

Substitute Notice

Notice of Cybersecurity Incident

Rebekah Children's Services ("RCS") is notifying individuals whose information may have been involved in a data incident. **At this time, RCS does not have any evidence to indicate that any personal information has been or will be misused as a result of this incident.**

We take the security of personal information seriously and want to provide information and resources that can be used to protect personal information.

What Happened:

On September 5, 2023, RCS detected suspicious activity on its network and equipment. An unauthorized third party attempted to infiltrate RCS's network. Upon discovery of this incident, RCS promptly engaged a specialized third-party cybersecurity firm to conduct an investigation to determine the nature and scope of the incident. The forensic investigation determined that certain information may have been compromised by an unauthorized actor.

Based on these findings, RCS performed a review of the affected systems to identify the specific individuals and the types of information that may have been compromised. On December 27, 2023, RCS finalized the list of individuals to notify.

What Information Was Involved? Although RCS is unaware of any fraudulent misuse of information, based on the investigation, the following information may have been subject to unauthorized access: Name; Address; Social Security Number; Date of Birth; Health Information, Health Insurance Information, Treatment Information, Medication information, and Driver's License.

As of this writing, RCS has not received any reports of related identity theft since the date of the incident (September 5, 2023 to present).

What We are Doing:

Data security is one of our highest priorities. Since the discovery of the incident, RCS moved quickly to investigate, respond, and confirm the security of our systems. Specifically, RCS disconnected all access to their network, changed administrative credentials, restored operations in a safe and secure mode, enhanced the security measures, and took steps and will continue to take steps to mitigate the risk of future harm.

Lastly, RCS informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Further, we value the safety of personal information and are providing impacted individuals with access to Credit Monitoring services **at no charge**. These services provide individuals with alerts for at least 12 months from the date of enrollment when changes occur to their credit files. This notification is sent to impacted individuals the same day that the change or update takes place with the credit bureau. In addition, we are providing impacted individuals with proactive fraud assistance to help with any questions, or in the event their identity is compromised. These services will be provided by Cyberscout, a TransUnion company.

How Will Individuals Know If They Are Affected By This Incident? RCS mailed notice letters to individuals whose information was determined to be in the affected files, for whom a valid mailing address

is available. If an individual does not receive a letter but would like to know if they are affected, they may call RCS's dedicated assistance line, detailed below.

Whom Should Individuals Contact For More Information? If individuals have questions or would like additional information, they may call RCS's dedicated assistance line at 1-833-603-9760. Representatives are available between the hours of 8:00a.m. to 8:00p.m. Eastern time, Monday through Friday, excluding holidays.

RCS encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors.

We encourage impacted individuals to take full advantage of this service offering. Call center representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Below is additional information regarding the resources available to impacted individuals, and the steps that they can take to further protect their personal information.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 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 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 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 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, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 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.

For Vermont Residents, if you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).