



City of Lewisburg Tennessee
131 East Church Street - 37091

MAY 2020 SECURITY INCIDENT

On May 13, 2020, the City of Lewisburg discovered that it had been the victim of a ransomware attack. The City immediately shut down its entire network and began the process of wiping all workstations and servers. Since that time, the City has been in the process of rebuilding its entire computer network from backups unaffected by the ransomware attack. The City also retained an outside computer forensics vendor to conduct an investigation into the attack and determine if personal information was potentially exposed.

Based upon the investigation completed on or about June 15, 2020 and the ransomware variant identified, there is a moderate probability that data exfiltration occurred during the security incident that occurred in mid-May. The data that was potentially exfiltrated includes affected individuals' name, address, and social security number. Individuals who are potentially affected by this breach includes: current and former employees of the City of Lewisburg and their spouses and minor dependents, current and former employees of the Lewisburg Water Department, and anyone who provided their social security number to the Lewisburg Police Department from 2012 to the present ("Affected Individuals").

The City has notified by U.S. Mail any current and former employees, their spouses, and their minor dependents who may be affected by the potential breach. The City has also notified by U.S. Mail current and former employees of the Lewisburg Water Department who may be affected by the potential breach. The City of Lewisburg was unable to identify the individuals who provided their social security numbers to the Lewisburg Police Department. Therefore, if you provided your social security number to the Lewisburg Police Department from 2012 to the present, including, for example, as a witness, arrestee or complainant, you are asked to pay particular attention to the information contained in this notice.

The City recommends that Affected Individuals remain vigilant for incidents of fraud and identity theft by regularly reviewing their account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Affected Individuals may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies.



City of Lewisburg Tennessee

131 East Church Street - 37091

You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 7402741
Atlanta, GA 30374

www.equifax.com

Report Credit Fraud:
(800) 685-1111

Request Credit Report:
(866) 349-5191

TransUnion
P.O. Box 2000
Chester, PA 19022

www.transunion.com

Report Credit Fraud:
(800) 680-7289

Request Credit Report:
(800) 916-8800

Experian
P.O. Box 2104
Allen, TX 75013

www.experian.com

Report Credit Fraud:
(888) 397-3742

Request Credit Report:
(888) 397-3742

In addition, Affected Individuals may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. Affected Individuals can add a fraud alert to their credit report file to help protect their credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. Affected Individuals may place a fraud alert in their file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, Affected Individuals can contact the nationwide credit reporting agencies regarding if and how they may place a security freeze on their credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

At this time, the City has not received any reports that any personal information for Affected Individuals has been misused or disseminated.

The City has alerted authorities and financial institutions of the potential data breach, and the City is continuing to monitor this situation. The City will notify Affected Individuals and provide an update on its website if it learns that fraudulent account activity has been traced to this potential data breach.

Again, we want to stress that we regret any inconvenience or concern this incident may cause Affected Individuals. Be assured that we place a top priority on protecting the security of personal information. Please do not hesitate to contact Donna Park, the City Treasurer for the City of Lewisburg, at (931) 359-1544 if you have any questions or concerns.

----- Phone 931-359-1544 Fax 931-359-7055 -----

www.lewisburgtn.gov