



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Brittany R. Bickel
Office: (267) 930-1129
Fax: (267) 930-4771
Email: bbickel@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 22, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom it May Concern:

We represent Verified Carbon Standard Association (“Verra”) located at One Thomas Circle, Northwest, #1050, Washington, DC 20005, and are writing to notify your office of an incident that may affect the security of certain personal information relating to eighteen (18) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Verra does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 12, 2022, Verra identified suspicious activity related to an employee’s email account. Upon learning of the suspicious activity, Verra immediately took steps to secure the email account and launched an investigation, with the assistance of third-party computer forensics specialists, to determine the nature and scope of the event. The investigation confirmed that certain employees’ email accounts were accessed by an unknown actor for various periods of time between January 23, 2022, and April 13, 2022.

Although the investigation was unable to confirm whether the unknown actor viewed any emails or attachments while in the accounts, Verra could not rule out the possibility that some information contained within the accounts may have been impacted. Therefore, in an abundance of caution, Verra worked with specialists to perform a comprehensive programmatic and manual review of the information stored in the email accounts at the time of the event to identify the types of

information contained within the accounts and to whom it related. This review was completed on October 4, 2022, and it was determined that information related to certain individuals was present in the impacted email accounts. Verra then conducted further review of its records to validate the data and confirm the identities and contact information for potentially affected individuals to provide notifications. The information that could have been subject to unauthorized access may vary by individual but includes name, Social Security number, driver's license number, financial account information, payment card information, medical information, and health insurance information.

Notice to Maryland Residents

On or about December 22, 2022, Verra began providing written notice of this incident to eighteen (18) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Verra enforced multi-factor authentication, locked legacy authentication, added cloud filter for spam filtering on our mailboxes, implemented conditional access policies for geolocation blocking, enabled advanced threat protection safe links, safe attachments, and anti-phishing policies, lowered the recipient limit to slow large-scale phishing attempts, and created mail flow rule for external messages that alert receipts that the message originated from outside the organization. Verra is also working on configuring data loss prevention to detect and act on sharing sensitive information externally.

Upon becoming aware of the event, Verra moved quickly to investigate and respond to the incident, assess the security of Verra systems, and identify potentially affected individuals.

Verra is also working on configuring data loss prevention to detect and act on sharing sensitive information externally and providing regular cyber security training to all employees. Verra is providing access to credit monitoring services for twelve (12) months through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Verra is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Verra is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Office of the Attorney General

December 22, 2022

Page 3

Verra is providing written notice of this incident to relevant federal and state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1129.

Very truly yours,

Brittany R. Bickel of
MULLEN COUGHLIN LLC

BRB/nad
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

111 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



December 22, 2022

NOTICE OF [EXTRA1]

Dear Sample A. Sample:

I am writing to inform you of an event that may involve some of your personal information. Although there is no indication that your information has been misused in relation to this event, we are providing you with this notification to describe what happened and how we responded, and to offer resources to help you protect your information.

What Happened? On or about April 12, 2022, we became aware of suspicious activity relating to an employee's email account. We immediately took steps to secure all email accounts and launched an investigation to determine the nature and scope of the activity. The study determined that there was unauthorized access to certain employees' email accounts for varying periods of time between January 23, 2022, to April 13, 2022.

Although we could not confirm whether the unknown actor viewed any emails or attachments while in the accounts, we could not rule out the possibility that some information contained within the accounts may have been impacted. Out of an abundance of caution, we undertook a comprehensive and time-intensive review of the contents of all the affected email accounts to determine whether sensitive information was present in the emails during the period in question. We recently completed that process. We are notifying you because that investigation determined that certain information related to you was present in the impacted email accounts.

What Information Was Involved? The information that this incident may have impacted includes your [Extra2], and name. To date, we have not received any reports of fraudulent misuse of any information as a result of this incident.

What We Are Doing. Data privacy and security are among our highest priorities, and we have security measures in place to protect information in our care. Upon learning of the activity, we immediately took steps to further secure our systems and investigate the event. We will also notify applicable state regulators, as necessary.

We are unaware of any fraudulent misuse of your information as a result of this incident, but as an added precaution, we are also offering [Extra3] months of complimentary access to credit monitoring services through Experian. Please follow the attached enrollment instructions if you wish to receive these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the enclosed *Steps You Can Take to Help Protect Your Information* to learn helpful tips to protect your information, should you feel it appropriate to do so. There you will find more information on the credit monitoring services we are making available to you. While Verra will cover the cost of these services, you will need to complete the enrollment and activation process.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or need assistance, please call our dedicated assistance line at (833) 541-1592 toll-free Monday through Friday from 8 am - 10 pm Central or Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number]. You can also write to Verra at emailus@verra.org or One Thomas Circle, NW, Suite 1050, Washington, DC 20005 ATTN: IT Security.

We apologize for any inconvenience or concern this incident may cause.

Sincerely,

A handwritten signature in black ink, appearing to read "William M. Ferretti", is displayed on a light gray rectangular background.

William M. Ferretti
Chief Operating & Financial Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra3] months.

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. 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 Identity Restoration is available to you for [Extra3] 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** February 28, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 541-1592 by February 28, 2023. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [EXTRA3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident.