THE CITY OF
COLUMBUS

The City of Columbus
Department of Technology
P.O. Box 2949
Columbus, Ohio 43216-2949

[RESIDENT NAME]
[RESIDENT ADDRESS]

September 11, 2024

RE: Important Security Notification. Please read this entire letter.

Dear Valued Resident of Montana:

The City of Columbus (the "City"), recently discovered that it was the victim of a cybersecurity incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? 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. Further discovery indicated the incident allowed the threat actor to view and access certain sensitive personal information. The incident was discovered expeditiously, cyber security experts were retained, and proper security measures were conducted to contain the incident.

What Information Was Involved? The information subject to the incident may have included sensitive personal information, such as your first and last name, date of birth, address, bank account information, driver's licenses, Social Security number, and other identifying information.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Upon learning of the incident, the City's Department of Technology quickly identified the threat and took action to significantly limit potential exposure by severing internet connectivity and immediately mobilizing a response team. The City engaged cyber security experts to guide them through this occurrence, and 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. Law enforcement was notified, and the City has retained legal counsel to ensure that response and remediation comply with all federal, state and local laws and regulations.

Additionally, the City is in the process of conducting a full forensic security audit to determine the extent of the incident. The Department of Technology, working with federal authorities and cybersecurity experts, has been engaged in a methodical process to ensure that its technology systems are hardened against further breach before bringing them back online. Thankfully, the emergency systems have remained operational throughout these efforts to protect and restore IT connectivity. The incident remains ongoing and the investigation is in its earliest stages. The City will continue to work closely with the Department of Technology, and our cyber security experts, to ensure we remain vigilant in the security of our operations.

What Actions You Can Take? As always, we recommend that you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You should report any suspicious activity to the appropriate service provider. If you observe unusual activity on any debit/credit card or you believe your personal bank account shows signs of compromise – we advise you to close out those accounts and request new cards and account credentials.

Additionally, you should report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general. To file a complaint with the FTC, go to IdentityTheft.gov or

call 1-877-ID-THEFT (1 (877) 438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general can be found below:

Attorney General Anthony G. Brown
Office of the Attorney General
Justice Building, Third Floor
215 North Sanders
P.O. Box 201401
Helena, MT 59620-1401
Phone: (406) 444-2026
E-mail: contactdoj@mt.gov
https://dojmt.gov/agooffice/

Please take advantage of additional free resources on identity theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacyidentity-online-security.

For more information, visit IdentityTheft.gov or call 1-877-ID-THEFT (1-877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, is on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_ recovery_plan.pdf.

Placing a Security Freeze

Any consumer in Montana may place a free security freeze on his or her credit report by: (i) requesting one in writing by certified mail to the consumer reporting agency, (ii) calling the agency directly, or (iii) submitting a form online directly to the agency. The consumer reporting agency is not allowed to charge a fee to victims for placing, removing for a specific period or party, or removing a security freeze on a credit report. To avoid a fee, the victim may need to send a valid copy of a police report to the consumer reporting agency. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. We recommend that you work collaboratively with potential lenders, employers and service providers to ensure that you are protecting both your information and the approval status of your applicable request.

In order to place a security freeze on your credit reports, you must contact all three bureaus and pay a fee to each, where applicable. For victims of identity theft, there are no fees. Your request to place a security freeze must be to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com), at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(888) 298-0045
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
https://www.experian.com/freeze/center.html

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8872
https://www.transunion.com/credit-freeze

The credit reporting agencies have five (5) business days after receiving your request to place a security freeze on your credit report, so we recommend placing the freeze as soon as you possibly can. However, if you are a victim of identity theft, the credit reporting agencies have 24 hours to place a security freeze after receiving notice, along with a valid police report, investigative report, or complaint filed with a law enforcement agency. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

Lifting or Suspending a Security Freeze

To temporarily lift or suspend the security freeze in order to allow a specific entity or individual access to your credit report, you must mail a request, call, request one online, or send a request via electronic media to the credit reporting agencies and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies shall comply with a request to temporarily lift a security freeze within three (3) business days after receiving such request via mail, or within 15 minutes if the request is received via telephone or secure electronic request.

Removing a Security Freeze

To remove the security freeze, you can either submit the request online, or send a written request to each of the three credit bureaus by mail, secure electronic method, or via their online form, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Monitoring

Based on recent public feedback as a good government community partner, and out of an abundance of caution, we are expanding our offer of no-cost credit monitoring to all those who believe they may have been impacted. To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 29, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **WQHW435TZR**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's

customer care team at 1**(833) 918-5161** by **November 29, 2024**. Be prepared to provide engagement number **B129832** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online please call 1**(833) 918-5161** toll-free **Monday through Friday from 9 am – 9 pm Eastern** (excluding major U.S. holidays). Be prepared to provide your engagement number **B129832**.

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,

Andrew J. Ginther
Mayor, City of Columbus

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.