



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

December 19, 2023

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 Great Valley School District (“Great Valley”), located at 100 Lindenwood Drive Malvern, PA 19355, and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately eight (8) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Great Valley 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 November 10, 2023, Great Valley became aware of a disruption to its technology network. Great Valley promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. Great Valley subsequently learned that, between October 31, 2023 and November 10, 2023, an unauthorized actor gained access to certain Great Valley systems and may have viewed or taken certain information contained in those systems. On November 21, 2023, the investigation also determined that the information potentially accessible during the event may have included personal information, including personal information relating to Great Valley employees and students.

Great Valley conducted a thorough review to identify the specific types of personal information potentially impacted and to whom such information relates. While this review process was still

ongoing, on November 27, 2023, Great Valley posted notice on its website that an event occurred which may involve unauthorized access to such information.

Great Valley completed its review on November 30, 2023, and then moved as quickly as possible to mail written notice to individuals for whom it currently has address information. For Maryland residents, the types of personal information potentially accessible during the event include the following: name, address, date of birth, Social Security number, driver's license, state ID, medical information, and financial account information.

Notice to Maryland Residents

On December 19, 2023, Great Valley began mailing written notice of this event to potentially impacted individuals, including approximately eight (8) 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

Upon becoming aware of the event, Great Valley moved quickly to investigate and respond to the event, assess the security of its network, determine whether personal information was potentially impacted, and notify potentially affected individuals. Great Valley notified federal law enforcement and will cooperate with any investigation they may conduct into this event. Additionally, Great Valley is working to implement additional administrative and technical safeguards to further enhance the security of its network. Great Valley also is providing access to identity monitoring services for twelve (12) months, through Equifax, to Maryland residents whose personal information was potentially affected by this event, at no cost to those individuals.

Additionally, Great Valley 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 bank, credit card company, or other applicable institution. Great Valley is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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.

Great Valley is providing written notice of this event to relevant state regulators, as required, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion. Pursuant to the Family Educational Rights and Privacy Act ("FERPA"), Great Valley also is documenting this event in the education records of any students whose information was identified as potentially impacted by this event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/aml
Attachment

EXHIBIT A



Great Valley School District

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

>>Mailing ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

<<Date>>

<<VARIABLE HEADER>>

Dear <<Name 1>>:

Great Valley School District ("Great Valley") is writing to inform you of a recent event that may impact the security of some of your information. Although we have received no confirmation of any actual or attempted identity theft or fraud as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened. On November 10, 2023, Great Valley became aware of a disruption to our technology network. That same day, we launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. We subsequently learned that, between October 31, 2023 and November 10, 2023, an unauthorized actor gained access to certain Great Valley systems and may have viewed or taken certain information contained in those systems, potentially including personal information related to individuals.

We conducted a thorough review to identify the specific types of personal information potentially impacted and to whom such information relates. While this review process was still ongoing, on November 28, 2023, we shared publicly that an event occurred that may involve unauthorized access to such information.

We recently completed our review and determined that the information potentially accessible may have included personal information related to you. Accordingly, we moved as quickly as possible to notify you directly of the event.

What Information Was Involved. The investigation determined that your name, address, <<Breached Elements>> were potentially accessible during the event.

What We Are Doing. The safety of our community, as well as the confidentiality, privacy, and security of information in our care, are our highest priorities. Upon becoming aware of the event, we moved quickly to investigate and respond to the event, assess the security of our network, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information from possible misuse, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering credit monitoring and identity restoration services through Equifax for <<12/24>> months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank, credit card company, or other applicable institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring and identity restoration services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 877-882-0687, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call. Again, we take the confidentiality, privacy, and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel Goffredo". The signature is fluid and cursive, with the first name "Daniel" being more prominent than the last name "Goffredo".

Daniel Goffredo, Ed.D.
Superintendent of Schools
Great Valley School District

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services

Enter your Activation Code: <<Activation Code>>

Enrollment Date: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a fraud alert or 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	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; 1-202-727-3400; 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 <https://www.marylandattorneygeneral.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.