



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

September 5, 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 Minneapolis Public Schools (“MPS”), located at 1250 W. Broadway Avenue, Minneapolis, MN 55411, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately thirty (30) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MPS 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 around February 18, 2023, MPS became aware of suspicious activity impacting its computer systems. MPS immediately commenced an investigation to confirm the nature and scope of the incident. The investigation determined that an unauthorized actor had access to certain information on its computer systems between February 6, 2023, and February 18, 2023.

A preliminary review of a smaller listing of impacted data was completed on March 22, 2023. On April 7, 2023, MPS sent notice to a limited number of known impacted individuals. However, it was necessary for MPS to undertake a comprehensive and time-intensive review of the involved systems to determine whether sensitive information was present in the involved systems at the time of the incident. On July 24, 2023, the review process was completed, and it was determined that information related to certain individuals was present in the impacted files. MPS then conducted additional review of its files to identify contact information for the impacted individuals. The information that could have been subject to unauthorized access includes name, Social Security number, financial account information, and health insurance information.

Notice to Maryland Residents

On April 7, 2023, MPS sent notice to a limited number of known impacted individuals. However, further investigation was needed to determine the full scope of the impacted population. On or about September 5, 2023, MPS provided written notice of this incident to approximately thirty (30) 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 discovering the event, MPS moved quickly to investigate and respond to the incident, assess the security of MPS systems, and identify potentially affected individuals. Further, MPS notified federal law enforcement regarding the event. MPS is also working to implement additional safeguards and training for its employees. MPS is providing access to credit monitoring services for twenty four (24) months through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MPS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. MPS 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.

MPS is providing written notice of this incident to relevant state and federal 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 (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/kzm
Enclosure

EXHIBIT A



MINNEAPOLIS
PUBLIC SCHOOLS

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 5, 2023

J9283-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01

APT ABC

123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



- Yog koj xav tau ib qhov copy ntawm cov kev qhia txog MPS cov ntaub ntawv uas neeg nyiaj nkag tau (data breach) ua lus Hmoob, thov email: privacy@mpls.k12.mn.us
- Haddii aad jeclaan lahayd nuqul ka mid ah macluumaadkaan la xidhiidha xogta la jabsaday MPS ee Somali, fadlan iimayl u dir privacy@mpls.k12.mn.us
- Si desea una copia en español de esta información relacionada con la vulneración de datos en MPS, envíe un correo electrónico a: privacy@mpls.k12.mn.us

NOTICE OF DATA BREACH

Dear Sample A. Sample:

Minneapolis Public Schools (MPS) is writing to notify you of an incident that occurred in February and may impact the security of some of your information. We are providing you with notice of the incident, steps MPS is taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On or around February 18, 2023, MPS became aware of suspicious activity impacting our computer systems. We immediately reported the event to law enforcement and commenced an investigation to confirm the nature and scope of the incident. The investigation determined that an unauthorized actor had access to certain information on our computer systems between February 6, 2023, and February 18, 2023.

Understanding what information had been impacted was critical. MPS, in partnership with national specialists, immediately began a comprehensive review of the involved computer systems. The purpose of the comprehensive review was to determine whether sensitive information was present and identify impacted individuals. This process was time-intensive and required both computer-assisted and manual review. This process was completed on July 24, 2023. Although it has been difficult to not share more information with you sooner, the accuracy and the integrity of the review were essential.

Following this comprehensive review, we worked to match the information we reviewed with contact information and then prepared notifications. MPS worked with a notification vendor to locate address information and provide the necessary resources to protect impacted individuals.

We are notifying you because the investigation determined some of your information was present in the involved systems.

B103341

0000001



J9283-L01

What Information Was Involved? The information of yours present in the files included your name, and [Extra1].

What We Are Doing. Upon discovery of this incident, MPS immediately took steps to secure the MPS environment and conducted a diligent investigation to confirm the nature and scope of the incident. As part of MPS's ongoing commitment to the security of information, our policies and procedures regarding information security are being reviewed and enhanced, additional safeguards have been implemented, and additional training is being conducted to reduce the likelihood of a similar event in the future.

As an added precaution, **we are also offering you free access to 24 months of credit monitoring and identity theft restoration services through Experian.** You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Personal Information* for additional information on these services.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Help Protect Personal Information*. 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 and to detect errors. We also encourage you to enroll in the free credit monitoring and identity restoration services. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions:

- Contact our dedicated assistance line at 833-388-2119, Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide engagement number B103341 when you call.
- You may also send an email to: privacy@mpls.k12.mn.us or write to MPS at 1250 W. Broadway Ave, Minneapolis, MN 55411.
- MPS will prepare a report on the facts and results of our investigation. This report will be published on our website, where you can also find a timeline of this situation since February. Or, if you would like us to send a copy of the report to you, please contact privacy@mpls.k12.mn.us.

We thank you for your patience and understanding as we move forward in this process.

Sincerely,

Minneapolis Public Schools
mpls.k12.mn.us

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Free Credit Monitoring and Identity Protection Services:

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 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 24 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 24-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 December 31, 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 833-388-2119 by December 31, 2023. Be prepared to provide engagement number B103341 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 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.

* 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
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

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 8 Rhode Island residents impacted by this incident.

