

Division Administration

Dr. Tracy B. Seitz
Superintendent

Dr. R. Byron Bishop
Assistant Superintendent



School Board Members

Elliott W. Reed, *Chairman*
Dr. Dana Burnett, *Vice Chairman*
Garland M. Harrow
Jenny McMurtrie
Claudia H. Soucek

Learners • Citizens • Leaders

June 14, 2023

Via E-mail (Idtheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann. § 14-3504(h)(1), I am writing on behalf of Middlesex County Public Schools ("MCPS"), in Virginia, to notify you regarding the nature and circumstances of a recent data security incident. MCPS's mailing address is P.O. Box 205, Saluda, VA 23149.

On May 15, 2023, MCPS was alerted to suspicious activity affecting our network. We launched an immediate investigation to determine the nature and scope of this activity, including engaging leading outside cybersecurity experts to investigate and remediate the incident. It became apparent that MCPS was the victim of a ransomware attack. While our remediation efforts continue to be ongoing, the cybercriminals responsible have claimed to remove certain data from our servers. We believe some of the files allegedly exfiltrated contain limited amounts of personal information.

It is unknown whether the cybercriminals actually exfiltrated all information that they claim to have acquired. Moreover, we cannot know whether they have actually discovered or accessed any personal information present in the relevant documents. There is no evidence indicating that the cybercriminals have used any personal information stemming from this event to cause any harm, or for any malicious purpose. However, as described in detail in the attached notification letters, the information involved may have included one or more of the following types of information pertaining to Marylanders: names in combination with Social Security numbers.

In response to this incident, we have notified the FBI Cyber Crimes Division and the Virginia State Police's Fusion Intelligence Center. Additionally, we have arranged to provide potentially impacted individuals with one year of credit monitoring and identity restoration services through Experian at no cost to them.

MCPS has identified two (2) Maryland residents potentially impacted by this incident. The School System has worked expeditiously to identify each of these individuals. Attached for your reference is a copy of the notice we plan to mail out to impacted Maryland residents on June 15, 2023.

If you have any questions, please contact our outside counsel, Beth Burgin Waller of Woods Rogers Vandeventer Black PLC, via email at beth.waller@wrwblaw.com.

Very truly yours,

Tracy B. Seitz, Ed.D.
Division Superintendent

Enclosures



C/O Experian Return Mail Processing
PO Box 999
Suwanee, GA 30024

61841 *****SNGLP

SAMPLE A. SAMPLE - L03

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



June 15, 2023

Dear Sample A. Sample:

As you may be aware, Middlesex County Public Schools (“MCPS”), like many school systems and organizations across the country, has unfortunately been the victim of a ransomware attack. We are writing to share with you how this incident may have affected your personal information and, as a precaution, to provide you with steps you can take to protect this information.

Although we have no evidence that a cybercriminal succeeded in removing your personal information from MCPS systems or is using it for a malicious purpose, we wanted to alert you to this matter.

MCPS takes the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

What Happened and What Information Was Involved

On or about May 15, 2023, we were alerted to suspicious activity affecting our network. We launched an immediate investigation to determine the nature and scope of the activity, including engaging leading outside cybersecurity experts to investigate and remediate the incident. It became apparent that MCPS was the victim of a ransomware attack.

Ransomware is a form of malware used by cybercriminals to prevent organizations from accessing files, and, in some cases, to extract and hold data hostage until a ransom is paid. In this matter, a cybercriminal accessed servers in the MCPS environment and encrypted them. We were able to recover from this matter and successfully prevented the ransomware from disrupting the end of our school year. However, the cybercriminal claims to have removed certain data from our servers.

Based on the names of files the criminals alleged to have taken, information pertaining to you might have been implicated. **Although some files allegedly acquired by the cybercriminals might pertain to you, we have no evidence that the cybercriminals actually obtained your personal identifying information. Still, out of an abundance of caution, we have arranged for free credit monitoring in addition to Experian’s ID protection services, which are retroactive to the date of the incident.** More information about the free credit monitoring services we are providing through Experian can be found in the attached Identity Theft and Protection Guide. If the cybercriminals actually acquired the files that they claim, and if these documents do actually relate to you, there is a possibility that one or more of the following types of personal information could conceivably have been implicated: your name, Social Security number, and/or address.

What We Are Doing

We have notified the FBI Cyber Crimes Division and the Virginia State Police's Fusion Intelligence Center of this ransomware attack. MCPS intends to support any law enforcement investigation into this incident. We take our obligation to safeguard personal information very seriously and continue to evaluate actions to strengthen our network security in the face of an ever-evolving cyber threat landscape.

What You Can Do

Please stay vigilant regarding your personal information and review the enclosed Identity Theft and Protection Guide for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary credit monitoring services being offered for you through Experian *IdentityWorks*. Information regarding the credit monitoring enrollment is included in the attached Identity Theft and Protection Guide.

For More Information

If you have any further questions regarding this matter or the credit monitoring services provided, please call 1-833-514-1014 toll-free Monday through Friday 9 am to 11 pm ET, or Saturday and Sunday from 11 am to 8 pm ET (excluding major U.S. holidays). Please be prepared to provide your engagement number B096582. Please also note that MCPS is utilizing Experian's return mail service, so the return address on this letter is to their mailing center.

We deeply regret that this incident occurred and are committed to supporting you.

Sincerely,

A handwritten signature in black ink that reads "Tracy B. Seitz". The signature is written in a cursive, flowing style.

Tracy B. Seitz, Ed.D.
Division Superintendent

IDENTITY THEFT PROTECTION GUIDE AND INFORMATION

We encourage affected individuals to take the following steps:

Register for Credit Monitoring and Identity Restoration Services.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twelve 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 twelve 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 your complimentary twelve-month membership in Experian IdentityWorks. 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** September 30, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: 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 1-833-514-1014 by September 30, 2023. Be prepared to provide engagement number B096582 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWELVE-MONTH MEMBERSHIP IN EXPERIAN IDENTITYWORKS

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 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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-916-8800
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as a home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

* 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.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-800-916-8800
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1 year and 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 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-800-916-8800
[www.transunion.com/fraud-
victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number. You may want to order copies of your credit reports and check for any bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your records.

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 (FTC). Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For Virginia residents: You may contact the Virginia Attorney General's Office, 202 North Ninth Street, Richmond, Virginia 23219, <https://www.oag.state.va.us/contact-us/contact-info>.

For North Carolina residents: The North Carolina Attorney General's Office may be contacted at 9001 Mail Service Center, Raleigh, NC 27699, (919) 716-6000, www.ncdoj.gov/contact-doj/.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

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 Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 150 South Main Street, Providence, RI 02903, 1-401-274-4400, <https://riag.ri.gov/>.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia at 400 6th Street, NW, Washington, DC 20001, 1-202-442-9828, <https://oag.dc.gov/consumer-protection/consumer-alert-online-privacy>.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.