MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

June 29, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

To Whom It May Concern:

We represent Peters Township School District ("PTSD") located at 631 East McMurray Road, McMurray, PA 15317, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two (2) New Hampshire residents. By providing this notice, PTSD does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 5, 2022, PTSD became aware that certain computer servers and systems in its environment were inaccessible. PTSD immediately took steps to secure its systems and conducted an investigation to determine the full nature and scope of the activity with assistance from third-party cybersecurity and digital forensic specialists. PTSD also promptly reported the event to federal law enforcement.

Through its investigation, PTSD determined that its systems were accessible to an unknown actor between February 11, 2022, and April 5, 2022. Although the investigation was unable to determine whether information stored in the impacted servers had actually been taken or viewed by the unauthorized actor, the possibility of such activity could not be ruled out. Therefore, in an abundance of caution, PTSD conducted a time-intensive and thorough programmatic and manual review of the information stored on the impacted systems and determined that certain sensitive information was contained therein. Following this review, PTSD conducted additional review of its records to confirm the identities and contact information for potentially affected individuals in order to provide notification. This review was recently completed.

The information that could have been subject to unauthorized access may vary by individual and includes

Notice to New Hampshire Residents

On or about June 29, 2023, PTSD provided written notice of this incident to two (2) New Hampshire 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, PTSD moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals. Further, PTSD notified federal law enforcement regarding the event. PTSD is also working to implement additional safeguards to better prevent a similar event from recurring in the future. Moreover, PTSD is providing access to credit monitoring services for through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, PTSD 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. PTSD 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.

PTSD is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at

Very truly yours,

Brittany R. Bickel of
MULLEN COUGHLIN LLC

BRB/jrm
Enclosure

EXHIBIT A

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

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

June 29, 2023

Re: <<Variable Header>>

Dear <<First Name>> <<Middle Name>> <<Last Name>>:

Peters Township School District ("PTSD") is writing to notify you of an incident that may involve some of your information. Although there is no indication that your information has been misused in relation to this incident, we are providing you with information about the event, our response to it, and what you may do to protect your information, should you feel it appropriate to do so.

What Happened? On or about April 5, 2022, PTSD became aware of suspicious activity impacting our servers and systems. We immediately took steps to secure our systems and commenced an investigation to determine the full nature and scope of the activity with assistance from industry-leading cybersecurity specialists. Our investigation determined that our systems were accessible to an unknown actor between February 11, 2022, and April 5, 2022. Although the investigation was unable to determine whether information stored in the impacted servers had actually been taken or viewed by the unauthorized actor, we could not rule out the possibility of such activity. Therefore, out of an abundance of caution, we conducted a time-intensive and thorough programmatic and manual review of the information stored on the impacted systems to identify whether it contained any sensitive information and to whom that information related. Once complete, we conducted additional review of our records to confirm the identities and contact information for potentially affected individuals. We are providing notice to you because we determined that information related to you was stored on the impacted systems at the time of the incident.

What Information was Involved? While PTSD has no indication at this time that any information has been misused, the information contained on the impacted systems includes

What We Are Doing. Safeguarding the privacy of information held in our care and the security of our network is among our highest priorities. Upon learning of this event, we promptly took measures to secure the network and launched an investigation to determine the nature and scope of the event. We also implemented additional security tools to better prevent a similar event from recurring. PTSD also reported this incident to law enforcement.

As an added precaution, PTSD is also offering you <<CM Length>> months of identity and credit monitoring services at no cost to you through Equifax. For more information on these services, please review the enclosed *Steps You Can Take to Protect Your Information*. Please follow the instructions provided below to enroll in the identity and credit monitoring services PTSD is making available to you, as we are unable to enroll you in these services on your behalf.

What You Can Do. PTSD encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Protect Your Information* for useful information on what you can do to better protect your information. You can also enroll in the free identity and credit monitoring services that PTSD is providing to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays. You can also write to PTSD at 631 East McMurray Road McMurray, PA 15317.

We sincerely regret any inconvenience or concern this may have caused you. PTSD remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

Peters Township School District

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

EQUIFAX®

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 notifications[1] 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 alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- 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 theft[4]

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 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 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 credit freeze or fraud alert, 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 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; 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 New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.