MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 22, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

To Whom It May Concern:

We represent Pioneer Valley Ophthalmic Consultants, PC ("PVOC"), formerly located at 489 Bernardston Road, Greenfield, MA 01301, and are writing to notify your office of an incident that occurred at one of PVOC's third-party vendors, Alta Medical Management and ECL Group, LLC (collectively "AMM"), which may affect the security of personal information relating to three hundred and fifty (350) New Hampshire residents. PVOC was in the process of dissolution when it was notified of the event by AMM. Please note that PVOC is no longer servicing patients as a practice, and dissolution of the practice is imminent at this time. By providing this notice, PVOC does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 3, 2022, PVOC learned that AMM's billing servers were subject to a malware attack by an unknown actor from November 13, 2021, to November 15, 2021. PVOC worked to gather information from AMM in order to determine the nature and scope of the issue. Additionally, on or about May 11, 2022, PVOC learned that Alta's online patient portal was vulnerable to potential unauthorized access of payment receipts until October 26, 2021. Please note that these incidents did *not* involve any internal PVOC computer systems or website, only AMM's. PVOC understands from AMM that AMM's investigations into both incidents were unable to confirm whether any PVOC patient information was accessed or taken by an unauthorized actor. Therefore, out of an abundance of caution, PVOC is providing notification of the incident to PVOC patients whose information was potentially at risk due to this incident.

The information that could have been subject to unauthorized access by the AMM malware incident includes: . The information that could have been subject to unauthorized access by the AMM online patient payment portal incident includes: name, email address, transaction date and time, transaction ID number, statement numbers, last four digits of payment card or account number, and information input into a comments field.

Notice to New Hampshire Residents

On or about May 19, 2023, PVOC began providing written notice of the above incident to affected individuals, which includes three hundred and fifty (350) New Hampshire residents. PVOC also provided notice to and/or published notice in media outlets, where appropriate. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

In addition to notifying potentially impacted individuals, PVOC also notified the Secretary of Health and Human Services ("HHS"), its primary federal regulator, pursuant to the federal Health and Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act.

Other Steps Taken and To Be Taken

Upon becoming aware of the incidents at AMM, PVOC immediately undertook efforts to coordinate with AMM to determine the full nature and scope of this incident. AMM has reported it has put additional measures in place to secure and monitor its environment and will be onboarding additional technical resources and security personnel. PVOC is providing access to credit monitoring services for one (1) year through Sontiq to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, PVOC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. PVOC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. PVOC also provided notice to other state regulators and the three major consumer/credit reporting agencies.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Alex Walker of
MULLEN COUGHLIN LLC

ATW/jlt
Enclosures

EXHIBIT A

Pioneer Valley Ophthalmic Consultants, PC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

May 22, 2023

Dear ,

Pioneer Valley Ophthalmic Consultants, PC ("PVOC"), is writing to inform you of two incidents that occurred at one of our third-party vendors, Alta Medical Management and ECL Group, LLC (collectively "AMM"), which may impact the privacy of some of your information. AMM provided PVOC with patient billing and accounting services to our patients. We are writing to provide you with information about the AMM incidents, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it appropriate to do so.

What Happened? On or about March 3, 2022, PVOC learned that AMM's billing servers were subject to a malware attack by an unknown actor from November 13, 2021, to November 15, 2021. PVOC worked to gather information from AMM in order to determine the nature and scope of the issue. Additionally, on or about May 11, 2022, PVOC learned that Alta's online patient portal was vulnerable to potential unauthorized access of payment receipts until October 26, 2021. Please note that these incidents did *not* involve any internal PVOC computer systems or website, only AMM's.

What Information Was Involved? AMM was unable to confirm whether your information was included in any information that may have been compromised as a result of the above two incidents. Therefore, out of an abundance of caution, PVOC is providing notification to potentially impacted individuals whose information was stored by AMM. The following types of information were potentially impacted by the AMM malware incident that occurred in November 2021 and may vary by individual: . The following types of information were potentially impacted by the AMM online patient payment portal incident that occurred in October 2021:

. To date, PVOC is not aware of any actual or attempted misuse of patient information in relation to these incidents.

What We Are Doing. PVOC takes this incident and the security of information within our and our third-party vendors' care very seriously. Upon becoming aware of this incident, we immediately undertook efforts to coordinate with AMM to determine the full nature and scope of this incident. AMM reported it has implemented additional measures to secure and monitor its environment and will be onboarding additional technical resources and security personnel. PVOC will also be notifying government regulators, as required.

As an added precaution, PVOC is also offering you access to twelve (12) months of complimentary credit monitoring services. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. Individuals who wish to receive these services must enroll by following the attached enrollment instructions. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification

is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your accounts statements and Explanation of Benefits reports, and to monitor your credit reports for suspicious activity and to detect errors. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.* There, you will also find detailed instructions for credit monitoring enrollment. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

For More Information. We understand that you may have questions about the AMM incident that are not addressed in this letter. Please call Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time. Representatives are available for 90 days.

Sincerely,

Pioneer Valley Ophthalmic Consultants, PC

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

1. Website and Enrollment. Go to and follow the instructions for enrollment. When prompted please provide the following unique code to receive services:

2. Activate the credit monitoring provided as part of your Cyberscout identity protection services. The monitoring included in the services must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

3. Telephone. Contact Cyberscout at to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in the Cyberscout credit monitoring services, notify them immediately by calling or by logging into the website referenced above and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a representative who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned a representative who will work with you to identify, stop and reverse the damage quickly.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Hofmann Arthritis Institute PLC is located at 24 South 1100 East Suite 101, Salt Lake City, UT 84102.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the

Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are approximately [34] Rhode Island residents impacted by this incident.