

<Date>

<First Name> <Last Name>
<Address 1>
<Address 2>
<City>, <State> <Zip>

Dear <First Name>,

We're serious about protecting your personal information. And we want to be open with you when there's a problem. That's why we're reaching out to let you know about a security incident that may result in a privacy risk to you. On November 9, 2020, our vendor, EyeMed, let us know it experienced a cyberattack that affected your information. EyeMed provides vision care for our members, and that's why they had your information.

What information was involved?

Someone could have found one or more of these facts about you:

- Name
- Date of birth
- Physical address
- Phone number
- Social security number
- Health plan information
- Member ID
- Treatment information

What happened?

On July 1, 2020, EyeMed found out someone illegally accessed one of its email mailboxes and used it to send phishing emails to email addresses in the mailbox's address book. After discovering this incident, EyeMed hired a cybersecurity firm to investigate. The investigation showed someone may have accessed or gotten some of your personal information. At this point, we're not aware of any fraud or misuse of any of your personal information as a result of this incident, but we still want to make sure you know about it.

What we're doing about it

We'll let you know if we learn something more that affects you or your information. EyeMed has already added new security measures, like stronger password requirements and additional training, to better protect the information it has.

To help protect you even more, EyeMed is offering you Kroll identity monitoring services at no cost for two years. Kroll is experienced in helping people whose information has been involved in a data breach or other cybersecurity incident. 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 March 1, 2021, to do so. Your EyeMed Member code is <Member Code>.

We've included more details about identity monitoring with this letter.

Other tips to help you protect your information

The Federal Trade Commission's website, consumer.ftc.gov, lists steps you can take to help protect your information and your privacy. You may also contact the credit reporting companies listed below to order your free annual credit reports, place a 90-day fraud alert on your credit file or place a security freeze on your credit file:

- Equifax: 1-800-525-6285
- Experian: 1- 888-397-3742
- TransUnion: 1-800-680-7289
-

We're here to help. If you have any questions about this letter, please call us at **1-888-455-3824** between 8:30 a.m. and 4:30 p.m. ET, Monday through Friday, or email us at Privacy_Office@BCBST.com.

Best of Health,

Sharon Saville
Privacy Analyst
BlueCross BlueShield of Tennessee Privacy Office

September 28, 2020

Thora A. Johnson

T 410.244.7747

F 410.244.7742

TAJohnson@Venable.com

VIA ONLINE FORM

Office of Consumer Affairs and Business Regulation

Attn: Undersecretary Edward A. Palleschi

501 Boylston Street, Suite 5100

Boston, MA 02116

Re: EyeMed Security Incident

To Whom It May Concern:

We are writing on behalf of our client, EyeMed Vision Care LLC (“EyeMed”), to notify you of a security incident currently known to involve █████ residents of Massachusetts. EyeMed’s address is 4000 Luxottica Place, Mason, OH 45040. The security incident affected individuals who currently or formerly received vision benefits from their employer. EyeMed manages vision benefits on behalf of covered entities subject to the Health Insurance Portability and Accountability Act (“HIPAA”).

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 were implicated, and in a few cases, medical diagnoses and conditions, and treatment information were implicated. While the review of the information is complete with respect to one covered entity, the assessment of the remaining information in the mailbox is ongoing with respect to other HIPAA covered entities.

EyeMed has taken immediate steps to enhance the protections in place before the incident. In addition to the investigation, EyeMed made changes to how authorized individuals access the

September 28, 2020

Page 2

EyeMed network and required immediate complex password changes to all employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training.

Beginning on September 28, 2020, EyeMed will mail notification letters via United States Postal Service First Class mail to affected individuals. We will provide these individuals with 2 years of complimentary identity monitoring services, including credit monitoring, fraud consultation, identity theft restoration, and SSN Trace for minors.

The information submitted herein is proprietary and confidential and should be afforded confidential treatment. If you have any questions, please contact me at (410) 244-7747 or TJohnson@Venable.com.

