



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

James Paulino
Office: (267) 930-4741
Fax: (267) 930-4771
Email: jpaulino@mullen.law

75 S. Clinton Avenue, Suite 510
Rochester, NY 14604

April 11, 2022

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 Potential Data Event

To Whom It May Concern:

We represent Hazelwood School District (“Hazelwood”) located at 15955 New Halls Ferry Road, Florissant, MO 63031, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three (3) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Hazelwood 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 about September 28, 2021, Hazelwood discovered unusual system activity on its network. Upon discovery, Hazelwood promptly took steps to respond and to commence an investigation into the activity. Through the initial investigation, Hazelwood determined that it was the target of a cyber-attack that encrypted certain files on its network. On or about October 26, 2021, Hazelwood confirmed that certain files on its system may have been accessed by an unauthorized individual. Hazelwood then promptly undertook a thorough and time intensive review of the data to determine the individuals whose information may be at risk, and then worked diligently to identify accurate address information to provide this written notification to all potentially impacted individuals. This process was completed on or about March 10, 2022.

The information that potentially could have been subject to unauthorized access includes name, Social Security number, and medical treatment/diagnosis information. We have no indication that any specific information has been subject to public disclosure or attempted misuse, and the

investigation to date has found no evidence confirming that any specific personal information was accessed or acquired.

Notice to Maryland Residents

On or about April 11, 2022, Hazelwood provided written notice of this incident to three (3) 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, Hazelwood moved quickly to investigate and respond to the incident, assess the security of Hazelwood's systems, and identify potentially affected individuals. Further, Hazelwood notified federal law enforcement regarding the event. Hazelwood is also working to implement additional safeguards and training to its employees. Hazelwood is providing access to credit monitoring services for two (2) years, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

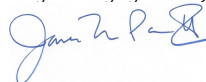
Additionally, Hazelwood is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Hazelwood is providing individuals with 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.

Hazelwood is also providing written notice of this incident to additional 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) 930-4741.

Very truly yours,

A handwritten signature in blue ink, appearing to read "James Paulino".

James Paulino of
MULLEN COUGHLIN LLC

JMP/rmm
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

Hazelwood School District (“Hazelwood”) is writing to notify you of an incident that may impact the privacy of some of your personal information. This notice provides you with information about the incident, our response, and steps you may take to better protect your information, should you feel it is appropriate to do so, along with an offer of 24 months of credit monitoring with \$1,000,000 in identity theft insurance at no cost to you; enrollment instructions can be found on the following pages.

What Happened?

On or about September 28, 2021, Hazelwood discovered unusual system activity on its network. Upon discovery, Hazelwood promptly took steps to respond and to commence an investigation into the activity. Through the initial investigation, Hazelwood determined that it was the target of a cyber-attack that encrypted certain files on our network. On or about October 26, 2021, Hazelwood confirmed that certain files on our system may have been accessed by an unauthorized individual. Hazelwood then promptly undertook a thorough and time intensive review of the data to determine the individuals whose information may be at risk, and then worked diligently to identify accurate address information to provide this written notification to all potentially impacted individuals. This process was completed on March 10, 2022.

What Information Was Involved?

While Hazelwood is currently unaware of any actual or even attempted misuse of information, and while we cannot confirm that your specific information was accessed or acquired, the information contained in the potentially impacted files includes your name, <<breached elements>>.

What We Are Doing.

Information security is one of Hazelwood’s highest priorities, and we have security measures in place to protect information in our care. We responded promptly when we discovered this incident by taking steps to secure our systems and commence a comprehensive investigation. We are also taking steps to further secure our systems, and are reviewing existing policies and procedures and implementing additional safeguards to further secure the information in our care. As an added precaution, Hazelwood is offering you access to 24 months of credit monitoring and identify protection services through Epiq at no cost to you.

What You Can Do.

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. Please review the attached “*Steps You Can Take To Protect Information*” for additional information on protecting your personal information. You will also find information on how to enroll in the credit monitoring services offered.

For More Information.

We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call 833-944-3165 between 8:00 AM and 8:00 PM CT, Monday through Friday (excluding major U.S. holidays). You may also write Hazelwood School District at 15955 New Halls Ferry Road, Florissant, MO 63031, Attention: Finance Department.

Sincerely,

Hazelwood School District

STEPS YOU CAN TAKE TO PROTECT INFORMATION

Enroll in Credit Monitoring



Enter your Activation Code: <ACTIVATION CODE>
Enrollment Deadline: <DEADLINE MMMM DD, YYYY>

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 notifications¹ 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 alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- 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 theft⁴

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.

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.

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.

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
1-888-298-0045	1-888-397-3742	1-833-395-6938
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

Internal Revenue Service Identity Protection PIN (IP PIN)

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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 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 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.