



4349 Easton Way
Suite 300
Columbus, OH 43219

June 29, 2020

NOTICE OF SECURITY INCIDENT

Buckeye Health Plan was recently notified that our vendor, Magellan, was the victim of a criminal ransomware attack. We are providing notice of this incident, along with background information of the incident and steps those affected can take.

Why Does Magellan Have My Personal Information

Buckeye Health Plan uses Magellan to provide consultation services to your health care provider about benefits, such as radiology services, like CT and MRI scans, physical therapy and occupational therapy.

What Happened

On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan's systems after sending a phishing email on April 6, 2020 that impersonated a Magellan client. Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. On June 2, 2020, the investigation revealed that this incident may have affected personal information.

We have no evidence that any personal information has been misused.

What Information Was Involved

The personal information may have included your name and one or more of the following:

- treatment information
- health insurance account information
- member ID
- other health-related information
- email addresses
- phone numbers
- physical addresses

In limited circumstances, Social Security Numbers may have been affected.

What We Are Doing

Buckeye Health Plan has worked closely with Magellan since this incident occurred. Magellan immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. In addition, to help prevent a similar type of incident from occurring in the future, Magellan has implemented additional security protocols designed to protect our network, email environment, systems, and personal information. Buckeye Health Plan will continue to work with Magellan to monitor the implementation and effectiveness of these new controls.

What You Can Do

Please review the “Information About Identity Theft Protection” reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file. Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit or other records. Review any statements you receive pertaining to your health plan benefits regularly and carefully. If you see indications of any treatment or services that you believe you did not seek or receive, then call the member service number listed below.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact us at 1-866-549-8289 (TTY: 711). We are available Monday through Friday, 8:00 A.M. to 8:00 P.M.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	Trans Union
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission’s (“FTC”) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone’s guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.