

March 12, 2024

Via Email: consumer_protection@ag.idaho.gov
Attorney General Raul Labrador
Office of the Idaho Attorney General
Consumer Protection Division
954 W. Jefferson, 2nd Floor
Boise, ID 83720

Re: Supplemental Notice of Data Security Incident

Dear Attorney General Labrador:

This notice is provided on behalf of my client, the City of Coeur D'Alene (the "City") as a supplement to the prior notice submitted to your office on February 14, 2024 (the "Prior Notice") regarding a ransomware attack that the City detected on February 11, 2024. As described in the Prior Notice, the City immediately began an investigation, with the assistance of legal counsel and a nationally-recognized cyber security and digital forensics firm to restore operations, investigate the scope of the incident and mitigate any resulting harm and also cooperated with Federal law enforcement's investigation. In the Prior Notice, the City reported that on February 13, 2024, it discovered that this incident involved unauthorized acquisition of personal information, as defined by Idaho law.

As part of its investigation the City conducted a thorough review of the City data that it believed was removed from the network in order to establish what information may have been involved, who may have been affected, and where those people reside so that it could provide notice. On February 29, 2024, the City completed the review of that data and began locating mailing addresses for individuals whose information was impacted, so that we could provide them with written notice of this incident. The affected data included Idaho residents' names, Social Security numbers, and driver's license and/or state identification card number.

The investigation of the data that we believe was impacted is now complete, and we will provide written notice to a total of fifty-seven (57) residents of Idaho on March 12, 2024. The notice letter includes general advice on how to protect one's identity, obtain free credit reports and security freezes, as well as instructions for enrolling in a one-year, complimentary membership with Experian for credit monitoring and identity theft services. A sample notice letter is enclosed an additional information regarding our response to this incident is below.

Because cyber threats are always evolving, the City is continuously working to identify and mitigate threats and evaluate its IT security protocols to protect sensitive data. To further enhance its security and to help prevent similar occurrences in the future, the City has taken or will be taking the following steps:

1. Deploying security tools to enhance detection and accelerate response to cyber incidents;
2. Conducted enterprise-wide password reset; and
3. Investing in hardware and system enhancements to further protect against cyber incidents.

In addition, consistent with our compliance obligations and responsibilities, we provided notice of this incident and regular updates to the Idaho Chief Information Security Officer and other state regulators as required under applicable law.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

Matthew H. Meade, Esq.



MUNICIPAL SERVICES DEPARTMENT
OFFICE OF THE CITY CLERK

CITY HALL, 710 E. MULLAN
COEUR D'ALENE, IDAHO 83816-3964
208/769-2231
FAX (208)769-2388

March 12, 2024

<<Full Name>>
<<Address 1>>
<<City, State, Zip>>

NOTICE OF DATA SECURITY INCIDENT

Dear <<Full Name>>:

The City of Coeur D'Alene (the "City") is writing to tell you about a recent cyber incident that involved personal information that we maintain related to law enforcement and/or court related matters. We take this matter very seriously because we are committed to the privacy and security of all information in our possession. **At this time, we are not aware of any misuse of your information.** However, we are providing this notice to you to inform you of the incident, offer complimentary identity monitoring services, and suggest ways that you can protect your information.

What Happened

On February 11, 2024, the City detected and responded to a ransomware attack on our computer network. We immediately began an investigation with assistance from a nationally recognized cyber security and digital forensics firm and notified federal law enforcement. Through our investigation, we learned that there was unauthorized access to the City's network between February 4 and February 11, 2024, and that the cyber criminals removed certain files from our servers during the attack. As soon as we learned this, we began an extensive review to determine what information may have been involved and who may have been affected, so that we could provide notice. On February 29, 2024, we completed the review and began locating mailing addresses for individuals whose information was impacted, so that we could provide them with written notice of this incident.

What Information Was Involved

The affected data included your <<variable>>.

What We Are Doing About It

Our investigators searched Dark Web sources and found no indication that any personal information that the City maintains had been released or offered for sale as a result of this incident. To further enhance our security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Deploying security tools to enhance detection and accelerate response to cyber incidents;
2. Conducted enterprise-wide password reset; and
3. Investing in hardware and system enhancements to further protect against cyber incidents.

We continue to cooperate with law enforcement's ongoing investigation. Additionally, we have provided notice of this incident to the Idaho Attorney General's office and will notify all appropriate state regulators.

What You Can Do

We recommend that you take the following preventative measures to help protect your information:

1. Enroll in a complimentary, 12-month membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.
2. Remain alert for incidents of fraud and identity theft by regularly reviewing any account statements, free credit reports for unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.
3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and will continue to take many precautions to safeguard it. If you have any questions or concerns about this incident, you may contact us at 208-769-2231, between 8:00 a.m. and 5:00 p.m. PST, Monday through Friday.

Sincerely,



Renata McLeod,
City Clerk

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit <https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/> for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at <https://consumer.ftc.gov/features/identity-theft>. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com
--	---	--

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. 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 consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf> and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report. You may be able to obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line,

or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above. This notice was not delayed as a result of a law enforcement investigation.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by: June 30, 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: [CM Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(877) 890-9332** by **June 30, 2024**. Be prepared to provide engagement number **B117688** as proof of eligibility for the identity restoration services by Experian. 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.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 at **(877) 890-9332**. 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 this Identity Restoration support is available to you for 12 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. You will also find self-help tips and information about identity protection at this site.

* 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.