THE CITY OF COLUMBUS

The City of Columbus
Columbus City Auditor
90 W Broad Street, Room 109
Columbus, OH 43215

September 12, 2024

RE: Notice of Data Breach

Dear Valued Clients:

The City of Columbus (the "City"), recently discovered that it was the victim of a cybersecurity incident. The Columbus City Auditor ("we," "us," or "our"), as an agency of a political subdivision, is providing this notice in compliance with section 1347.12 of the Ohio Revised Code, as well as other applicable state data breach notification statutes. We want to provide you with information about the incident, steps we are taking in response, and steps impacted residents may take to guard against identity theft and fraud, should they feel it is appropriate to do so. Please note that this notice is in relation to the same incident that the City posted notice of on their website, a copy of which can be found at the link below.

On July 18, 2024, the City discovered that it had experienced a cybersecurity incident in which a foreign cyber threat actor attempted to disrupt the City's IT infrastructure, in a possible effort to deploy ransomware and solicit a ransom payment from the City. The City's continuing investigation of the cyber security incident has determined that the threat actor gained unauthorized access to the City's technology infrastructure, which may have included data in connection to the Columbus City Auditor. Further discovery indicated the incident allowed the threat actor to view and access certain sensitive personal information, which may have included first and last name, date of birth, address, bank account information, City employee account number and position, City employment and payroll records, Social Security number, and other identifying information.

Upon discovery of the attack, the City engaged legal counsel and a data breach remediation firm to conduct a thorough investigation into the scope and extent of the illicit attack. While the threat actor's activity was disrupted, an investigation is still ongoing to determine the amount of City data that may have been accessed and the Columbus City Auditor recognizes the *potential* that the files' security has been impacted, and is providing this notice in accordance with section 1347.12 of the Ohio Revised Code.

The City's Department of Technology, working with federal authorities and cybersecurity experts, has been engaged in a methodical process to ensure that the City's technology systems are hardened against further breach before bringing them back online. The Department of Technology will continue to work closely with cyber security experts to ensure the City, and all of its departments and divisions, remain vigilant in the security of operations.

The City provided affected individuals notice of the security incident via U.S. mail on August 6, 2024, or via approved methods of substitute notice, in compliance with section 1347.12 of the Ohio Revised Code and applicable state data breach notification statutes. The City posted notice of this incident on their website on August 16, 2024, which you can find a copy of here:

- City of Columbus- Cybersecurity Home Page: https://www.columbus.gov/Services/Cybersecurity
- Notice for Impacted Individuals: https://www.columbus.gov/Services/Cybersecurity/Experian-for-Impacted-Individuals

Additionally, the City has secured the services of Experian, to establish 24-month no-cost credit monitoring for impacted individuals, as well as a call center to respond to any questions affected individuals may have about the

cyberattack. If you believe you are an individual who has been impacted by this incident, instructions for how affected individuals can place and remove a security freeze, can be found in the links above.

Thank you for your immediate attention to this situation, as well as your understanding in the short-term. Our cyber security, as well as the safety and stability of our citizens, and visitors, is of the utmost importance to us and we remain committed to protecting your information. Again, we sincerely apologize for any impact caused by this incident. We will continue to monitor the incident and advise you of any updates as may be necessary.

Sincerely,

The Office of the Columbus City Auditor

THE CITY OF COLUMBUS

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

THE CITY OF COLUMBUS

FAQS ABOUT THIS NOTICE

Posted September 12, 2024

What happened?

On July 18th, the City of Columbus's Department of Technology discovered a cyber incident affecting the City's systems. Since then, the City of Columbus (the "City") has been actively working to restore services and investigate the security breach. We are also collaborating with federal authorities and cybersecurity experts to fully assess the situation. As this investigation and remediation efforts are ongoing, we encourage everyone to visit Columbus.gov/cyber regularly for the latest updates and additional details about the event.

Why am I receiving this notice?

During the investigation, it was discovered that a threat actor had obtained and posted an unencrypted backup copy of the City's General Ledger database to the dark web. This database contains financial transaction records from 1999 to 2015. While the majority of these records are public, a subset of vendors, including sole proprietors and independent contractors, may have used their Social Security Number as their tax identification number when conducting business with the City. The City Auditor is notifying vendors who fall into this category. We are sending direct notices to vendors with email addresses on file and have also posted this notice on our website.

What are General Ledger records?

General Ledger records contain the City's accounting and transactional data, including details about its assets, liabilities, revenues, and expenses. The General Ledger is the system the City uses to record and account for financial transactions. These records include information such as the transaction amount, the department or division involved, and the accounting codes used to classify the transaction. Vendor information is also included as supporting documentation for expense and liability transactions.

Why does the City still have these old records?

Ohio law, specifically Ohio Revised Code Chapter 149, establishes the rules and procedures for creating, maintaining, and accessing public records. This law requires the City to follow a retention schedule and make records available for public inspection.

The Ohio History Connection, which serves as the state archivist, also advises local governments on how to preserve and dispose of their records. General Ledger records, in particular, are recommended by the Ohio History Connection to be kept for a minimum of 25 years.

What should I do?

We encourage everyone to regularly visit Columbus.gov/cyber for the most up-to-date information. To help protect the community, the City is offering free Experian credit monitoring for two years to all current and former employees, residents, and affected individuals. This service includes $1 million in protection against fraud and identity theft. Please visit Columbus.gov/cyber and follow the instructions under "Residents and Other Affected Individuals" to sign up for this free credit monitoring service.

What other systems of the City Auditor's Office were affected?

At this time, it appears that the only City Auditor asset taken from the datacenter and posted to the dark web was the backup file of the historical financial system database.

The **City's income tax system** operates on a separate network and has remained secure and fully operational. Additionally, credit card and banking information related to online tax payments are not stored within the City's tax system.

The City's **current financial accounting system**, which holds certain vendor records, was not compromised. While accounts payable payments to vendors are processed in this system, vendor bank account information is neither collected through the Vendor Services portal nor stored in the system.

The City's **current payroll system** is also separate, ensuring employees have continued to be paid accurately and on time, without any interruption during this incident.
All three of these systems are cloud-based, and transactions are processed outside of the City's infrastructure.

Outside of this Notice, what other City systems and data were involved in the breach?

For the most up-to-date information and complete details regarding the impact on the City's systems and data, please visit Columbus.gov/cyber. This website provides the latest updates on the incident and how it affects the entire City organization.

What else can I do besides sign up for credit monitoring and identity theft protection at Columbus.gov/cyber?

In addition to signing up for credit monitoring, you can consider placing a security freeze on your credit reports. A security freeze is free, does not affect your credit score, and adds an extra layer of protection by preventing new credit from being opened in your name. You can temporarily unfreeze your credit when applying for a loan or credit card. Here are the links to request a security freeze from the three major credit bureaus:

- Experian
- Equifax
- TransUnion

Additionally, be vigilant for potential scams and identity theft. Here are steps you can take to protect yourself:

- Never give out personal information over the phone, by email, or by text unless you initiated the contact.
- Delete texts from unknown numbers.
- Avoid replying to emails asking for money, and do not click on unfamiliar links.
- Use different passwords for each of your personal accounts.
- Regularly monitor your bank and credit card statements for unauthorized activity. If you notice anything suspicious, contact law enforcement and the credit bureaus.
- You can obtain a free copy of your credit report by visiting annualcreditreport.com or calling 1-877-322-8228.