The City of Chicago Provides Notice of Third-Party Data Incident

The City of Chicago (the "City") is providing notice of an event that may impact the privacy of certain individuals' information. At this time, the City is not aware of any fraud that might have resulted from this event, but it cannot say with certainty that none has occurred or will occur.

What happened? City computer systems were not subject to or involved in this incident. The City provided secure access to copies of certain City email accounts to an outside law firm as part of a project undertaken at the City's request. To assist in the project, the law firm received copies of certain City emails and then provided access to the emails via Accellion, a software service that includes a File Transfer Appliance (the "Accellion appliance") that is used by the law firm and others for the secure transfer of large files. As part of the work being performed for the City, the law firm used the Accellion appliance to transfer certain files, including some containing the emails at issue, to one of its sub-contractors assisting on this project.

Recently, the City learned from the law firm that a previously unknown and unreported vulnerability with the Accellion appliance was exploited and allowed a subset of the emails within the email accounts at issue to become accessible to unauthorized individuals. Upon learning of this incident, among other things, the City worked quickly to respond to the incident and investigate it with the law firm. Through these efforts, the City learned from the law firm that the incident involved a limited amount of email data that had been transferred through the Accellion appliance between January 14 and January 20, 2021. Upon receiving this information, the City continued to work closely with the law firm and others to confirm the nature and scope of the data at issue, as well as to whom such data related. The law firm reviewed this data with outside assistance and provided the final results of its review on or about April 1, 2021. The City promptly evaluated these results, took additional steps to identify affected individuals, and determined the scope of information present in the data that resided on the Accellion appliance at the time of the incident.

What Information Was Involved? As noted above, City computer systems were not subject to or involved in this incident. The City cannot confirm if any specific information relating to individuals was accessed or viewed by an unauthorized person as a result of the incident. However, the investigation and review outlined above determined that the data present on the Accellion appliance at the time of the incident included certain individuals' names, driver's license numbers, financial account information, Social Security numbers, medical information, and health insurance information. Please note that the information varies by individual and Social Security numbers were affected for only a few individuals.

What We Are Doing. The privacy of the people we serve is very important to us. Upon learning of this incident, we worked closely with the law firm and others to respond and determine the impact to City data and you. We have also received assurance from the law firm that it is maintaining and will continue to maintain maximum safeguards to protect City information. Toward that end, no City data exists in the law firm's Accellion appliance.

What We Are Offering. Out of an abundance of caution, we are also offering affected individuals access to 12 months of complimentary credit monitoring and identity restoration services through Experian. If you did not receive written notice of this incident but believe you may be affected, please contact our dedicated assistance line, which can be reached at (888) 401-0552 (toll free), Monday through Friday from 8 am –10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central, excluding U.S. holidays. The call center will verify whether you are eligible for services.

What You Can Do. Individuals can learn more about how to protect themselves generally against the possibility of theft or misuse of personal information by reviewing the below guidance, "Steps You Can Take to Protect Information."

For More Information. If you have questions or concerns that are not addressed in this notice, please do not hesitate to contact (888) 401-0552 (toll free).

Steps You Can Take to 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 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. This notice has not been delayed by law enforcement.