

NOTICE OF SECURITY INCIDENT

St. Clair County, IL (“St. Clair County”) is notifying certain individuals of a recent data privacy event that may impact the privacy of a limited amount of personal and/or medical information. St. Clair County is unaware of any misuse of individual information but is providing notice to potentially affected individuals so they may take steps to protect themselves if they feel it is appropriate.

About the Data Incident.

On or about May 30, 2021, St. Clair County discovered anomalous and suspicious activities on its computer network. St. Clair County immediately launched an investigation with the assistance of third-party computer forensic specialists. The investigation determined that St. Clair County’s computer network was infected with malware, which caused a temporary disruption to St. Clair County’s services. St. Clair County also notified federal law enforcement of this disruption. On July 13, 2021, the investigation determined that an unknown actor gained access to St. Clair County’s systems on May 27, 2021 and removed certain files from the County’s computer systems on May 30, 2021. The County reviewed these files to determine if they contain sensitive information. St. Clair County recently completed that thorough and time-consuming review and determined sensitive information for certain individuals was impacted.

What Information Was Involved?

While the investigation found no evidence of actual or attempted misuse of information related to this incident, the types of personal and/or medical information that may have been impacted vary by individual and may have included: Social Security numbers, driver’s license or state identification numbers, medical diagnosis, treatment, and provider information, health insurance information, dates of birth, addresses, and names.

What We Are Doing.

St. Clair County treats its responsibility to safeguard sensitive information as an utmost priority. As such, St. Clair County responded immediately to this event and worked diligently to provide potentially affected individuals with accurate and complete notice of the event as soon as possible. As part of the ongoing commitment to the privacy and security of personal information in its care, St. Clair County is conducting a review of existing internal policies and procedures relating to data protection and security. St. Clair County has also provided notice of this event to state regulators, as required.

What You Can Do.

St. Clair County encourages all potentially affected individuals to remain vigilant against potential incidents of identity theft and fraud by reviewing medical and financial account statements and credit reports for suspicious activity. Potentially affected individuals can find out more about how to safeguard information in the section below titled *Steps You Can Take to Protect Personal Information*.

For More Information.

St. Clair County sincerely regrets any inconvenience or concern this incident may have caused. St. Clair County understands potentially affected individuals may have questions about this incident that are not addressed in this notice. To ensure questions are answered in a timely manner, please call the dedicated information line at Toll-Free Number: 855-632-1644 Call Center Hours: Monday through Friday, 8:00 am to 5:30 pm Central Time, excluding major US holidays.

If you think you may be affected but did not receive a letter, please call the dedicated hotline.

STEPS YOU CAN TAKE TO PROTECT PERSONAL 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, 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.