

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Visit us online at
www.C-WLAW.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

December 14, 2022

Via Email

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
Idtheft@oag.state.md.us

RE: Security Incident Notification

To Whom It May Concern:

We serve as counsel for H.R. Allen, Inc. ("H.R. Allen"), located at 2675 Rourk St., Charleston, SC 29405, and provide this notification to you of a recent data security incident. We will provide updates as necessary to supplement this notice. By providing this notice, H.R. Allen does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about June 14, 2022, H.R. Allen discovered suspicious activity related to several employee email accounts. Upon discovery, H.R. Allen took immediate action to address and investigate the incident, which included engaging third-party specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that certain employee email accounts were subject to unauthorized access on several occasions between March 18, 2022 and June 16, 2022. H.R. Allen then began a thorough and time intensive review of the contents of the accounts in order to determine the type of information contained within the accounts and to whom that information related. On November 2, 2022, this review was completed, and H.R. Allen immediately worked to obtain up-to-date address information in order to provide impacted individuals with a notice letter. The type of information related to Maryland residents included name, Social Security Number, Incidental Health Reference, Health Insurance Information, and Treatment Cost Information. On November 29, 2022, it was discovered that two (2) potentially impacted individuals reside within Maryland.

H.R. Allen is providing notice of this incident to potentially impacted individuals, including two (2) Maryland residents via letter mailed on December 14, 2022. The notice letter includes an offer of complimentary credit monitoring and identity protection services offered through Kroll for twelve (12) months. A copy of the notice letter is attached hereto as **Exhibit A**.

Please contact me should you have any questions.

Very truly yours,

By



Exhibit A



<<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>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident experienced by our company that may have involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that your information was subject to actual or attempted misuse as a result of this incident, this letter includes information about the incident and steps you can take to help protect your information.

What Happened: On or about June 14, 2022, we discovered suspicious activity related to several employee email accounts. Upon discovery, we took immediate action to address and investigate the incident, which included engaging third-party specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that certain employee email accounts were subject to unauthorized access on several occasions between March 18, 2022 and June 16, 2022. We then began a thorough and time intensive review of the contents of the accounts in order to determine the type of information contained within the accounts and to whom that information related. On November 2, 2022, this review was completed, and we immediately worked to obtain up-to-date address information in order to provide you with this notice. On November 29, 2022, this process was completed, and we worked to provide you with this notification as soon as possible.

What Information Was Involved: The types of information contained within the affected email accounts included your first and last name, in combination with the following data element(s): <<b2b_text_2 (data elements)>>. Please note that we have no reason to believe that your information has been or will be misused as a result of this incident.

What We Are Doing: We have taken the steps necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took steps to secure the email accounts and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. 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, Fraud Consultation, and Identity Theft Restoration.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line which can be reached at [1-800-833-8333](tel:1-800-833-8333), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

Jeanne M. Ellis
Controller

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

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

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

Membership Number: <<Membership Number s_n>>

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 will 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.

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.

You can sign up for the online identity monitoring service anytime between now and <<b2b_text_6 (activation date)>>. Due to privacy laws, we cannot register you directly. Enrolling in this service will not affect your credit score. You must be over age 18 with a credit file activate these services.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;

6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order 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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. H. R. Allen may be contacted at 2675 Rourk St., Charleston, SC 29405.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>. H. R. Allen may be contacted at 2675 Rourk St., Charleston, SC 29405.