



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED
JUN 23 2022
CONSUMER PROTECTION

Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

1452 Hughes Road, Suite 200
Grapevine, TX 76051

June 17, 2022

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

Dear Sir or Madam:

We represent Sharper Vision P.A. ("Sharper Vision") located at 11184 Antioch Road, Suite 356 Overland Park, KS 66210 and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Sharper Vision 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 December 6, 2021, Sharper Vision discovered that it was unable to access their electronic medical record ("EMR") system hosted on their vendor, Eye Care Leaders' ("ECL") systems. Sharper Vision immediately reverted to paper records to ensure patient care continued uninterrupted. Functionality to the EMR was restored the following week. On April 19, 2022, Sharper Vision received additional information from ECL regarding the event. Sharper Vision has confirmed, through ECL, that the outage was the result of an unauthorized actor gaining access to ECL's systems on December 4, 2021. Unfortunately, the investigation was unable to determine what information, if any, was accessed or acquired by the unauthorized actor as a result of this event. As such, Sharper Vision is providing notice of this incident to its patients out of an abundance of caution. There is currently *no evidence* that this event involved any of Sharper Vision internal systems and all evidence suggests that this event occurred only on ECL's systems.

The information that could have been subject to unauthorized access includes name, Social Security number, government issued identification, and financial account information.

Mullen.law

Notice to New Hampshire Resident

On or about June 17, 2022, Sharper Vision provided written notice of this incident to one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon being notified of the event, Sharper Vision moved quickly to investigate the incident, assess the information available regarding the incident, and identify potentially affected individuals. Sharper Vision is also working to implement additional safeguards around its vendor relationships and training to its employees. Sharper Vision is providing access to credit monitoring services for one (1) year, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Sharper Vision 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. Sharper Vision is also 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.

Sharper Vision is providing written notice of this incident to relevant state and fed regulators, as necessary. Sharper Vision is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1697.

Very truly yours,

Amanda Harvey of
MULLEN COUGHLIN LLC

ANH/jlm
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF <<Variable Header>>

Dear <<Name 1>>:

Sharper Vision P.A. ("Sharper Vision") is writing to inform you of an event that occurred with one of our third-party vendors, Eye Care Leaders ("ECL"), which may affect the privacy of your information. ECL operates and manages Sharper Vision's electronic medical record ("EMR") system through its myCare Integrity software. We are writing to provide you with information about ECL's incident, 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 December 6, 2021, Sharper Vision discovered that it was unable to access the EMR hosted on ECL's systems. Sharper Vision immediately reverted to paper records to ensure patient care continued uninterrupted. Functionality to the EMR was restored the following week. On April 19, 2022, Sharper Vision received additional information from ECL regarding the event. Sharper Vision has confirmed, through ECL, that the outage was the result of an unauthorized actor gaining access to ECL's systems on December 4, 2021. Unfortunately, the investigation was unable to determine what information, if any, was accessed or acquired by the unauthorized actor as a result of this event. As such, Sharper Vision is providing you notice of this incident in an abundance of caution. There is currently *no evidence* that this event involved any of Sharper Vision internal systems and all evidence suggests that this event occurred only on ECL's systems.

What Information Was Involved?

As the investigation was unable to determine if your information was accessed or acquired as a result of this event, we are taking steps to notify you out of an abundance of caution. Your entire patient file may be at risk as a result of this event. This may include your name, address, Social Security number, date of birth, government issued identification number, financial information, health insurance and billing information, diagnosis information, treatment information, and prescription information. To date, ECL has not reported any actual or attempted misuse of this information to Sharper Vision.

What We Are Doing.

Sharper Vision takes this incident and the security of information within our care very seriously. Upon being notified of this incident, we immediately launched an investigation to determine the nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing existing security policies and procedures regarding our third-party vendors and are working to evaluate additional measures to further protect against similar incidents moving forward. We will also be notifying state and federal regulators, as required.

In addition, we are offering credit monitoring and identity theft protection services for <<CM length>> months through Equifax. Please note that while Sharper Vision is offering this at no cost to you, we are unable to enroll you in these services. Please reach out to our dedicated assistance line below for assistance in enrolling in these services.

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 attached enrollment code when calling or enrolling on online, so please do not discard this letter.

For More Information.

We understand you may have additional questions about the ECL incident not addressed in this letter. Please call 877-890-9931 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time for any additional questions you may have or assistance in enrolling in credit monitoring.

Sincerely,

Dr. Aaron R. Florkowski

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION



<<Name 1>>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.
You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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 1-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 will need to provide the following information:

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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a 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
888-298-0045	1-888-397-3742	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

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, DC 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. Sharper Vision is located at 11184 Antioch Road, Suite 356, Overland Park, KS 66210.

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 violators. 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 are <<RI Count>> Rhode Island residents impacted by this incident.

NH DEPT OF JUSTICE
JUN 23 2022 PM 1:08