Sincerely,

_____/s/_____
Thora A. Johnson

From: Data Breaches <noreply+63308160d0553ecb@formstack.com>
Sent: Monday, September 28, 2020 3:30 PM
To: Johnson, Thora A. <IAJohnson@Venable.com>
Subject: Security Breach Notifications

Caution: External Email

Thank you for using the Security Breach Online Notifications Form. The following information has been submitted

Submission Time: Sep 28, 2020 3:30 PM

Section 1: Organization and Contact Information

Business Name: EyeMed Vision Care LLC
Business Address:
Company Type: Commercial
Your Name: Thora Johnson
Last Name: Johnson
Title: Partner, Venable LLP
Contact Address: 750 E. Pratt Street
Suite 900
Baltimore, MD 21202
Telephone Number: (410) 244-7747
Ext:
Email Address: IAJohnson@Venable.com
Relationship to Org: Other

Section 2 Breach Information

Breach Type: Electronic

Date Data Breach Was Discovered: 07/01/2020

Number of Massachusetts Residents Affected: [REDACTED]

Person in custody of personal information when breach occurred. If multiple persons were in custody of personal information, select the relationship of the primary person: Unknown

Please give a detailed explanation of how personal information was protected at the time of the breach, and state the means used (for example, locks/encryption methods): Please see attached letter.

Please select the types of personal information that was included in the data breach: Social Security numbers = Selection(s)

Please check all of the boxes that apply to your breach: The breach was a result of a malicious/criminal act. = Selection(s)

Section 3 Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data: N/A

Date of last review of written security program:

Physical access to systems containing personal information was restricted to authorized personnel only: N/A

Network configuration of breached system: Internet Access Available [REDACTED]

Section 4 Remediation

The company has notified all Massachusetts residents affected by the breach: Yes

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply): Option2 | US Mail

Please explain your answer of other above:

Date notices were first sent to Massachusetts residents: 09/28/2020

Your company offered complimentary credit monitoring services to Massachusetts residents affected by the breach: Yes

Law enforcement has been notified of this data breach: No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring: EyeMed immediately launched an investigation into the incident and engaged a cybersecurity firm to assist in its efforts. In addition to the investigation, EyeMed has taken immediate steps to enhance the protections already in place before the incident. EyeMed made changes to how authorized individuals access the EyeMed network and required immediate complex password changes to all employee accounts. EyeMed is also reinforcing and providing additional mandatory security awareness training. EyeMed also significantly shortened the data retention period for this mailbox. EyeMed is also launching an updated security risk assessment.

Attached file 1:

https://s3.amazonaws.com/files.formstack.com/uploads/3269138/71421777/668246281/71421777_eyemed_regulator_notice_letter_ma_office_of_consumer_affairs.pdf

Attached file 2:

https://s3.amazonaws.com/files.formstack.com/uploads/3269138/71421778/668246281/71421778_eyemed_sample_notification_letter_ma.pdf

Attached file 3:

Attached file 4:

▪



EMERGENCY ALERTS

Coronavirus Updates and Information

HIDE ALERTS ^

Get notified by text, email, or phone in your preferred language. Sign-up for COVID-19 alerts. Nov. 29th, 2020, 5:00 pm [Read more](#) »

For the latest information on COVID-19 Cases, Travel, & Reopening. Nov. 30th, 2020, 5:00 pm [Read more](#) »

Menu

Select Language ▼

State Organizations

Log In to...



Mass.gov

Search Mass.gov

SEARCH

PART OF Identity Theft, Data Privacy and Cyber Security

OFFERED BY Office of Consumer Affairs and Business Regulation

Data Breach Notification Submission

MGL Chapter 93H requires that data breaches be reported to the Office of Consumer Affairs and Business Regulation

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. Keep a copy of this submission for your own records. Please note a [separate notification](#) or follow-up to a previous notification must be sent to the Attorney General's Office.

Are you aware that Massachusetts General Laws Chapter 93H, the Data Breach Notification Law, has changed? Please read our [Frequently Asked Questions](#) regarding data breach notifications and the changes to M.G.L. Chapter 93H.

If you're mailing your submission, please send to: Office of Consumer Affairs and Business Regulation, 501 Boylston St., Suite 5100, Boston, MA 02116 Attention: Undersecretary Edward A. Palleschi

- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please do not include any personally identifiable information for Massachusetts residents in any of the fields.
- Please do not submit your notification more than once (send either by email or mail - not both).

