MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeff Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 20, 2020

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

Dear Sir or Madam:

Our office represents the Allegheny Intermediate Unit ("AIU"), located at 475 East Waterfront Drive, Homestead, PA 15120. AIU is a statutorily created public education service agency. We write on behalf of AIU to notify your office of an incident that may affect the security of some personal information relating to twenty-four (24) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AIU 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 October 28, 2019, the AIU discovered that certain servers within its systems had been infected with ransomware. The AIU immediately launched an investigation with its in-house information technology department and third-party experts to determine the nature and scope of the incident. They determined that the AIU had backup versions of the most critical information and were able to restore access to the affected files without engaging or paying the unknown intruder. On January 27, 2020, the AIU determined the unauthorized individual who introduced the malware may have had access to servers containing protected personal information. The potentially accessible information included names, mailing addresses, email addresses, Social Security Numbers, passport numbers, and drivers' license numbers.

Notice to New Hampshire Residents

On or about May 20, 2020, AIU is providing written notice of this incident to all affected individuals, which includes twenty-four (24) New Hampshire residents. A sample of the letter is attached hereto and labeled as ***Exhibit A***.

Other Steps Taken and To Be Taken

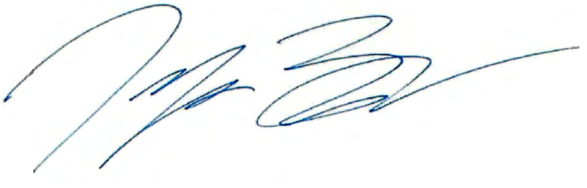
Upon discovering the event, the AIU moved quickly to investigate and respond to the incident, assess the security of AIU systems, and notify potentially affected individuals. The AIU is also working to implement additional safeguards and training to its employees. The AIU is providing affected individuals whose personal information was potentially affected by this incident with access to twelve (12) months of credit monitoring services through IDExperts at no cost to these individuals.

Additionally, the AIU 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. The AIU 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. The AIU is also reporting this matter to other regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4784.

Very truly yours,



Jeff Boogay of
MULLEN COUGHLIN LLC

Enclosure

EXHIBIT A

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-579-1098
Or Visit:
https://ide.myidcare.com/aiu
Enrollment Code: <XXXXXXXXXX>

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

May 20, 2020

Re: Notice of Data Event

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

The Allegheny Intermediate Unit ("AIU") is following up on our public notification of February 7, 2020 and writing to provide details regarding a recent event that may impact the privacy of some of your personal information. While we are unaware of any actual or attempted misuse of your information, we are providing you with this description of the event, our response, and steps you may take to protect against any misuse of your information, should you feel it is necessary to do so.

What happened? On October 28, 2019, we discovered that certain servers within our systems had been infected with malware known as ransomware that prevented us from accessing some of our files. We immediately began working with our in-house information technology department and third-party experts to determine the nature and scope of the incident. We determined that we had backup versions of the most critical information and were able to restore access to the affected files without engaging or paying the unknown intruder. On January 27, 2020 we determined the unauthorized individual who introduced the malware may have had access to servers containing protected personal information.

What information was involved? We have no evidence the unknown actor actually accessed or acquired any personal or protected information stored on AIU servers. However, some of the servers impacted stored personal information. Our investigation determined that the personal information which was present on the servers that may have been accessed included names, mailing addresses, email addresses, Social Security Numbers, passport numbers, and drivers' license numbers. We have no evidence of actual or attempted misuse of any information on the servers. However, out of an abundance of caution, we are providing you notice of the incident because your personal information was present on the server.

What is the AIU doing? We take this matter, and the security of information in our possession, very seriously. In addition to completing our investigation and restoring the integrity of our systems, we are continuing to review our policies and procedures and enhancing the security of our information systems to avoid a similar situation in the future. Though we have no evidence of actual or attempted misuse of any personal information, out of an abundance of caution we are providing this notice.

As an added precaution, we are providing you with access to twelve months of credit monitoring and identity protection services through ID Experts. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Your Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

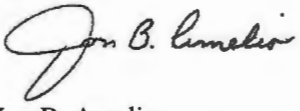
What can potentially affected individuals do? While we have no evidence that any personal information was subject to unauthorized access, or has been or will be misused, we encourage anyone who thinks their information may have been

impacted to monitor financial accounts and notify their bank immediately if they detect unauthorized or unusual activity. Please review the enclosed *Steps You Can Take to Protect Your Personal Information.* We also encourage you to enroll in the free credit monitoring being offered through ID Experts.

For more information. We understand some people may have additional questions concerning this incident. If you have additional questions, please contact our dedicated call center at 1-833-579-1098 during 9 am – 9 pm Eastern Time, Monday through Friday except U.S. holidays.

The AIU apologizes for any inconvenience this may cause and remains committed to the privacy and security of all information it maintains.

Sincerely,



Jon B. Amelio
Chief Technology Officer

Steps You Can Take to Protect Your Personal Information

Enroll In Credit Monitoring.

The AIU is providing free credit monitoring to impacted individuals through ID Experts. You can enroll in credit monitoring by following the below steps.

We encourage you to enroll in the free credit monitoring and insurance services by using the enrollment code included in this letter and going to https://ide.myidcare.com/aiu or calling 1-833-579-1098. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is August 20, 2020. Your unique enrollment code is provided at the top of this letter.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

Credit Reports.

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

Security Freeze.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008

www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission.

The Federal Trade Commission ("FTC") also encourages those who discover that their information has been misused to file a complaint. The FTC can 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. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.

For Maryland residents, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***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 agencies 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 violators. 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 Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. ***For North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov. ***For Rhode Island Residents***: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 15 Rhode Island residents impacted by this incident. This notice has not been delayed by a law enforcement investigation.