

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700

Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

KATHLEEN MONAGHAN
KMonaghan@c-wlaw.com

December 30, 2024

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

To Whom It May Concern:

We serve as counsel for CR&R Incorporated ("CR&R") located at 11292 Western Avenue, Stanton, CA 90680 and provide this notification to your Office of a recent data security incident experienced by CR&R. By providing this notice, CR&R does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about December 13, 2022, CR&R experienced a network disruption that impacted certain systems. Upon discovery, CR&R immediately took steps to secure their network and engaged third-party specialists to determine the nature and scope of the incident. A thorough investigation determined that certain information stored on the network was subject to unauthorized access. CR&R then began a comprehensive manual review of the contents of the potentially impacted data in order to determine the type(s) of information impacted and to whom that information related. Once this review was completed, CR&R worked to obtain up-to-date address information in order to provide individuals with notification of this incident. That process was completed on October 30, 2024.

On October 30, 2024, CR&R discovered that information related to six (6) residents of Maryland was potentially impacted by this event. The information may have included the individual's first name or initial and last name in combination with their Social Security number and/or health insurance information.

CR&R provided written notice of this incident to the potentially impacted Maryland residents via First Class Mail on December 26, 2024. A copy of the notice letter is attached hereto as **Exhibit A**, which provides details of the incident, complimentary credit monitoring services for twelve (12) months, and steps impacted individuals can take to protect their data.

Please contact me should you have any questions.

Very truly yours,

A handwritten signature in cursive script, reading "Kathleen Monaghan". The signature is written in a light gray or blue ink.

Kathleen Monaghan, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

DB 09762 CR&R Incorporated
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
[REDACTED]



[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

December 26, 2024

Re: Notice of Data Breach

Dear [REDACTED]:

CR&R, Incorporated ("CR&R") writes to notify you of an incident that may have impacted some of your information described below. We take the privacy and security of information in our care very seriously. We are providing you with information about this incident, our response, and steps you can take to help protect your information should you feel it is appropriate to do so.

What Happened: On or about December 13, 2022, CR&R experienced a network disruption that impacted certain systems. Upon discovery, we immediately took steps to secure our network and engaged third-party specialists to determine the nature and scope of the incident. A thorough investigation determined that certain information stored on our network was subject to unauthorized access. We then began a comprehensive manual review of the contents of the potentially impacted data in order to determine the type(s) of information impacted and to whom that information related. Once this review was completed, we worked to obtain up-to-date address information in order to provide you with this notice. That process was completed on October 30, 2024.

What Information Was Involved: The types of information that may have been contained within the affected data includes your first or initial and last name, in combination with your [REDACTED]
[REDACTED]
[REDACTED].

What We Are Doing: CR&R has taken steps to address this incident and is committed to protecting information in its care. Upon learning of this incident, we immediately took steps to secure our network and undertook a thorough investigation. As an additional safeguard, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Due to privacy laws, we cannot activate these services for you, and you must enroll yourself. Additional information on how to activate the complimentary credit monitoring services is enclosed.

What You Can Do: In addition to enrolling in credit monitoring services, we recommend that you remain vigilant in regularly reviewing and monitoring all of your bank account statements and credit history to guard

against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, notify your financial institution or company if applicable, and take any additional steps needed to protect your account.

Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. Please review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please contact our dedicated call center at 1-833-799-4433, Monday through Friday from 5am to 5pm (Pacific Standard Time) (excluding major U.S. holidays). You can also write us at 11292 Western Avenue, Stanton, CA 90680.

Sincerely,

Michael Zorzi
Chief Financial Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Credit Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you 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 the age of 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.

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.

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 <https://www.marylandattorneygeneral.gov/>.

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 incident. There are 0 Rhode Island residents impacted by this incident.