

September 18, 2018

Via USPS and email: attorneygeneral@doj.nh.gov
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Security Breach: Med-A-Vision, Inc.

To Whom It May Concern:

Our firm represents Med-A-Vision, Inc. (Maine Insurance License Number TAD117543), a third-party administrator providing health reimbursement and related services for over 185 companies in the State of Maine. Med-A-Vision is a small company with five (5) employees, located in the city of Brewer, Maine.

Pursuant to N.H. Rev. Stat. § 359-C:20, we are writing to notify you of an unauthorized access or use of personal information, in electronic form, involving twenty-eight (28) New Hampshire residents. We previously reported this incident to the Maine Bureau of Insurance on August 31, 2018, at which time our investigation was ongoing. Enclosed please find a copy of our letter to the Main Bureau of Insurance for your reference. During the week of September 4, 2018, we were able to verify that personal information had been compromised, and to identify the affected individuals.

In sum, an unauthorized user accessed and copied emails containing personal information in a Med-A-Vision employee's mailbox as early as July 17, 2018 at 1:28PM. Med-A-Vision first became aware of an authorized access on August 13, when a third party reported receiving a peculiar email from what appeared to be the Med-A-Vision employee's account. Our firm became involved in this matter shortly thereafter. On Tuesday, September 4, 2018, we were able to verify that personal information was contained in the emails that were accessed, and, over the subsequent week, we worked to identify each individual whose personal information was compromised, which number totals approximately 1,057.

The twenty-eight (28) affected New Hampshire residents will shortly receive written notice pursuant to N.H. Rev. Stat. § 359-C:20. Enclosed please find a copy of such notice. The notice letter will include free credit monitoring for one year, through Experian, to all impacted individuals. We believe that no other information or files within Med-A-Vision's system were accessed, apart from the email account of the single employee, and we have taken steps to ensure that emails and attachments containing personal information are promptly deleted and not stored

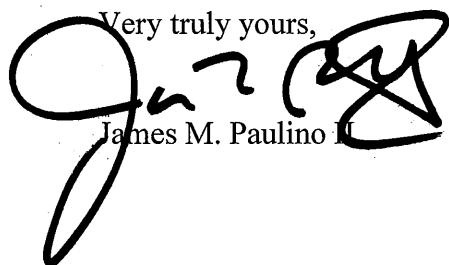
 **We've gone paperless**

Please send mail to our scanning center at: PO Box 487, Buffalo, NY 14201

Office Location: 2 State Street, Suite 1200, Rochester, NY 14614-1342
585.295.5400 | Fax: 585.295.8300 | www.GoldbergSegalla.com

in email accounts. We have also increased the security associated with Med-A-Vision email accounts going forward.

We remain available should you have any questions or concerns regarding the foregoing, and we will provide any supplemental information as it becomes available.

Very truly yours,

James M. Paulino II

JMP:rmp

August 31, 2018

Via Email Benjamin.Yardley@maine.gov

Superintendent Eric Cioppa
Bureau of Insurance
76 Northern Avenue
Gardiner, Maine 04345

Re: Notification of Security Breach

Dear Superintendent Cioppa:

Our firm represents Med-A-Vision, Inc. (License Number TAD117543), a third-party administrator providing health reimbursement and related services for over 185 companies and their employees in the State of Maine. Med-A-Vision is a small company with five (5) employees, located in the City of Brewer.

This week, as the result of forensic analysis, we became aware that an unauthorized user accessed and copied emails potentially containing personal information in a Med-A-Vision employee's mailbox. At this time, we believe no other mailboxes or systems were accessed. We are in the process of investigating whether or not personal information was contained in the emails that were accessed, and, if so, the identities of any Maine residents whose personal information may have been disclosed, which investigation we hope to complete next week. Once we determine the identities of any affected individuals, we will take prompt steps to provide written notice.

We have been unable to determine exactly how the attacker gained access to the email account, but our investigation revealed that the access may have occurred as early as July 17, 2018 at 1:29PM. Med-A-Vision became aware of an unauthorized access on Monday, August 13, 2018, when a third-party reported receiving a peculiar email from what appeared to be the Med-A-Vision employee's account. My firm became involved on Friday, August 17, 2018, and we promptly arranged for a forensic investigation to determine whether the intrusion was limited to sending malicious emails, or extended to accessing emails potentially containing personal information in the subject mailbox. The investigation also analyzed other Med-A-Vision mailboxes associated with the subject account.

As a result of the forensic investigation, we have determined that the intruder did in fact view and copy emails from the single employee's mailbox, in addition to using the mailbox to send messages. We are currently in the process of determining whether the emails viewed and/or copied by the intruder contain personal information, as there were limited emails in the subject account containing such information. We anticipate the investigation will be completed by

 **We've gone paperless.**

Please send mail to our scanning center at: PO Box 487, Buffalo, NY 14201

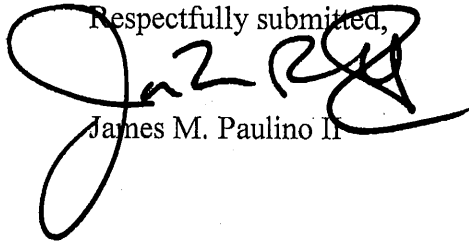
Office Location: 2 State Street, Suite 1200, Rochester, NY 14614-1342
585.295.5400 | Fax: 585.295.8300 | www.GoldbergSegalla.com

Superintendent Eric Cioppa
August 31, 2018
Page 2

Tuesday, September 4, 2018. At this point, we do not know the number of potentially affected individuals; however, we do not believe it would reach the threshold requiring notification to national consumer reporting agencies.

We remain available should you have any questions or concerns regarding the foregoing, and we will provide any supplemental information as it becomes available.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'James M. Paulino II', written over the typed name.

James M. Paulino II

JMP:rmp

September 14, 2018

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter.

Dear [Insert customer name]:

We are contacting you regarding a data security incident that has occurred at Med-A-Vision, Inc., where the email account of one of our employees was accessed by an unauthorized user. The email account contained emails with attachments that included your name and social security number, and may have included information regarding your health savings or flexible spending account. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident.

It seems that on August 13, 2018, an unauthorized user was sending emails with malicious attachments from one of our employee's email account, while that employee was on vacation. When one of the recipients of the email contacted us, we immediately began an investigation to determine who had accessed the account, and what information may have been compromised. Our investigation ultimately revealed that the unauthorized user was not simply sending emails from the account, but also accessed numerous emails containing personal information. Last week, we were able to determine that emails containing your personal information were accessed.

We believe that no other information or files within our system were accessed, apart from the email account of the single employee, and we have taken steps to ensure that emails and attachments containing personal information are promptly deleted and not stored in email accounts. We have also increased the security associated with our email accounts going forward.

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. 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:** December 31, 2018 (Your code will not work after this date.)
- **Enroll at** the Experian IdentityWorks website: <https://www.experianidworks.com/credit>
- Provide your **activation code:** [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team

at 877-890-9332 by December 31, 2018. Be prepared to provide engagement number **DB08673** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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:

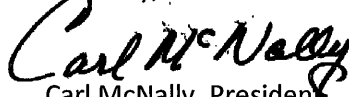
- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are 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.
- **Up to \$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 and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. 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 (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 this Identity Restoration support is available to you for one year 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. You will also find self-help tips and information about identity protection at this site.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 877-890-9332.

Sincerely,



Carl McNally, President
Med-A-Vision, Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions