

WHITEFORD, TAYLOR & PRESTON L.L.P.

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

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

July 7, 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, North Iowa Community Action Organization (“NICA0”) (located at 218 5th Street SW, Mason City, Iowa 50401), to notify you of a security breach incident involving five-hundred and twelve (512) Iowa residents.

Nature

On March 31, 2021, we became aware of suspicious activity related to an employee’s email account. After discovering the incident, we promptly secured the impacted email account and began taking steps to determine the nature, scope, and extent of the incident. On approximately May 10, 2021, NICA0 concluded its forensic investigation and determined that an unauthorized individual gained access to five employee email accounts via a phishing email. Further, the forensic investigative findings are inconclusive as to whether the personal information was actually obtained. After concluding the forensic investigation, NICA0 initially identified 58 Iowa residents whose personal information was potentially accessed. On May 26, 2021, NICA0 provided written notification to these potentially impacted individuals in a substantially similar form as the enclosed letter (attached as Exhibit A).

NICA0 continued performing a comprehensive and detailed review of the potentially impacted email accounts. As a result, on July 1, 2021, NICA0 concluded its search for potentially affected individuals and located all their recent contact information.

Finally, as stated above, the forensic investigative findings are inconclusive as to whether the personal information was actually obtained, but as of now, NICA0 has no evidence indicating misuse of its data or information. However, out of an abundance of caution and due to the impacted email account containing

personal information, NICAO proactively is providing notice to your office and will provide notice to the potentially affected individuals.

Notice and NICAO's Response to the Event

On July 8, 2021, NICAO 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, NICAO intends to provide the potentially impacted individuals the following: is providing these potentially affected individuals the following:

- Free access to credit monitoring services for at least twelve months (12)
- 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.
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Finally, NICAO is working to improve its cybersecurity policies, procedures, and protocols, implementing any necessary additional safeguards to strengthen 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) 832-2002 or email me at spollock@wtplaw.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

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

Exhibit A



P. O. Box 1627, Mason City, IA. 50402-1627
Phone: 641-423-8993, Fax: 641-494-1899

July 1, 2021

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

RE: Notice of Data Breach/Security Incident

Dear <First Name> <Last Name>,

At North Iowa Community Action Organization, 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 HAPPENED?

On March 31, 2021, we became aware of suspicious activity related to an employee's email account. After discovering the incident, we promptly secured the impacted email account and began taking steps to determine the nature, scope, and extent of the incident. Our investigation revealed that an unauthorized individual gained access to the employee's email account via a phishing email. At that time, we began a comprehensive review of the emails to determine what information and individuals were involved and locate the most recent contact information for each.

We recently concluded our review and believe that some of your information could have been accessed and or potentially obtained. **However, we have no evidence indicating that your personal information was misused. Finally, we believe the unauthorized individual was attempting to access payroll information and that your information was therefore likely not the target of the unauthorized access.**

WHAT INFORMATION WAS INVOLVED?

The information that could have been involved included your <PII present>.

WHAT WE ARE DOING AND WHAT YOU CAN DO

As stated above, to date, we have no evidence indicating that your personal information was misused. However, we take this incident very seriously and strongly encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you detect

suspicious activity, please contact the institution issuing the statement.

Further, since this incident, we began reviewing our privacy and security policies and procedures to improve our cybersecurity protections, implement new technical safeguards, and work with our employees to raise awareness about these types of attacks to minimize the likelihood of this type of incident occurring again.

Also, we are providing you with access to Single Bureau Credit Monitoring. These services provide you with alerts for one year from the date of enrollment when changes occur to your Experian credit file. We are providing this service free of charge, and signing up for this service will not impact your credit score. This product helps detect any potential misuse of your personal information and gives you identity protection services that will help with resolving and identifying any potential identity fraud or theft. These services will be provided by Sontiq, a company specializing in fraud assistance and remediation services.

You have 90 days from the date of this letter to redeem these services.

We sincerely regret this incident and take this incident very seriously. 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 between the hours of 8:00 am to 5:00 pm Eastern time, Monday through Friday. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed below.

Sincerely,

Cindy Davis

Cindy Davis, Executive Director
North Iowa Community Action Organization

OTHER IMPORTANT INFORMATION

Enroll for Credit Monitoring and Identity Theft Protection Services

To enroll in these services, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <CODE HERE.> To receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

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](https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf) 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 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.