



VIA ELECTRONIC MAIL

May 8, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: IDTheft@oag.state.md.us

RE: Notification of Keenan & Associates Security Incident

Dear Office of the Attorney General representative:

Aetna is providing your office with notice of a security breach that occurred at Keenan & Associates. This incident impacted 3 Maryland residents who are members of a self-funded employee benefit plan sponsored by Fannie Mae for which Aetna serves as the third-party administrator. Aetna has agreed to fulfill the notification obligations for Fannie Mae with respect to the incident described below.

Keenan & Associates ("Keenan") is an insurance brokerage company that provides insurance related risk management, and claims services to clients across the country. One of Keenan's clients is Ontrak Health, a company that provided services in support of Aetna's behavioral health business.

Please note that no Aetna system or service, and no data maintained by Aetna, was involved in this data incident.

I. Brief Description of the Breach

On August 27, Keenan discovered certain disruptions occurring on some Keenan network servers. Keenan immediately began investigating the issue and discovered suspicious activity on a limited number of servers. As a precaution, Keenan disconnected the entire network to contain the incident. Keenan has engaged leading third-party cybersecurity and forensic experts to assist in the investigation and remediation, and law enforcement has been notified. Within hours of identifying the incident, Keenan had contained it.

Keenan's investigation determined that an unauthorized party gained access to certain Keenan internal systems at various times between approximately August 21, 2023, and August 27, 2023. Findings from the investigation indicate that the unauthorized party obtained some data from certain Keenan systems during this period. Keenan was able to retrieve the data involved from the unauthorized party and has taken steps to delete the data. At this time,

Keenan has no reason to believe this data was further copied or retained by the unauthorized party.

Keenan conducted a thorough review of the data involved to identify individuals whose personal information was included. On or around December 11, 2023, Keenan completed its review of the data and began notifying direct clients, including Ontrak, of any client-related personal information included in these files. The review determined that the files contained protected health information along with other personal information for a subset of its clients.

Keenan is not aware of any fraud or misuse of any personal information because of this incident. Keenan does not believe personal information was targeted by the unauthorized party for identity theft purposes, but rather, such information happened to be included in documents taken by the unauthorized party as part of the ransomware incident to extort the company.

The personal information data elements impacted for the individuals were first and last name, date of birth, member ID, and health insurance coverage information.

II. How Keenan Responded

Keenan engaged third party cybersecurity and forensics experts to assist in their investigation and remediation. Law enforcement was also notified. To help prevent a similar type of incident from occurring in the future, Keenan implemented additional security protocols designed to enhance the security of its network, internal systems and applications. Keenan also continues to evaluate additional steps that may be taken to further increase its defenses going forward.

III. How Aetna Responded

On January 10, 2024, Aetna received notice from Ontrak indicating the potential for Aetna membership to have been impacted by this incident. After investigating, we determined that certain PHI of self-funded members may have been impacted by the ransomware attack on Keenan. We had to take incomplete data from the vendor and turn it into something that was actionable, a process that was completed on March 27, 2024. We began notifying our impacted covered entity clients promptly thereafter and accepted delegation for this notice as requested.

In accordance with the obligations set forth at 45 C.F.R. §164.404 and Maryland law, Aetna issued notifications to the impacted members on May 2, 2024 by first class U.S. mail and offered 24 months of credit monitoring. A draft of the notice made to the affected individuals is attached. Aetna is also notifying other federal and state regulatory agencies as required by law.

I want to assure you that Aetna expects its vendors to adhere to the highest of privacy standards.

Sincerely,
Aetna Privacy Office



151 Farmington Avenue, RC61
Hartford, CT 06156

<<Date>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address 2>>

<<City>>, <<State>> <<Zip>>

RE: Notice of Vendor Data Breach

Dear Aetna Member,

Aetna places a high priority on protecting the privacy and security of our members' information and takes its responsibility to safeguard this information very seriously. We are writing on behalf of <<Entity>> to inform you of a recent security incident at Keenan & Associates ("Keenan") that may have involved your protected health information ("PHI").

Keenan is an insurance brokerage company that provides insurance-related risk management, and claims services to clients across the country. One of Keenan's clients is Ontrak Health ("Ontrak"), a company that provided services in support of Aetna's behavioral health business.

