ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

VIA ELECTRONIC MAIL:
stephanie.guyon@ag.idaho.gov

January 14, 2021 *2022*

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 Security Incident

Dear Attorney General Wasden:

This letter is in follow-up to the October 19, 2021 Notice of a Data Security Incident provided on behalf of Valley Regional Transit (VRT), the Regional Public Transportation Authority (RPTA) for Ada County and Canyon County, Idaho. As you may recall, a ransomware attack affected certain VRT systems in October of 2021. VRT 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 VRT will provide written notice of a data breach to approximately 477 Idaho residents next week. 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.

On October 18, 2021, the cybercriminals indicated that they had removed certain folders from VRT's network prior to deploying the ransomware. On October 19, 2021, VRT began reviewing the contents of the folders identified by the threat actors and determined that it contained personal information of Idaho residents. VRT's forensic experts then obtained a decrypted copy of all exfiltrated data. Legal counsel reviewed this data in order to determine what information was involved, who may have been affected, and where those people reside so that VRT could provide proper notice.

Legal counsel completed its review of the affected data on December 20, 2021, and determined that the incident involved the names, dates of birth, addresses, Social Security numbers, or driver's license numbers of Idaho residents. The incident also involved one individual's payment card number with the accompanying expiration date. In the weeks following the legal review, VRT worked diligently to locate addresses for all individuals but was unable to find mailing addresses for 38 individuals that are presumed to be Idaho residents based on the population VRT serves. As a result, VRT will providing substitute notice in major statewide media and on its website.

VRT is continuing to monitor its network to ensure containment, and prohibit the spread, of any new or residual malware. SentinelOne has not identified anything of concern related to the ransomware incident. Because cyber threats are always evolving, VRT continuously works to mitigate threats and evaluates its IT security protocols to ensure that sensitive data is protected. To further improve its network security, VRT has taken, or will be taking, the following steps:

1. Enhancing security so that VRT can limit and restrict access to its computer network;
2. Installing an intrusion detection system that monitors for malicious activity;
3. Patching identified system vulnerabilities, including the vulnerability that led to this incident;
4. Enhancing patch management procedures to ensure that patches are promptly deployed;
5. Reviewing the network to ensure that personal information is stored in secure areas designated for sensitive information; and
6. Implementing greater security for VRT administrator accounts used to manage the network.

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

VRT 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.

5. Reviewing our network to ensure that personal information is stored in secure areas designated for sensitive information; and
6. Implementing greater security for VRT administrator accounts used to manage our network.

In addition, VRT notified the Federal Bureau of Investigation and the Transportation Security Administration. We also have been providing regular updates about this incident to the Idaho Chief Information Security Officer, Attorney General, Chief Information Officer and Office of Risk Management.

What You Can Do

In an abundance of caution, 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 monitoring free credit reports for any unauthorized 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

We sincerely regret any inconvenience this incident may cause you. **If you have any further questions regarding this incident, please contact us at 208-258-2777**, Monday through Friday, 8 a.m. to 4 p.m., MT.

Sincerely,

Kelli Badesheim
Executive Director, Valley Regional Transit

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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	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 **[number]** 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.