



ELMORE COUNTY PROSECUTING ATTORNEY

SHONDI K. LOTT
PROSECUTING ATTORNEY

190 South 4th East
Mountain Home, Idaho 83647
Phone: (208) 587-2144 Ext. 503
Facsimile: (208) 587-2147
e-mail: prosecutor@elmorecounty.org

January 13, 2022

Office of the Attorney General, State of Idaho
Brett Delange, Deputy A.G./Chief
Consumer Protection Division
P.O. Box 83720
Boise, Idaho 83720-0010
Via email to brett.delange@ag.idaho.gov
consumer_protection@ag.idaho.gov

Re: Supplemental/Final Notice of Data Breach

Dear Mr. Delange:

This notice is provided on behalf of Elmore County, as a supplement to the prior notices submitted to your office on December 14, 2022, and December 15, 2022 (the "Prior Notices"). In the Prior Notices, we provided notice of a data breach that appeared to impact three email accounts belonging to Elmore County employees. We immediately began working with Sylint, a digital forensic firm, and legal at Eckert Seamans Cherin & Mellott, LLC, to secure the email environment and investigate the scope of the incident.

The forensic investigation determined that only one email account was subject to a breach of the security of the system, as defined in Idaho Code § 28-51-104(2). We then worked with legal counsel and the digital forensics firm to review the entire contents of the impacted email box to determine what information may have been affected and to whom that information relates, to provide proper notice. The affected data included Idaho residents' names, social security numbers, driver's license and/or state identification card number. For one individual, a payment card number with accompanying CVV and expiration date was affected.

The investigation is now complete, and we will provide written notice to a total of eleven individuals on January 13, 2022. 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, we continuously work to mitigate threats and evaluate our IT security protocols to ensure that sensitive data is protected. To further enhance email and network security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

Lee Fisher
*Chief Deputy
Prosecuting
Attorney*

Ralph R. Blount
*Deputy Prosecuting
Attorney*

Elizabeth A. Harrison
*Deputy Prosecuting
Attorney*

Hayes Hartman
*Deputy Prosecuting
Attorney*

Philip R. Miller
*Deputy Prosecuting
Attorney*

1. Changed passwords and took steps to further secure any impacted email accounts,
2. Geoblocking certain foreign IP addresses,
3. Working to implement two factor authentication to our email accounts; and
4. Reviewing and strengthening security policies and procedures.

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.

On behalf of Elmore County Prosecutor Shondi K. Lott, thank you.

Ralph R. Blount
Ralph R. Blount
Deputy Prosecutor

cc: Sandy Moser, ICRMP

CLERK OF THE DISTRICT COURT
ex officio, AUDITOR, RECORDER
ELMORE COUNTY COURTHOUSE
150 South 4th East Suite #3
State of Idaho
Mountain Home 83647-3097

January 13, 2023

<<Full Name>>
<<Address 1>>
<<Address 2>>

NOTICE OF DATA SECURITY INCIDENT

Dear <<Full Name>>:

We are writing to tell you about a recent incident that involved Elmore County (the “County”) employee email accounts. Based on our investigation, we discovered unauthorized access to and removal of the contents of one County employee’s email box, including information about some employees, contractors, and others related to the County. At this time, we have no indication that any of your personal information has been inappropriately used by anyone. However, we are providing this notice to you as a precautionary measure, to inform you, explain the complimentary services that we are offering you, and suggest ways that you can protect your information.

What Happened

On December 13, 2022, we learned that a County email address was sending a large number of suspicious emails without authorization. We immediately launched an investigation, with the assistance of a nationally recognized digital forensics firm, to determine the nature and scope of this incident. The investigation determined that data which appeared to contain personal information had been removed from one County email account on December 13, 2022. We then worked with legal counsel and the digital forensics firm to review the entire contents of the impacted email box to determine what information may have been affected and to whom that information relates, so that we could provide proper notice. On December 21, 2022, we confirmed that the email account contained personal information relating to certain individuals. We then began locating mailing addresses for those individuals, so that we could inform them of this incident.

What Information Was Involved

Based upon our investigation, the impacted information included your name, Social Security number, and/or driver’s license number.

What We Are Doing About It

When we discovered this incident, we immediately secured the email account and notified all recipients of the suspicious emails. To further enhance email and network security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Changed passwords and took steps to further secure any impacted email accounts,
2. Geoblocking certain foreign IP addresses,
3. Working to implement two factor authentication to our email accounts; and
4. Reviewing and strengthening security policies and procedures.

In addition, consistent with our compliance obligations and responsibilities, we provided notice of this incident to the Idaho Attorney General's office and have been providing regular updates to the Idaho Chief Information Security Officer.

What You Can Do

Although we have no evidence of any misuse of personal information involved in this incident, as a precaution, we recommend that you take the following preventative measures to help protect your information:

1. Enroll in a complimentary, one-year 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 vigilant for incidents of fraud and identity theft by regularly reviewing your account statements, and free credit reports for any 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, the major credit bureaus and/or the Federal Trade Commission.

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 by calling us at (208) 587-2130, extension 1212, between the hours of 9:00 a.m. to 12 p.m. and 1 p.m. to 4:00 p.m. MST, Monday through Friday.

Sincerely,



Shelley Essl
Elmore County Clerk of the District Court

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 www.consumer.ftc.gov/features/feature-0014-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 1-888-909-8872 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: 4/30/2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code: <<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 **4/30/2023**. Be prepared to provide engagement number **<<ENGAGEMENT>>** 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 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 (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 one year 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.