



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

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

August 20, 2024

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 Upper Darby School District (“UDSD”) located at 8201 Lansdowne Avenue, Upper Darby, PA 19082, and write to notify your office of an incident that may affect the personal information relating to five (5) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, UDSD 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

UDSD identified unauthorized access to certain IT systems. UDSD promptly took steps to secure its systems and initiated an investigation into the nature and scope of the issue. While their investigation is ongoing, to date, UDSD has determined that certain files were potentially copied from their systems by an unauthorized person on or around June 20, 2024. UDSD are reviewing the relevant files to determine what information is present and to whom it relates. UDSD is notifying individuals because they found their information as part of that review. Based on these efforts, it was confirmed that the information contained data related to five (5) Maryland resident(s). The potentially affected information includes name, Social Security number, date of birth, financial account information, medical information, and health insurance information, was potentially accessible during the event.

Notice to Maryland Residents

On August 20, 2024, UDSD will provide written notice of this incident to certain potentially affected individuals, including five (5) Maryland resident(s). 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 identifying unusual system activity, UDSD took prompt steps to secure its systems and initiate a comprehensive investigation, which is currently ongoing. Further, UDSD notified federal law enforcement and the Delaware County, PA Office of the District Attorney regarding the event. Additionally, UDSD is notifying potentially affected individuals and providing information on steps they may take to better protect their personal information from misuse, including 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. UDSD is also providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. UDSD is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-6643.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/lcf
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 11 *****AUTO**MIXED AADC 302

SAMPLE A. SAMPLE - L01



APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



August 20, 2024

RE: Notice of Data Security [Extra1]

Dear Sample A. Sample:

Upper Darby School District (“UDSD”) is writing to inform you of a recent event that may affect your personal information. We take this incident seriously and are providing you with information about the incident, our response to it, and resources available to you to help you better protect your personal information, should you feel it appropriate to do so.

What Happened. UDSD identified unauthorized access to certain IT systems. We promptly took steps to secure our systems and initiated an investigation into the nature and scope of the of the issue. While our investigation is ongoing, to date, we have determined that certain files were potentially copied from our systems by an unauthorized person on or around June 20, 2024. We are reviewing the relevant files to determine what information is present and to whom it relates. You are receiving this letter because we found your information as part of that review.

What Information Was Involved. The investigation determined that information from your HR file, including name, Social Security number, date of birth, financial account information, medical information, and health insurance information, was potentially accessible during the event. Please note that we are not aware of any actual or attempted fraudulent misuse of information as a result of this incident.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. We are working diligently to investigate and respond to this incident. 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 affected individuals, and providing information on steps you may take to better protect personal information. As an added precaution, we are offering you access to credit monitoring and identity restoration services through Experian for [Extra2], at no cost to you. Enrollment instructions are attached to this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your 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 Help Protect Your Personal Information*.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-866-362-1773, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. Additionally, you can write to us at 8201 Lansdowne Avenue, Upper Darby, PA 19082.

Sincerely,

Upper Darby School District

Steps You Can Take To Help Protect Your Personal Information

Enroll in Credit Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra2] 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 [Extra2] 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 [Extra2]-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** November 29, 2024 (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 1-866-362-1773 by November 29, 2024. Be prepared to provide **engagement number** [Engagement Number].

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

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, your state Attorney General, and the Federal Trade Commission. 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 <https://oag.dc.gov>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 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 https://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 <https://www.ncdoj.gov>.