Choice Health

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589



October 7, 2022

i4357-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

***RE: Notice of Data Breach. Please read this entire letter.***

Dear Sample A. Sample:

At Choice Health, we are committed to protecting the confidentiality and security of your personal information. We are sending you this letter to let you know that Choice Health recently experienced a security incident that may have resulted in unauthorized access to your personal information. At this time, we are not aware of any misuse of your personal information.

**What Happened?** On May 14, 2022, Choice Health learned an unauthorized person was offering to make available data allegedly taken from Choice Health. We promptly began an investigation into the incident. On May 18, 2022, we determined that, due to a technical security configuration issue caused by a third-party service provider, a single Choice Health database was accessible through the Internet. Based on our investigation, an unauthorized individual accessed the database from the Internet and obtained certain database files on or about May 7, 2022. We are notifying you of this incident because your personal information was in the database.

**What Information Was Involved?** The files obtained by the unauthorized individual contained the following types of personal information, some of which may have been included about you first and last name, address, provider names, medical history, SSN, email, dates of coverage, health plan Id number, Medicaid number, plan information, and Medicare number.

**What Are We Doing?** Upon learning of the incident, we promptly worked with our third-party service provider to reconfigure the security settings on the database, and we confirmed that the database is no longer accessible through the Internet. We have also taken steps to enhance our data security measures to prevent the occurrence of a similar event in the future, including requiring multi-factor authentication for all access to database files.

Although we have no reason to believe that your information has been misused because of this incident, we would like to offer you a complimentary 24-month membership of Experian IdentityWorks℠. 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 January 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(866) 578-5413** by **January 31, 2023**. Be prepared to provide engagement number [redacted] as proof of eligibility for the Identity Restoration services by Experian.

Please review the sheet enclosed with this letter for information about activating Experian's IdentityWorks services.

**What You Can Do.** You should consider taking the following steps to protect yourself:

- Be attentive to documents related to medical services that you usually receive and that suddenly do not arrive, as you usually receive them.
- All mail related to medical or financial information should be destroyed and preferably shredded before you throw it away.
- Be careful when offering personal information over the phone, mail or internet, and unless you are sure of the person with whom you are dealing, offer as little information as possible.
- Review the "General Information About Identity Theft Protection" materials that are included with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

**As a precaution to protect against misuse of your health information, we recommend that you regularly monitor account statements and the explanation of benefits statements that you receive from your health plan to check for any unfamiliar health care services. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please contact the number on your member identification card. If you do not regularly receive explanation of benefits statements, you may request that your health plan send you these statements following the provision of any health care services in your name or plan number by contacting the number on your member identification card.**

**For More Information.** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call **(866) 578-5413** 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). Be prepared to provide your engagement number **B072358.**

Sincerely,

*Colleen Pappas*

Colleen Pappas, Vice President
Choice Health

## ADDITIONAL DETAILS REGARDING YOUR TWENTY-FOUR (24) MONTHS 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 specialists 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.
- **$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).

Please note that Identity Restoration is available to you for twenty-four (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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) months membership.

* 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.

## Reference Guide

### Order Your Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you find anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report as soon as possible so the information can be investigated, and if found to be in error, corrected.

### Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides and interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

**Step 1: Call the companies where you know fraud occurred.**

**Step 2: Place a fraud alert and get your credit report.**

**Step 3: Report identity theft to the FTC.**

**Step 4: File a report with your local police department.**

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at IdentityTheft.gov/steps.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC at the address below or visiting the website below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-438-4338
1-866-653-4261 (TTY)
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

### Place 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 a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by

calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

| Credit Agency | Mailing Address | Phone Number | Website |
|---|---|---|---|
| **Equifax** | Equifax Information Services LLC<br>P.O. Box 105069<br>Atlanta, GA 30348-5069<br><br>Equifax Fraud Request Form<br><br>*Mail the fraud request form to the address listed above. | 1-800-525-6285 | https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ |
| **Experian** | Experian<br>P.O. Box 9554<br>Allen, TX 75013 | 1-888-397-3742 | www.experian.com |
| **TransUnion** | TransUnion LLC<br>P.O. Box 2000<br>Chester, PA 19016 | 1-800-680-7289 | https://fraud.transunion.com/ |

## Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request. You can request a security freeze by contacting the credit bureaus at:

| Credit Agency | Mailing Address* | Phone Number | Website |
|---|---|---|---|
| **Equifax** | Equifax Security Freeze<br>P.O. Box 105788<br>Atlanta, GA 30348<br><br>Equifax Freeze Request Form<br><br>*Mail the freeze request form to the address listed above. | Automated line:<br>1-800-349-9960<br><br>Customer Care:<br>1-888-298-0045 | https://www.equifax.com/personal/credit-report-services/credit-freeze// |
| **Experian** | Experian<br>P.O. Box 9554<br>Allen, TX 75013 | 1-888-397-3742 | www.experian.com/freeze |
| **TransUnion** | TransUnion<br>P.O. Box 160<br>Woodlyn, PA 19016 | 1-888-909-8872 | https://www.transunion.com/credit-freeze |

**Additional Attorney General Office Identity Theft Resources.** You can obtain information from your state's Attorney General's Office about steps that you can take to help prevent identify theft. Please see the information below for states that provide these resources:

**For California Residents**. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

**For District of Columbia Residents**. You can obtain additional identity theft information from the District of Columbia's Attorney General Office (https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft) to learn more about protection against identity theft.

**For Maryland Residents**. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491
Fax: 1-410-576-6566
Email: idtheft@oag.state.md.us
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

**For North Carolina Residents** You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000

Website: https://ncdoj.gov/

Identity Theft Link: Protecting Your Identity - ID Theft Protection by NC DOJ.

**For Oregon Residents**. You can obtain additional identity theft information from the Oregon Attorney General Office (https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/) to learn more about protection against identity theft.

**For Rhode Island Residents**. You can contact the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

Phone: 1-401-274-4400
Fax: 1-401-462-9532
Email: DBR.Insurance@dbr.ri.gov
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#

**Precautions to Help You Avoid Becoming a Victim**

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown, individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).

5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.