Notice of Data Incident

September 19, 2022 – The City of Quincy, Illinois (the "City") is issuing notice of a recent incident that may impact the privacy of information related to certain individuals. With this notice, the City is providing information about the incident, our response, and steps potentially affected individuals may take to better protect against the possibility of identity theft and fraud, should they feel it is appropriate to do so.

What Happened? On May 7, 2022, the City experienced a cybersecurity incident that affected the accessibility of its computer systems and caused a temporary disruption to certain municipal services. The City immediately launched an investigation to confirm the nature and scope of the incident, working quickly to restore our normal business operations and dedicating substantial resources to the response effort. Through the City's investigation, the City learned that an unauthorized actor accessed certain City computer systems between April 27, 2022 and May 7, 2022 and acquired a limited number of files stored on those systems. The City undertook a thorough review of the affected files to determine whether any personal information was present and therefore accessible. The City finalized this review on September 7, 2022.

What Information was Affected. The City confirmed that the information present in the affected files included names, addresses, dates of birth, driver's licenses, Social Security numbers or state-issued identification numbers, military identification numbers, and health insurance information.

What We are Doing. The privacy of the people we serve is very important to the City. The City treats its duty to safeguard the information entrusted to it as an utmost priority. The City responded immediately to this incident, promptly notified law enforcement authorities, and has been working diligently to provide impacted individuals with accurate and complete notices of the incident as soon as possible. The City has taken steps to enhance the security of its systems, which included resetting employees' account passwords. The City is also in the process of decommissioning legacy systems and migrating to a Cloud-based email platform. As part of its ongoing commitment to the privacy and security of information in its care, the City is reviewing its existing policies and procedures related to data security. The City is also providing additional training to employees to mitigate any risk associated with this incident and to better prevent future incidents.

What Affected Individuals Can Do. The City encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Information*.

For More Information. If you have additional questions, please call our dedicated toll-free assistance line at (855) 662-8108, Monday through Friday from 6am to 8pm PST and Saturday through Sunday from 8am to 5pm PST, excluding major U.S. holidays. You may also write to us directly at: City of Quincy, Risk/Cyber Security Department, 730 Maine Street, Quincy, IL 62301.

Steps You Can Take To Help Protect 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 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, 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
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box	Experian Fraud Alert, P.O.	TransUnion Fraud Alert, P.O.

105069 Atlanta, GA 30348-5069	Box 9554, Allen, TX 75013	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. 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: 441 4th St. NW #1100 Washington, D.C. 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;1-888-743-0023; 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.