ThreeRivers
REGIONAL COMMISSION
www.threeriversrc.com
P.O Box 989728
West Sacramento, CA 95798-9728

Counties Served: Butts, Carroll, Coweta, Heard, Lamar, Meriwether, Pike, Spalding, Troup and Upson

To Enroll, Please Call:
(833) 676-2138
Or Visit:
https://response.idx.us/threerivers
Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

March 30, 2022

Dear <<First Name>> <<Last Name>>

Three Rivers Regional Commission ("Three Rivers") is writing to notify you of an event that may involve some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? On July 20, 2021, Three Rivers identified that certain of our computer systems had become encrypted due to a sophisticated cyber-attack by an unknown actor. We immediately launched an extensive investigation to determine the nature and scope of the event, and worked quickly to: (1) secure our systems; (2) restore access to the information so we could continue to operate without disruption, and (3) investigate what happened and whether this resulted in any impact to information housed on our systems by the unknown actor. We also promptly reported this event to federal and state law enforcement. Through the investigation, we determined that the unknown actor gained access to certain systems between July 18, 2021 and July 20, 2021 and certain data was viewed or downloaded.

We then worked with data specialists to conduct a comprehensive review of information stored on the impacted systems to determine what information was affected and to whom the information related. We then conducted a manual review of our records to determine the identities and contact information for potentially impacted individuals. On or around February 25, 2022, we completed our review.

What Information Was Involved? Our investigation determined that at the time of the event, your name, <<Variable1>>, <<Variable2>> and <<Variable3>> were stored within the impacted systems. To date, Three Rivers has not received any reports of fraudulent misuse of any information potentially impacted by this event.

What We Are Doing. We take this event and the security of your information seriously. Upon learning of the activity, we immediately took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further enhance our information security posture.

While we are unaware of any fraudulent misuse of your information as a result of this event, as an additional precaution, Three Rivers is offering you access to <<12/24>> of complimentary credit monitoring and identity restoration services through IDX. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please

review the enclosed document, *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. If you have additional questions, please contact our toll-free dedicated assistance line at (833) 676-2138. This toll-free line is available Monday – Friday from 9 am - 9 pm Eastern Time (excluding U.S. holidays). The toll-free line is available until June 30, 2022. You may also write to Three Rivers at P.O. Box 818, Griffin, Georgia 30224.

Sincerely,

Kirk Fjelstul
Executive Director
Three Rivers Regional Commission

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (833) 676-2138 or going to https://response.idx.us/threerivers and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 30, 2022.

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 credit 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 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 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 is 1 Rhode Island resident impacted by this event.

March 30, 2022 – This is an update to our prior message of November 5, 2021 regarding a data security event involving Three Rivers Regional Commission ("Three Rivers"), that may have impacted the security of information related to certain individuals enrolled in services administered by Three Rivers. The individuals that may be impacted are senior citizens, and related individuals, who have participated in various programs through the agency in the following ten (10) West Central counties in Georgia which include Butts, Carroll, Coweta, Heard, Lamar, Meriwether, Pike, Spalding, Troup and Upson. Programs impacted could include, but are not limited to, Senior Community Service Employment Program, Nursing Home Transitions, Money Follows the Person, the Aging and Disability Resource Connection, or the Georgia Cares program. While Three Rivers is currently unaware of any actual misuse of this information, we are providing updated information about the event, the response to this event, and steps affected individuals may take to better protect against the possibility of identity theft and fraud, should affected individuals feel it is necessary to do so.

What Happened. On July 20, 2021, we identified that certain of our computer systems had become encrypted due to a sophisticated cyber-attack by an unknown actor. We conducted an extensive investigation, aided by third-party specialists, to determine the nature and scope of the event. Through the investigation, we determined that the unknown actor gained access to certain systems between July 18, 2021 and July 20, 2021, and certain data was viewed or downloaded from our systems.

We then worked with data specialists to conduct a comprehensive review of information stored on the impacted systems to determine what information was affected and to whom the information related. We then conducted a manual review of our records to determine the identities and contact information for potentially impacted individuals. We recently completed this review. On March 30, 2022, we mailed written letters to individuals impacted by this event for whom we had address information.

What Information Was Affected. The information involved will vary by individual. Our investigation determined that the types of information stored on our systems that relate to individuals may include name, address, driver's license number, state identification card number, Social Security number, financial account information, payment card information, medical information, such as clinical information, diagnosis and treatment, lab results, medications and Medicare/Medicaid identification number and/or health insurance information. If you receive a written letter regarding this event, your letter will identify what information related to you was specifically impacted.

What We are Doing. We take this event and the security of your information seriously. We immediately took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our existing policies and procedures to enhance our security posture. We also implemented additional administrative and technical safeguards to further secure the information in our systems. We reported this event to the Federal Bureau of Investigation, the Georgia Bureau of Investigation, and the Georgia Emergency Management and Homeland Security Agency. Further, on March 30, 2022, we notified potentially impacted individuals for whom we had address information so that

they may take further steps to help protect their information, should they feel it is appropriate to do so.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and credit reports for unusual activity and to detect errors. Additional resources can be found below in the *Steps You Can Take to Help Protect Your Information.*

For More Information. If you have additional questions, you may contact our toll-free dedicated assistance line at (833) 676-2138, Monday through Friday, during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time (excluding U.S. holidays). The toll-free number is available until June 30, 2022. You may also write to Three Rivers at 120 N. Hill Street, P.O. Box 818, Griffin, Georgia 30224.

Steps You Can Take To Help Protect Your Information

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 1-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, military identification, 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 fraud alert or 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 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 and your state attorney general.