VIA ELECTRONIC MAIL

December 10, 2020

North Dakota Office of the Attorney General
600 East Boulevard Avenue
Department 125
Bismarck, ND 58505-0040
ndag@nd.gov

RE: Notification of EyeMed Information Security Incident

Dear Office of the Attorney General representative:

Aetna is writing to notify the Office of the Attorney General (the "Office") that it recently determined that a security incident that occurred at one of its vendors, EyeMed Vision Care LLC ("EyeMed"), affected 569 North Dakota residents who are/were members of fully-insured Aetna Vision plans. Aetna is providing this notice to the Office in accordance with N.D. Cent. Code Ann. §51-30-02. Please note that no Aetna system or service, and no data maintained by Aetna, was involved in this data breach.

I. Brief Description of the Breach

On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book. On the same day, EyeMed took immediate action to block the unauthorized individual's access to the mailbox and secured the mailbox. EyeMed immediately launched an investigation into the incident and engaged a cybersecurity firm to assist in its efforts. It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.

Following a detailed analysis and review of all compromised emails and files, EyeMed determined that personal information that may have been accessed could include the following types of information: full name, address, date of birth, phone number, email address and vision insurance account/identification number. For a relatively small subset of individuals, partial or full social security numbers and/or financial account numbers were implicated, and in a few cases, medical diagnoses and conditions, and treatment information were implicated.

II. How EyeMed Responded

EyeMed retained Kroll, a firm that handles cyber incidents and breach response, to assist in the investigation. The parties involved are not aware of any fraud or misuse of any personal information as a result of this incident. EyeMed does not believe that personal information was targeted by the threat actor for purposes of identity theft, but rather, such information happened to be included in the email account accessed by the threat actor as part of a broader phishing campaign.

EyeMed has already implemented the measures set forth below, among others, in response to this incident:

-Required complex password changes to all its employee accounts and added multifactor authentication.
-Engaged third-party security vendors to assess existing security and privacy controls and identify possible opportunities to monitor and reduce risk.
-Engaged a third-party to complete a new enterprise level HIPAA risk assessment to ensure EyeMed continues to provide strong security controls based on the processes and type of data retained by the organization.

In addition, EyeMed is evaluating and implementing new tools and technologies to recognize and prevent potential threats to its data. EyeMed is also implementing password assessment products, improved secure transport tools, improved phishing blocking and threat hunting technology.

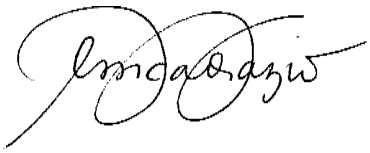
III. How Aetna Responded

EyeMed first notified Aetna of this incident on September 28, 2020. On October 14, 2020, EyeMed confirmed an impact to Aetna membership and provided Aetna with a cursory list of affected individuals. Because the list lacked certain important information, Aetna promptly initiated a review of this list to identify Aetna members, their benefit plans, and other pertinent information needed for the response. The list Aetna received from EyeMed did not consistently include this information. Aetna worked diligently, and expended considerable time and resources, to review the limited, inconsistent personal information included in the EyeMed list to locate the information necessary to attribute the listed individuals to their respective employer groups. This process was completed on December 3, 2020. Aetna has also had several communications with EyeMed regarding this breach to assist in its own investigation and review of the matter.

In accordance with the obligations set forth at 45 C.F.R. §164.404 (notifications to individuals by a HIPAA covered entity) and North Dakota law, EyeMed will be issuing notification on Aetna's behalf to the impacted members by first class U.S. mail as well as offering 24 months of credit monitoring. Aetna anticipates that the mailing of all such notifications will take place beginning on December 11, 2020. A draft of the notice that will be sent 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. If you have any questions, you may contact me at 860-273-4006 and DorazioJ1@aetna.com or by mail at 151 Farmington Avenue, RC61, Hartford, CT 06156.

Sincerely,



Jessica Dorazio
Executive Director, Senior Counsel – Privacy & Security

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>

<<b2b_text_1 (Security Incident / Re: Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

EyeMed manages vision benefits on behalf of your <<b2b_text_2 (carrier or Name of Covered Entity)>>. EyeMed takes the privacy and confidentiality of your information very seriously. We write to inform you of a data security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and steps you can take in response.

What happened?

On July 1, 2020, EyeMed discovered that an unauthorized individual gained access to an EyeMed email mailbox and sent phishing emails to email addresses contained in the mailbox's address book. On the same day, EyeMed took immediate action to block the unauthorized individual's access to the mailbox and secured the mailbox. EyeMed immediately launched an investigation into the incident and engaged a cybersecurity firm to assist in its efforts. It was determined that the unauthorized individual first gained access to the mailbox on June 24, 2020, and that access terminated on July 1, 2020.

What information was involved?

The mailbox contained information about individuals who formerly or currently receive vision benefits through EyeMed. Although EyeMed could not fully determine whether, and to what extent, if any, the unauthorized individual viewed or copied personal information, it is possible that personal information was viewed or acquired by the unauthorized individual.

Following a detailed analysis and review of all potentially compromised emails and files, EyeMed identified the names of all individuals who were impacted, as well as the type of information included in those files. Personal information that may have been accessed could include the following types of information: <<b2b_text_3 (Impacted Data)>><<b2b_text_4 (Impacted Data)>>.

What we are doing:

EyeMed is committed to safeguarding your personal information and has taken immediate steps to enhance the protections that were already in place before this incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all our employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **December 28, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your identity monitoring services is included with this letter.

What you can do:

EyeMed is not aware of any misuse of your information. However, we want to let you know of steps you may want to take to guard against potential identity theft or fraud. We encourage you to remain vigilant by regularly reviewing your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify services that you did not receive or accounts, charges, or withdrawals that you did not authorize, you should immediately contact and report to the involved company and to credit reporting agencies.

Please also review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

More Information:

If you have questions, please call 1-888-974-0076, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time<<b2b_text_5 (or visit https://eyemed.com/en-us/notice)>>. Please have your membership number ready.

Sincerely,

Jason D. Groppe
Chief Privacy Officer (N.A.)

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

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.

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).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a security freeze 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 5 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, and display your name, current mailing address, and the date of issue.

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 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.oag.state.md.us, 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 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

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 if you are a victim of identity theft.

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

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.