



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

APR 26 2021

CONSUMER PROTECTION

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

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

April 21, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Health Aid of Ohio, Inc. ("Health Aid"), located at 5230 Hauserman Road, Parma, OH, 44130, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Health Aid does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 19, 2021, Health Aid became aware of suspicious activity relating to its systems and immediately launched an investigation to determine the nature and scope of the activity. Health Aid determined that an unauthorized actor gained access to certain Health Aid systems on or about February 18, 2021, and removed and/or viewed certain files from the Health Aid network.

While the unauthorized actor was able to confirm that some files were taken from Health Aid's network, the investigation could not confirm precisely which files were impacted. As a result, Health Aid took steps to notify individuals whose information may have been present in the impacted systems at the time of the event.

The information that could have been subject to unauthorized access includes name and Social Security number.

Mullen.law

Notice to New Hampshire Residents

On April 20, 2021, Health Aid began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident who had information protected by the New Hampshire data event statute impacted. Health Aid notified additional individuals in accordance with HIPAA regulations. 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, Health Aid moved quickly to investigate and respond to the incident, assess the security of Health Aid systems, and notify potentially affected individuals. Health Aid is also working to implement additional safeguards and training to its employees. Health Aid is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose Social Security number was potentially affected by this incident, at no cost to these individuals.

Additionally, Health Aid 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. Health Aid 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. Health Aid also notified the Federal Bureau of Investigation and the Department of Health and Human Services of the incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/zlg
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>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Dear <<Name 1>>:

Health Aid of Ohio, Inc. (“Health Aid”) is writing to notify you of a recent incident involving some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this incident, we are providing you with information about the incident, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? On February 19, 2021, Health Aid became aware of suspicious activity relating to its systems and immediately launched an investigation to determine the nature and scope of the activity. Health Aid determined that an unauthorized actor gained access to certain Health Aid systems on or about February 19, 2021, and removed and/or viewed certain files from our network.

Although the investigation has been unable to confirm which specific files were impacted, we could not rule out the possibility that some of your information may have been viewed or taken. Therefore, in an abundance of caution we reviewed the information that is housed on our systems, and it was determined that certain information related to you may have been impacted.

What Information Was Involved? Our investigation determined that the following types of your information may have been impacted by this incident: name, address, telephone number, Social Security number, date of birth, medical diagnosis, insurance information, and the type of equipment we delivered to your house or repaired in your home. To date, Health Aid has not received any reports of fraudulent misuse of any information impacted in relation to this incident.

What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities, and we have security measures in place to protect information in our systems. Upon learning of this incident, we immediately took steps to secure our systems and investigate the incident. Health Aid’s vendors deployed advanced endpoint monitoring tools to the network and changed passwords in response to the event. We notified the Federal Bureau of Investigation (“FBI”) of this incident, and are also notifying certain regulators, as necessary, including the Department of Health and Human Services.

While we are unaware of any fraudulent misuse of your information as a result of this incident, as an additional precaution, Health Aid is offering you access to <<12/24>> months of complimentary credit monitoring services through TransUnion. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What Can You Do? Please review the enclosed document, “Steps You Can Take to Help Protect Your Information,” which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that Health Aid is offering to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please contact our toll-free dedicated assistance line at 800-521-6912. This toll-free line is available Monday – Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Individuals may also write to Health Aid at 5230 Hauserman Road, Parma, OH 44130 with questions.

Sincerely,

A handwritten signature in cursive script that reads "Carol Gilligan".

Carol Gilligan

Steps You Can Take to Help Protect Your Information

Enroll in Complimentary Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<12/24>> months provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code << Activation 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 six-digit telephone passcode <<Engagement Number>> 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.

You can sign up for the online or offline 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 a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR <<12/24>>-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and credit score.
- 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, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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.

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, military identification, 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 fraud alert or 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
888-298-0045	1-888-397-3742	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

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 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.