CONTACT

Office of Consumer Affairs and Business Regulation

Address

501 Boylston St, Suite 5100,
Boston, MA 02116

[Directions](#) »

Phone

Consumer hotline

(617) 973-8787

Open M-F 9:00am-4:30pm.

Section I: Organization & Contact Information

Business Name *

EyeMed Vision Care LLC

Is the business located in the United States? *

Yes

No

Business Address *

4000 Luxottica Pl

Address Line 1

Address Line 2

Mason

City

Ohio



State

45040

ZIP Code

Reporting Company Type *

Commercial



Reporting on behalf of another company? *

Yes

No

Your Name *

Thora

First Name

Johnson

Last Name

Title *

Partner, Venable LLP

Contact Address *

750 E. Pratt Street

Address Line 1

Suite 900

Address Line 2

Baltimore

City

Maryland



State

21202

ZIP Code

Telephone Number *

(410) 244-7747

Extension (optional)



Email Address *

TAJohnson@Venable.com

Relationship to Org *

Other



Section II: Breach Information

Is this a follow-up to a previous notification received by our office? *

Yes

No

Breach start date *

Jan 24 2020

Breach end date *

Jul 01 2020

Date Breach was Discovered *

07 01 2020

Person responsible for data breach. *

Unknown

Breach Type *

Electronic

Number of Massachusetts Residents Affected *

168478

Please give a detailed explanation of how the data breach occurred. *

This response was previously provided in the report filed on September 28, 2020.

768 \$50

Please select the type of personal information that was included in the breached data. *

Selection(s)

Financial Account Number:

Social Security numbers:

Driver's License:

Credit/Debit Card Number:

Please check ALL of the boxes that apply to your breach. *

Selection(s)

The person(s) with possession of personal information had authorized access:

The breach was a result of a malicious/criminal act:

The breach occurred while the data was being transported outside of your premises:

The breach occurred at the location of a third party service provider:

There is a written contract in place with the third-party provider requiring protection of personal information.

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data. *

Yes

No

N/A

Physical access to systems containing personal information was restricted to authorized personnel only. *

Yes

No

N/A

Network configuration of breached system *

Internet Access Available

For breaches involving electronic systems, complete the following *

Selection(s)

Breached data was encrypted.

The key to encrypted data was stolen.

Personal information stored on the breached system was password-protected and/or restricted by user permissions.

N/A

Does your business maintain a Written Information Security Program (WISP)? *

Yes

No

Section IV: Remediation

All Massachusetts residents affected by the breach have been notified of the breach. *

Yes

No

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply): *

E-mail

US Mail

Online posting

TV Radio publication

Other

Date notices were first sent to Massachusetts residents (MM DD YYYY) *

09 ▾ 28 ▾ 2020 ▾ 

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services. *

Yes

No

If the breach of security includes a Social Security number, Massachusetts law requires your credit monitoring comply with Section 3A of Chapter 93H *

I acknowledge our credit monitoring complies with section 3A of Chapter 93H

Our breach did not include a Social Security number

Law enforcement has been notified of this data breach. *

Yes

No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring, including updating your WISP. *

This response was previously provided in the report filed on September 28, 2020. Notification to affected Massachusetts residents is ongoing.

708.850

Any documents pertaining to the data breach including the letter being sent to Massachusetts residents must be submitted in this form or sent via email to data.breaches@mass.gov

Do you have any documents that you wish to attach? NOTE: Up to 4 uploads are allowed.

Yes / No *

Yes

No

Note, Massachusetts General Laws Chapter 93H, the Data Breach Notification Law, has changed. Please read our Frequently Asked Questions regarding data breach notifications and the changes to M.G.L. Chapter 93H.

Please review the information you have entered and click on the "Submit Form" button below.

SUBMIT FORM

Did you find what you were looking for on this webpage? *

Yes No

SEND FEEDBACK



[Living](#)

[Site Policies](#)

[Working](#)

[Public Records Requests](#)

[Learning](#)



ck

© 2020 Commonwealth of
Massachusetts

Mass.gov is a service of the
Department of Information
Technology

[Mass.gov Privacy Policy](#)

visiting & exploring

Your Government

Feedback

Accessibility

© 2020 Commonwealth of Massachusetts. All rights reserved. | [Privacy Policy](#) | [Accessibility](#) | [Feedback](#)