WHITEFORD, TAYLOR & PRESTON L.L.P.

TOWSON COMMONS, SUITE 300
ONE WEST PENNSYLVANIA AVENUE
TOWSON, MARYLAND 21204-5025
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

June 1, 2021

Privileged and Confidential
VIA EMAIL AND FIRST CLASS MAIL

Director Bill Brauch
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

Re: Security Breach Notification

Dear Director Brauch,

We are writing on behalf of our client, United Community School District ("UCSD") (located at 200 Adams Street, La Porte City, Iowa 50651), to notify you of a security breach incident involving five hundred and fifty (550) Iowa residents.

Nature

On April 7, 2021, USCD was the victim of a cyberattack from an unauthorized individual that resulted in its systems and servers being inoperable for a limited time. After discovering the attack, USCD quickly took steps to secure its systems and restore operations. At that time, UCSD had no facts indicating that incident involved acquiring personal information or its data. However, on April 21, 2021, UCSD learned that the unauthorized individual obtained some information from its systems during the incident. Once UCSD learned about this, they immediately engaged third-party forensic experts to conduct a thorough investigation of the incident's nature and scope and contacted the FBI to seek assistance and guidance.

UCSD recently concluded its investigation and determined that the incident was a ransomware attack. Currently, UCSD has no evidence indicating that personal information was obtained and or misused. However, out of an abundance of caution, UCSD is providing notice to the potentially impacted individuals proactively.

Notice and UCSD's Response to the Event

On June 6, 2021, UCSD will mail written notifications to the potentially affected Iowa residents, in accordance with Iowa Code § 715C.1-2 in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, UCSD is providing these potentially impacted individuals the following:

- Free access to credit monitoring services for at least twelve months (12), through Equifax;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank.
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- 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 and law enforcement to report attempted or actual identity theft and fraud.

Finally, UCSD is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 917-5189 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

UNION COMMUNITY SCHOOL DISTRICT

"Education to Meet Tomorrow's Challenges"
200 Adams Street
La Porte City, IA 50651
319-342-2674 • Fax 319-342-2393
www.union.k12.ia.us

<date>

<First Name> <Last Name>
<Street>
<City>, <State> <Zip>

Re: Notice of Data Breach

Dear <First Name> <Last Name>

At Union Community School District, we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information, what we did in response, and steps you can take to protect yourself against possible misuse of your personal information.

What Happened

On April 7, 2021, we were the victim of a cyberattack from an unauthorized individual that resulted in our systems and servers being inoperable for a limited time. After discovering the attack, we quickly took steps to secure our systems and restore operations. At that time, we had no facts indicating that any information was obtained. However, on April 21, 2021, we learned that the unauthorized individual obtained some information from our systems during the incident. Once we learned about this, we immediately engaged third-party forensic experts to conduct a thorough investigation of the incident's nature and scope and contacted the FBI to seek assistance and guidance.

We recently concluded our investigation. Currently, we have no evidence indicating that your information was obtained and or misused. However, out of an abundance of caution, we wanted to let you know that your information could have been involved in the incident.

What Information Was Involved

The information that could have been involved included your social security number.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. As stated above, while we have no evidence indicating your information was obtained and or misused, we strongly recommend you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement.

Additionally, in response to this attack, we implemented additional safeguards and employee training related to cybersecurity. Further, we are working with our external legal and cybersecurity experts to improve our

cybersecurity policies, procedures, and protocols to attempt to minimize the likelihood of this type of attack succeeding again.

Also, we are offering a complimentary one-year membership Equifax Credit Watch™ Gold. This product provides you credit monitoring, fraud alerts, identity theft insurance, and identity theft restoration services. Please see the information on the following page for additional details and instructions on how to register. Please note that you must register for this product by August 31, 2021.

For More Information

We sincerely regret this incident and are working to implement any necessary additional safeguards and policies to best minimize the likelihood of this occurring again. We understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, please call our toll-free helpline response line at [toll-free number] between 7:00 a.m. and 7:00 p.m. (CDT) Monday – Friday.

Sincerely yours,

Travis Fleshner
Superintendent

EQUIFAX®

<FIRST NAME> <LAST NAME>
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 notifications[1] 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 alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- 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 theft[4]

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.

---

[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.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action.

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Provided below are the three nationwide credit reporting agencies' contact information to request a copy of your credit report or general identified above inquiries.

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Remain Vigilant, Review Your Financial Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by closely reviewing your financial account statements and credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains the account. You also should immediately report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement.

To file a complaint or to contact the FTC, you can (1) send a letter to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338).

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Security Freeze (also known as a Credit Freeze)

You may have the right to put a credit or security freeze on your credit file. A security freeze makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check.

You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued

identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.
Since the instructions for how to establish a security freeze differ based on your state residency, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above in the **"Obtain and Monitor Your Credit Report"** section).

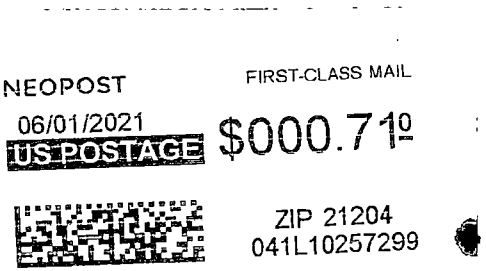
Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf

Iowa residents may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

SPollock
Whiteford, Taylor & Preston LLP
One W. Pennsylvania Avenue, Suite 300
Towson, MD 21204



PRIVILEGED AND CONFIDENTIAL
Director Bill Brauch
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines. Iowa 50319-0106