila*
Melbourne
Seoul
Shanghai
Singapore
Sydney
Taipei
Tokyo
Yangon

**Europe, Middle East
& Africa**

Abu Dhabi
Almaty
Amsterdam
Antwerp
Bahrain
Barcelona
Berlin
Brussels
Budapest
Cairo
Casablanca
Doha
Dubai
Dusseldorf
Frankfurt/Main
Geneva
Istanbul
Jeddah*
Johannesburg
Kyiv
London
Luxembourg
Madrid
Milan
Moscow
Munich
Paris
Prague
Riyadh*
Rome
St. Petersburg
Stockholm
Vienna
Warsaw
Zurich

The Americas

Bogota
Brasilia**
Buenos Aires
Caracas
Chicago
Dallas
Guadalajara
Houston
Juarez
Lima
Los Angeles
Mexico City
Miami
Monterrey
New York
Palo Alto
Porto Alegre**
Rio de Janeiro**
San Francisco
Santiago
Sao Paulo**
Tijuana
Toronto
Washington, DC

* Associated Firm
** In cooperation with
Trench, Rossi e Watanabe
Advogados

April 20, 2022

Via Electronic Mail

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street, Concord, NH 03301
attorneygeneral@doj.nh.gov

RE: Data Breach Reporting

Dear New Hampshire Attorney General,

I am writing on behalf of Henry Company (“Henry”) to notify you of a recent data security incident. Specifically, Henry was the victim of unlawful ransomware activity from approximately January 21, 2022, to January 29, 2022, that impacted certain servers and workstations in the United States and Canada. In response to this activity, Henry engaged a leading third-party cybersecurity forensics firm to restore the security and integrity of its systems, and then determine the scope of the information affected. In the course of its investigation, on March 11, 2022, Henry learned that some files containing information about New Hampshire residents residing on the impacted servers and workstations may have been subject to unauthorized access.


As part of Henry's investigation, Henry learned that certain information about approximately six (6) New Hampshire residents may have been stored on compromised systems, including individuals' name and Social Security number. At this point, however, Henry has no reason to believe that any such information has been used to commit identity theft, fraud, or any other unlawful activity.

In response to the incident, Henry immediately took the impacted systems offline to secure those systems first, as well as the information contained on them, and Henry has been diligent to ensure that its systems were scanned and reviewed to verify that they were safe to use prior to bringing them back online. Henry continues to work closely with its external industry-leading service providers to implement additional incremental security measures to protect its systems, and to help it defend against this type of unlawful activity in the future.

As a precautionary measure, Henry purchased identity theft protection services (at no cost to impacted New Hampshire residents) through Experian, a leading data breach resolution services expert. The purchased services include twenty-four (24) months of credit monitoring. A sample copy of the notice being sent to New Hampshire residents is attached to the email containing this notice. We expect to deliver this notice to New Hampshire residents on April 20, 2022.

Please feel free to contact me with any questions at Brian.Hengesbaugh@bakermckenzie.com or (312) 861-3077.

Best regards,

Brian Hengesbaugh, 

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 20, 2022

H8026-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Notice of Data Breach

Dear Sample A. Sample:

Henry Company ("Henry") is writing to inform you of a security incident that may have involved information about you. We take the protection of your information seriously. We are contacting you now to explain what information may have been involved, what happened, and the steps you can take to protect your information.

WHAT HAPPENED

Henry was the victim of unlawful ransomware activity from approximately January 21, 2022, to January 29, 2022, that impacted certain servers and workstations in the United States and Canada. In response to this activity, we engaged a leading third-party cybersecurity forensics firm to restore the security and integrity of our systems, and then determine the scope of the information affected. In the course of our investigation, on March 11, 2022, we learned that some files containing information about you residing on the impacted servers and workstations may have been subject to unauthorized access.

WHAT INFORMATION WAS INVOLVED

As part of our investigation, we learned that certain information about you may have been stored on compromised systems, including your name, driver's license / state identification number, and/or Social Security number. At this point, however, we have no reason to believe that your information has been used to commit identity theft, fraud, or any other unlawful activity.

WHAT WE ARE DOING

In response to the incident, we immediately took the impacted systems offline to secure those systems first, as well as the information contained on them, and we have been diligent to ensure that our systems were scanned and reviewed to verify that they were safe to use prior to bringing them back online. We continue to work closely with our external industry-leading service providers to implement additional incremental security measures to protect our systems, and to help us defend against this type of unlawful activity in the future.

As a precautionary measure, we purchased twenty-four (24) months of identity theft protection services (at no cost to you) through Experian, a leading data breach resolution services expert. 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).

0000001



Please note that Identity Restoration is available to you for twenty-four (24) 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 twenty-four (24) 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** July 8th, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **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 (844) 933-2743 by July 8th, 2022. Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWENTY-FOUR (24) 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. Daily credit reports are available for online members only.*
- **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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

WHAT YOU CAN DO

We encourage you to enroll in Experian IdentityWorks and contact Experian with any questions you may have about enrollment by calling (844) 933-2743 and using the enrollment code provided above.

Please review the enclosed *Information about Identity Theft Protection* for additional information on how to protect against identity theft and fraud. In addition, we encourage you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Henry will never contact you in any way, including by email, asking for your Social Security number or any other sensitive information about you (e.g., payment card number or other financial account details). If you are ever asked for this information, you can be confident Henry is not the entity asking. Henry encourages you to remain vigilant, review your account statements, and monitor your credit reports closely.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

FOR MORE INFORMATION

Please call Experian directly at (844) 933-2743 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays) for any additional questions about enrollment you may have. Be prepared to provide your engagement number B046925. We apologize for any inconvenience this may cause you.

Sincerely,

Henry Company



Information about Identity Theft Protection

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 request 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

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
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.

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

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

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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Maryland Residents: 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.

North Carolina Residents: 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: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

