[November 5, 2021] – A recent data security event involving Three Rivers Regional Commission ("Three Rivers"), may impact the security of information related to certain individuals enrolled in services administered by Three Rivers. The individuals that may be impacted are senior citizens 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 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.

In an abundance of caution, we are in the process of performing a comprehensive review of the information stored in our systems at the time of the event to identify any individuals whose information may have been accessed by the unknown actor. Once this review is complete, we will work to determine the identities and contact information for potentially impacted individuals and provide notice via written letter.

What Information Was Affected. The investigation is ongoing at this time, and the information involved will vary by individual. The types of information stored on our systems that relate to individuals may include name, address, driver's license number, Social Security number, and medical information, such as clinical information, diagnosis and treatment, lab results, medications and Medicare/Medicaid identification number.

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 its existing policies and procedures and implementing additional administrative and technical safeguards to further secure the information in our systems. We also reported this event to the Federal Bureau of Investigation, the Georgia Bureau of Investigation, and the Georgia Emergency Management and Homeland Security Agency. Further, we will be notifying potentially impacted individuals 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 us toll-free at (844) 999-4055, Monday through Friday, during the hours of 9:00 a.m. to 4:00 p.m., Eastern Time (excluding U.S. holidays). You may also write to Three Rivers at 120 N. Hill Street, PO 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.