

March 23, 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 February 23, 2022 Notice of Data Breach provided on behalf of Shelley School District, located in Shelley, Idaho (the "District"). As you may recall, a ransomware attack affected the District late last year. The District immediately began working with cybersecurity experts and legal counsel to contain and eradicate any malware, investigate the scope of the incident, and determine whether the incident involved personal information.

The investigation is now complete and the District will provide written notice of a data breach to approximately 171 Idaho residents on March 24, 2022. 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.

After the investigation confirmed that the cybercriminals removed data from the District's environment, the District performed a comprehensive and thorough review of the data in order to determine what information was involved, who may have been affected, and where those people reside so that it could provide proper notice. With assistance from its legal counsel and forensic experts, the District determined that the affected data could have included Idaho residents' names, dates of birth, addresses, and Social Security or driver's license numbers. For a small number of individuals, a bank account number, routing number or payment card number with accompanying CVV and expiration was also included.

Because cyber threats are always evolving, the District continuously works to mitigate threats and evaluates its IT security protocols to ensure that sensitive data is protected. To further improve its network security, the District has taken, or will be taking, the following steps:

- Deploying end-point detection and response tools to enhance network monitoring;
- Deleting or archiving outdated information;
- Adding Multi-Factor Authentication;
- Strengthening backups and ability to recover data from backups;
- Closely monitoring and restricting outside access to its computer network;

- Increasing password complexity requirements;
- Strengthening email filtering to help block dangerous emails;
- Updating its incident response procedures to more quickly and effectively respond to incidents; and
- Enhancing cyber training and providing regular communications in order to increase cyber awareness.

In addition, the District notified the Federal Bureau of Investigation (FBI) and has been providing regular updates about this incident to the Idaho Chief Information Security Officer, Chief Information Officer and Office of Risk Management.

The District 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.

Shelley School District #60

545 Seminary Avenue
Shelley, Idaho 83274

 208-357-3411  208-357-5741



"Where Students Come First"

March __, 2022

<First> <MI> <Last>
<Address>
<City>, <State> <Zip>

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear <First> <MI> <Last>:

Shelley School District (the "District") is writing with important information regarding a recent data security incident that involved information that we maintain about our current or former students, employees, or their families, including information related to you. We wanted to tell you about the incident, explain the complimentary services that we are offering, and let you know that we continue to take significant measures to protect your information.

What Happened

On December 6, 2021, a ransomware attack impacted our IT system. District IT staff immediately launched an investigation and hired legal counsel with an expertise in cybersecurity. Legal counsel also hired a nationally-recognized cyber security and digital forensics firm to assist us so that we could better understand what happened and help prevent something like this from happening again.

The District worked closely with its experts to contain the attack, securely restore operations and determine whether the incident involved personal information. The investigation revealed that the cybercriminals removed data from our environment before deploying the ransomware. With the assistance of our legal counsel and cyber team, we thoroughly reviewed the affected data in order to determine what information may have been involved, who may have been affected, and where those people reside so that we could provide notice. On February 22, 2022, we learned that the data included your information.

What Information Was Involved

Based upon the investigation, your name, date of birth, address, and Social Security or driver's license number may have been involved in the incident.

What We Are Doing

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. In addition, to further improve our network security and help prevent similar occurrences in the future, we have taken, or will be taking, the following steps:

- Deploying end-point detection and response tools to enhance our network monitoring;
- Deleting or archiving outdated information;

- Adding Multi-Factor Authentication;
- Strengthening backups and ability to recover data from backups;
- Closely monitoring and restricting outside access to our computer network;
- Increasing password complexity requirements;
- Strengthening our email filtering to help block dangerous emails;
- Updating our incident response procedures to more quickly and effectively respond to incidents; and
- Enhancing our cyber training and providing regular communications in order to increase cyber awareness.

In addition, we notified the Federal Bureau of Investigation and have been providing regular updates about this incident to the Idaho Chief Information Security Officer. We also notified the Idaho State Department of Education and the Idaho Attorney General's office.

What You Can Do

We recommend that you take the following preventative measures to help detect and mitigate any potential misuse of your personal 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 further questions regarding this incident, please contact Blake Jenson, Director of Operations, at 208-357-5760, Monday-Thursday between the hours of 8:00 AM and 4:00 PM, MST.

Sincerely,



Mr. Chad Williams,
Superintendent of Schools

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit 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. 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 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.

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.

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.

**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: [date]** (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 **[date]**. Be prepared to provide engagement number **[insert]** 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.