

Maryland Attorney General

Entity Name:	Hartford Fire Insurance Company (The Hartford)
---------------------	--

Contact Person Regarding Events:	Rachael Lavina
Contact Information:	One Hartford Plaza, Hartford, CT 06155
Contact Phone:	860-547-3144
Contact Email:	Rachael.Lavina@thehartford.com

The Hartford is providing this notice to the Attorney General's Office, pursuant to Md. Code Ann., Com. Law § 14-3504(h), because we determined on December 27, 2022, that notice is required to be provided to one (1) Maryland resident pertaining to the incident described below.

This incident occurred at our vendor, Elevate Services, Inc. (Elevate), which was subject to a ransomware incident. Elevate provides independent medical bill audits, depositions, and expert testimony associated with Property and Casualty claims. Several law firms that represent The Hartford's insureds also use Elevate as a service provider.

Elevate became aware of this incident on March 14, 2022. Upon further investigation, Elevate determined that an unauthorized actor had access to a limited number of their systems and gained access to some files from March 5, 2022 through March 15, 2022. As part of Elevate's investigation of this incident, they identified impacted individuals, aligning them with the correct insurance carrier or company. After Elevate provided The Hartford with the names of impacted individuals affiliated with The Hartford, Hartford began verifying those individuals' identities, relationships with The Hartford, and addresses for notification purposes. Currently 99 individuals related to The Hartford are in scope. The Hartford was informed by Elevate that their other customers were also impacted by this incident, and The Hartford is a small part of the overall incident.

The data elements impacted vary for each individual, but could have included name, address, date of birth, medical history, Social Security number, or driver's license number. Elevate will be mailing notification letters to all impacted individuals related to The Hartford and will offer, at no cost to the affected individuals, identity protection and credit monitoring services.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Re: Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>,

Elevate Services, Inc. (“Elevate”) is writing to inform you of a recent data security event that may involve some of your information. Elevate provides legal and other technology services to <<b2b_text_2Data Owner>>. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On March 14, 2022, we became aware that certain computer systems in our environment were inaccessible as a result of malicious file encryption. We immediately took steps to secure our systems and launched an investigation to determine the full nature and scope of the event. We also promptly notified federal law enforcement. Through our investigation, we determined that an unknown actor gained access to a limited number of our systems between March 5, 2022 and March 15, 2022, and certain files on those systems were accessed and downloaded by the unknown actor. The investigation was unable to determine which specific files within those systems were actually impacted.

Therefore, in an abundance of caution, we performed a comprehensive review of the contents of the affected systems to determine what information could have been contained in the impacted files and to whom the information related. Upon completion of the review, we then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and the Elevate customers with whom they were associated. The review recently completed.

What Information Was Involved? Although the investigation could not determine the specific impacted files, the following types of information relating to you were present on our systems during the event: your name, address, date of birth, personal injury claim and/or legal documentation, partial or full medical history, medical billing history, Social Security number, driver’s license number, and employment information and/or compensation information.

What We Are Doing. We take this event, and the security of information, very seriously. Upon becoming aware of the event, we immediately took steps to secure our systems. We also conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative processes as part of our ongoing commitment to data security. As an additional precaution, we are offering complimentary credit monitoring and identity restoration services for twelve (12) months through Kroll.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed Steps You Can Take to Protect Personal Information. There you will find more information on the credit monitoring and identity restoration services we are making available to you. While we will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at (XXX) XXX-XXXX, Monday through Friday, 9:00am to 6:30pm Eastern Standard Time (except U.S. holidays). You may also write to Elevate at 1711 W. Greentree Dr., Suite 108, Tempe, AZ 85284.

Sincerely,

[Signature]

Steve Harmon
Chief Operating Officer & General Counsel
Elevate Services, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Activate Identity and Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<MembershipNumber (S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that 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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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 \[#\] Rhode Island residents impacted by this event.](#)