COZEN O'CONNOR

July 18, 2022

Matthew J. Siegel
Direct Phone 215-665-3703
Direct Fax 215-701-2303
msiegel@cozen.com

VIA EMAIL (NDAG@ND.GOV)

Office of North Dakota Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040

Office of North Dakota Attorney General
Consumer Protection and Antitrust
1050 East Interstate Avenue, Suite 200
Bismarck, ND 58503-5574

To Whom it May Concern:

I write on behalf of our client, AllOne Health, a provider of mental health and well-being benefits for organizations worldwide. Pursuant to N.D. Cent. Code §§ 51-30-01 et *seq.*, this letter is to inform you that AllOne Health recently discovered that an unauthorized individual gained access to one of its employees' email accounts and information contained within that account. On June 10, 2022, AllOne Health determined that the unauthorized access may have affected 16 North Dakota individuals.

As background, on February 11, 2022, AllOne Health learned that certain wire transfers meant for one of its payees were unintentionally routed to a fraudulently created bank account. Immediately upon learning of this fraud, AllOne Health launched an internal investigation to determine what happened and reported the theft to the FBI and local law enforcement. On approximately March 23, 2022, during AllOne Health's initial investigation, it learned of the unauthorized individual's access to one of its employees' email accounts, which may have occurred between approximately September 2021 and February 11, 2022.

Immediately after learning of the fraud, AllOne Health shut down the unauthorized access, reset all company passwords, and implemented additional security measures for its systems. AllOne Health also retained a specialized forensic firm to assess the intrusion and to ensure that there was no further access to either the employee's mailbox or other mailboxes or systems in its environment. That analysis revealed that while the individual gained access to limited financial documents, it appears from the investigation that the individual's intention was to commit wire fraud. AllOne Health has seen no evidence that any personal or sensitive information was acquired or sent outside of its network.

AllOne Health has determined that the information that may have been viewed or accessed by the unauthorized individual may have included names, addresses, dates of birth, driver's license numbers, Social Security numbers, and/or some limited health information of employees and customers of AllOne Health. No other personally identifiable information was available, and we have no evidence that any specific information was taken from the email account or that it is being used in any way by the unauthorized person.

AllOne Health is committed to ensuring the privacy and security of the information of its employees and customers. AllOne Health is offering identity protection and credit monitoring services to the affected individuals through Epiq, free of charge for one year. Attached for your reference is a sample of the notice to the affected individuals, which we sent via first class mail on July 15, 2022.

If you have any questions, please feel free to contact me at (215) 665-3703 or msiegel@cozen.com.

Sincerely,

COZEN O'CONNOR

By: Matthew J. Siegel

MJS

Enclosure

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>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We are writing to advise you of a data security incident that may have involved some of your personal information. AllOne Health has always taken measures to protect the privacy and security of the personal information it maintains and this is the reason that, as a precaution, we are providing you with this notification.

What Happened?

In February 2022, our finance group learned that certain wire transfers meant for one of our payees were unintentionally routed to a fraudulently created bank account. Immediately upon learning of this fraud, we launched an internal investigation to determine what happened and reported the theft to the FBI and local law enforcement. During our initial investigation, we learned that an unauthorized individual gained access to one of our employees' email accounts to perpetrate the fraudulent transfers. We then retained a specialized forensic firm to assess the intrusion and to ensure that there was no further access to either the employee's mailbox or other mailboxes or systems in our environment. That analysis revealed that while the individual gained access to limited financial documents, it appears from our investigation that the individual's intention was to commit wire fraud. We have seen no evidence that any personal or sensitive information was acquired or sent outside of our network. However, because the unauthorized individual had access to the employee's email account and may have viewed such information, we are sending you this notification out of an abundance of caution.

What Information Was Involved?

We have determined that the information that may have been viewed or accessed by the unauthorized individual may have included your name, address, date of birth, driver's license number, Social Security number, and/or some limited health information. No other personally identifiable information was available, and we have no evidence that your specific information was taken from the email or that it is being used in any way by the unauthorized person.

What We Are Doing.

We have taken various measures to help ensure that all personal information in our possession is protected. Immediately after learning of the fraud, we shut down the unauthorized access, reset all company passwords, and implemented additional security measures for our systems. Although we have no indication that any of your information was actually acquired or that anyone has taken any steps to commit identity theft, to help protect your identity we are offering you one year (12 months) of complimentary credit monitoring services through *my*TrueIdentity. The attachment included with this letter provides details for how to use this service.

What You Can Do.

In addition to the credit monitoring services we are offering, we have prepared the attached Reference Guide to give you additional details to help you protect your personal information, including information on obtaining your free annual credit report and reporting concerns regarding identity theft. We encourage you to remain vigilant by monitoring your credit report and reviewing your account statements.

For More Information.

If you have any additional questions or concerns, please feel free to contact our toll-free line at 877-289-1884 from 9:00 a.m. – 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

Steven O'Connor
Director of IT

Reference Guide

We encourage you to take the following steps:

Enroll in Credit Monitoring. As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<CM Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you place an initial fraud alert and order your credit reports. You can then create an FTC Identity Theft Affidavit by submitting a report about the theft at http://www.ftc.gov/complaint or by calling the FTC. Then file a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit with you when you file the police report. Your Identity Theft Report is your FTC Identity Theft Affidavit plus your police report. You may be able to use your Identity Theft Report to remove fraudulent information from your credit report, prevent companies from refurnishing fraudulent information to a consumer reporting agency, stop a company from collecting a debt that resulted from identity theft, place an extended seven-year fraud alert with consumer reporting agencies, and obtain information from companies about accounts the identity thief opened or misused.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. You can freeze and unfreeze your credit file for free. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202. By phone: (888) 743-0023 (toll-free in Maryland) or (410) 576-6300. Or visit: www.oag.state.md.us

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001. By phone: (877) 566-7226 (toll-free in North Carolina) or (919) 716-6400. Or visit: www.ncdoj.gov