

1555 N. RiverCenter Drive
Suite 206
Milwaukee, WI 53212



August 8, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Case # 489813

NOTICE OF DATA BREACH

Dear Jeff Karberg;

The purpose of this letter is to notify your office of a recent privacy incident that occurred impacting two residents of your state. First, let me state that Humana takes all privacy concerns seriously and is taking appropriate steps to prevent errors such as this in the future.

What Happened?

The Centers for Medicare and Medicaid Services (CMS) Interoperability and Patient Access rule is focused on breaking down barriers in the nation's health system for patients to get access to their electronic health information when they need it. To help patients access their electronic health information through an application of their choice, Independent Care Health Plan ("iCare") has contracted with Onyx Technology, LLC ("Onyx").

On June 28, 2022, Onyx became aware of suspicious activity within systems used every day in the course of using information technology. Onyx immediately began an investigation to confirm the security of their network and to determine the nature and scope of this event. With the assistance of third-party forensic investigators, Onyx learned that a server was subject to unauthorized access between March 29, 2022, and June 28, 2022. On July 7, 2022, Onyx concluded its investigation. They were unable to determine what files on the server were viewed by the unauthorized person.

What Information Was Involved?

The investigation determined that at the time of the event, the following information pertaining to residents of your state was stored within the files on the impacted server: name, date of birth, address, phone number, iCare member Identification number, Medicare Identification date of service, and provider's name.

What We Are Doing

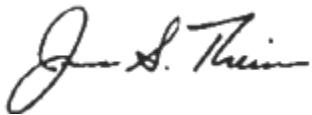
iCare takes this incident and the security of information within their care very seriously. Onyx immediately engaged legal counsel and launched an in-depth investigation upon discovery of this incident to determine the full nature and scope.

Notification letters were sent to two residents who were impacted by this situation on August 12, 2022. Attached you will find a copy of the letter that includes an application for free credit monitoring, and free identity theft protection for two years. In accordance with Maryland state law, we have also notified the Department of Insurance.

iCare will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,

A handwritten signature in black ink, reading "James S. Theiss". The signature is fluid and cursive, with the first name "James" and last name "Theiss" clearly legible.

James S. Theiss
Associate VP, Privacy & Ethics
Humana Inc.
502-580-4322
jtheiss@humana.com

Attachments



INDEPENDENT CARE HEALTH PLAN

Return Mail Processing

PO Box 589

Claysburg, PA 16625-0589

onyx

August 12, 2022

i1919-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



RE: 489813

NOTICE OF DATA BREACH

Dear Sample A. Sample:

Background

Onyx Technology, LLC ("Onyx"), is a vendor of Independent Care Health Plan ("iCare"). Onyx is writing to notify you of an event that may involve some of your personal information. iCare has contracted with Onyx to help patients get access to their electronic health information when they need it. We do not think that your information has been misused because of this event. We are giving you things you can do to protect your information.

What Happened?

On June 28, 2022, Onyx learned of an attack on their computer systems. Onyx immediately reviewed their systems and hired a security firm to investigate. Onyx regained access to its systems on July 7, 2022. A server may have been removed or accessed beginning on March 29, 2022, and ending on June 28, 2022. On July 15, 2022, the security firm found that some information related to you may have been accessed.

What Information Was Involved?

The personal information that was at risk includes:

- Name
- Date of Birth
- Address
- Phone number
- iCare member ID Number
- Medicare ID Number
- Date of Service
- Provider's Name

0000001



i1919-L01

We Know That You May Be Worried About What Took Place

We would like to help you safeguard your information from potential misuse. We have partnered with Experian Consumer Services. You are entitled to free credit monitoring for two years. A description of this product and instructions about how to enroll are included in this mailing in the "STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION" Section.

What You Can Do

We do not think your personal information will be used inappropriately because of the incident that took place. However, we ask you to remain vigilant. There are steps you can take to protect yourself. Review the following for suspicious activity:

- Explanation of Benefit (EOB) Letters
- SmartSummary Statements
- Medical Records
- Account Statements and Credit Reports

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.

For More Information

If you have additional questions, please contact our toll-free, dedicated assistance line at **(833) 475-1811**, Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **B058421**. If you have a speech or hearing impairment and use a TTY, call **800-833-3301**. You may also write to Onyx at 6518 Meadowridge Road #100, Elkridge, Maryland 21075.

Sincerely,

A handwritten signature in black ink, appearing to read "M. Scrimshire", with a stylized flourish at the end.

Mark Scrimshire
Chief Interoperability Officer
Onyx Technology, LLC

Enclosures

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring Services

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: November 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 475-1811**, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays) by **November 30, 2022**. Be prepared to provide engagement number **B058421** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring: Actively** monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000001



Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

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, 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
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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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 New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

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.