We want you to understand the steps we have taken to address this issue and additional steps you can take to protect your information. The remaining sections of this letter explain the incident and offer additional assistance for protecting your information.

What Happened: On August 27, 2023, Keenan discovered certain disruptions occurring on its network servers and undertook an investigation. Keenan determined it was impacted by a ransomware incident where an unauthorized party gained access to certain Keenan internal systems between August 21 and August 27, 2023, and the unauthorized party obtained data from Keenan's systems. According to Keenan, they were able to retrieve the data from the unauthorized third party and reported they had no reason to believe the data was further copied or retained by the unauthorized party.

On or around December 11, 2023 Keenan completed its review of the data and began notifying direct clients, including Ontrak, of any client-related personal information included in these files. On January 10, 2024, Aetna received notice from Ontrak indicating the potential for Aetna

membership to have been impacted by this incident. After investigating, we determined that certain elements of your PHI may have been impacted by the security incident at Keenan.

What Information Was Involved: The personal information included your <<Data Elements>>. **It is important to note that Social Security Numbers and financial account information were not impacted.**

What We are Doing: As soon as we became aware of the incident, we took immediate action to investigate. Keenan confirmed that they engaged law enforcement as well as third party cybersecurity and forensics experts to assist in their investigation and remediation. Keenan implemented additional security protocols designed to enhance the security of its network, internal systems, and applications. Please note that no Aetna system or service, and no data maintained by Aetna, was involved in this data incident.

What You Can Do: Aetna is providing this notification to all impacted individuals via First Class Mail. As a precaution, we have secured the services of Equifax to provide identity theft restoration and credit monitoring services at no cost to you for 24 months. Information about the Equifax Complete™ Premier identity theft protection product is included with this letter.

We also encourage you to remain vigilant in monitoring your account statements, EOBs, and credit reports for incidents of unauthorized activity, and to promptly report such incidents. For more information on how to protect your personal information and online accounts, please visit <https://consumer.ftc.gov/articles/protect-your-personal-information-and-data>.

Protection of your information:

Order Your Free Credit Report. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

The three credit bureaus (Equifax, Experian, and TransUnion) provide free annual credit reports only through the website, toll-free number, or request form. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax	www.equifax.com	(800) 685-1111
Experian	www.experian.com	(888) 397-3742
TransUnion	www.transunion.com	(800) 916-8800

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the “inquiries” section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the “personal information” section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus 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 credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff’s office because it may signal criminal activity.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

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, and local law enforcement. You may also contact these agencies for information on how to prevent or minimize the risks of 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).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov/Pages/CPD/default.aspx, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 for more information about preventing identity theft.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For Rhode Island residents: You may contact the Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, <https://riag.ri.gov/>.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to obtain a police report.

Placing a Security Freeze. You have a right to place a “security freeze” on your credit report, at no charge, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services/>

<https://www.experian.com/freeze/center.html>

<https://www.transunion.com/credit-freeze>

As of February 20, 2023, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	Online	Physical Mail	Phone Number
Equifax	<i>Freeze request may be submitted via your myEquifax account, which you can create here:</i> https://my.equifax.com/consumer-registration/UCSC/#/personal-info	<i>Mail the Equifax Freeze Request Form to:</i> Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 <i>Form may be found here:</i> https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	<i>Freeze request may be submitted here:</i> https://www.experian.com/ncaconline/freeze	<i>Mail the request to:</i> Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 <i>Request must include:</i> ● Full Name ● Social security number ● Complete address for last 2 years ● Date of birth ● One copy of a government issued identification card, such as a driver's license, state ID card, etc. ● One copy of a utility bill, bank or insurance statement, etc.	888-397-3742
TransUnion	<i>Freeze request may be submitted via your TransUnion account, which you can create here:</i> https://service.transunion.com/dss/orderStep1_form.page?	<i>Mail the request to:</i> TransUnion P.O. Box 160 Woodlyn, PA 19094 <i>Request must include:</i> ● Full Name ● Social security number ● Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert. To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-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. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

We take the privacy of member information very seriously and deeply regret that this incident occurred. Should you see any suspicious activity on your account, or have any additional questions, you may contact Aetna at the toll-free number on the back of your ID card.

Sincerely,

Aetna Privacy Office