

March 24, 2022

**Via electronic mail:**  
**stephanie.guyon@ag.idaho.gov**  
Office of the Attorney General  
State of Idaho  
700 W. Jefferson Street, P.O. Box 83720  
Boise, ID 83720

Re: Follow-up to Notice of Data Breach

Dear Attorney General Wasden:

This letter is in follow-up to the March 4, 2022 Notice of Data Breach provided on behalf of Teton County (the "County").

As you may recall, the County had an issue impacting the public records request search function on the County website, where searches for otherwise public records could have returned unintended information. More specifically, in late December 2021, the County learned of an issue relating to its online portal used for public record searches on its website (*laserfiche2015.co.teton.id.us*). The portal utilized an application named Laserfiche to allow County residents to search for copies of their recorded documents, such as deeds, notice of liens, court records, and other publicly available documents. The County discovered that some of these documents contained sensitive information that should not have been publicly available.

Once it learned of this issue, the County launched an investigation and engaged legal counsel with an expertise in cybersecurity. Legal counsel also hired a nationally recognized cyber security and digital forensics firm to assist with the investigation so that the County could better understand what happened, and, more importantly, prevent something like this from happening again. Through its investigation the County determined that personal information in these documents could have potentially been accessible to the public from when they were uploaded until December 22, 2021. After learning this, the County immediately removed access to the portal and later took steps to secure all such personal information from future online searches.

The investigation revealed that a limited amount of the information that was searched and accessible within the online portal included personal information. The County conducted an extensive review of this data to determine what information may have been involved, who may have been affected, and where those people reside so that it could provide proper notice. Based upon its review the County provided written notice of a data breach to approximately 60 Idaho residents today. The notice letter includes general advice on how to protect one's identity and 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 where a driver's license or Social Security number was involved. A sample notice letter is enclosed and additional information on the incident is below. In addition, the County has been providing regular updates about this incident to the Idaho Chief Information Security Officer, Chief Information Officer and Office of Risk Management.

The County is committed to making this right and is investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. Because cyber threats are always evolving, the County is continuously working to identify and mitigate threats and evaluate its IT security

protocols to make sure that sensitive data is protected. In addition, to help prevent similar occurrences in the future, the County has taken or will be taking the following steps:

- Searching all documents for sensitive information so they can be removed from the public records database; and
- Ensuring newly added documents do not contain sensitive information.

The County is committed to protecting the security and confidentiality of sensitive information and will continue to invest in the internal resources and tools necessary to help prevent something like from happening again. Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

*Matthew H. Meade*

Matthew H. Meade, Esq.

Enclosure



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

**Board of County Commissioners**

Cindy Riegel – [criegel@co.teton.id.us](mailto:criegel@co.teton.id.us)  
Bob Heneage – [bheneage@co.teton.id.us](mailto:bheneage@co.teton.id.us)  
Michael Whitfield – [mwhitfield@co.teton.id.us](mailto:mwhitfield@co.teton.id.us)  
[www.tetoncountyidaho.gov](http://www.tetoncountyidaho.gov)

1 1 108 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



March 24, 2022

**NOTICE OF DATA SECURITY INCIDENT**

Dear Sample A. Sample:

The privacy and security of your personal information is of the utmost importance to Teton County (the “County”). We are writing with important information regarding a recent data security incident that involved our online portal used for public record searches. We are providing this notice as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering you, and suggest ways that you can help protect your information.

**What Happened**

The County recently learned of an issue relating to its online portal used for public record searches on its website [laserfiche2015.co.teton.id.us](http://laserfiche2015.co.teton.id.us). The portal utilized an application named Laserfiche to allow County residents to search for copies of their recorded documents, such as deeds, notice of liens, court records and other publicly available documents. We discovered that some of these documents contained sensitive information that should not have been publicly available. Personal information in these documents could have potentially been accessible to the public through the portal from when they were uploaded until December 22, 2021. As soon as we learned this, we immediately removed access to the portal and secured all such personal information from future online searches. We also launched an investigation and engaged legal counsel with an expertise in cybersecurity. Legal counsel also hired a nationally recognized cyber security and digital forensics firm to assist with the investigation so that the County could better understand what happened, and, more importantly, prevent something like this from happening again.

The investigation revealed that a limited amount of the information that was searched and accessible within the online portal included personal information. We immediately began an extensive review of this data to determine what information may have been involved, who may have been affected, and where those people reside so that we could provide proper notice. On March 3, 2022, we learned that the data included your personal information.

**What Information Was Involved**

Based upon our investigation, that information may have included your name, address, date of birth, and Social Security number.

**What We Are Doing About It**

Again, we have secured all such personal information from future online searches. We have conducted a Dark Web search and found no credible evidence of County data on the Dark Web as a result of this incident. We are committed to making this right and are investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. Because cyber threats are always evolving, we are continuously

working to identify and mitigate threats and evaluate our IT security protocols to make sure that sensitive data is protected. As you can probably imagine, this is a constant battle in our world today. In addition, to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

- Searching all documents for sensitive information so they can be removed from the public records database; and
- Ensuring newly added documents do not contain sensitive information.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state regulators.

### **What You Can Do**

We are notifying you so that you can take steps to protect yourself. We recommend that you remain vigilant to the possibility of fraud and identify theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity. If you find any unauthorized or suspicious activity, you should contact local law enforcement.

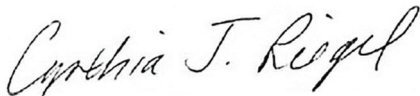
We strongly encourage you to take the following preventative measures to help detect and mitigate any misuse of your information:

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 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 by calling us at 208-354-2703 between the hours of 9:00 a.m. to 5:00 pm, MDT, Monday through Friday.

Sincerely,



**Cindy Riegel, Chair**



**Greg Adams, IT Director**

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit [www.experian.com/credit-advice/topic-fraud-and-identity-theft.html](http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html) 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](http://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

|  |   |  |
|--|---|--|
| <b>Equifax</b><br>P.O. Box 105788<br>Atlanta, GA 30348<br>1-888-298-0045<br><a href="http://www.equifax.com">www.equifax.com</a> | <b>Experian</b><br>P.O. Box 9554<br>Allen, TX 75013<br>1-888-397-3742<br><a href="http://www.experian.com">www.experian.com</a> | <b>TransUnion</b><br>P.O. Box 160<br>Woodlyn, PA 19094<br>1-888-909-8872<br><a href="http://www.transunion.com">www.transunion.com</a> |
|--|---|--|

### 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](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/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.

**For Colorado, Georgia, Maryland and Vermont residents:** You may 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 at least 90 days. 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](http://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.

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.

## **STATE SPECIFIC INFORMATION**

**MARYLAND residents:** You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
[www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer)  
Toll-free: 1-888-743-0023

**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, 2022
- **Visit** the Experian IdentityWorks website to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
- Provide your **activation code**: **ABCDEFGHI**

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, 2022. Be prepared to provide engagement number B028970 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](http://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.