May 27, 2022 – Finkelstein Eye Associates is issuing notice of a recent data security event that occurred at a third-party vendor, Eye Care Leaders, that may impact the security of certain patient information. On March 1, 2022, we received notification from one of our third-party vendors, Eye Care Leaders, of its ongoing investigation into a cyber event. Eye Care Leaders is a cloud-computer provider that manages the electronic health record system for optometry practices, including Finkelstein Eye Associates. Upon receiving notice of this event, we immediately commenced an investigation to better understand the nature and scope of the event and impact on our data. This notice provides information about the Eye Care Leaders event, our response, and the resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? Eye Care Leaders reported that on December 4, 2021, it experienced a cyber event that resulted in the unauthorized access to, and deletion of, certain customer data on its systems. Eye Care Leaders reported the event to law enforcement and worked with forensic investigators to determine the nature and scope of the event. On April 1, 2022, Eye Care Leaders provided an update on its ongoing investigation and confirmed that an unknown actor potentially had access to all its customers' data. While Eye Care Leaders did not identify any acquisition or exfiltration of customer data, due to limitations in the available evidence for review, it could not definitively rule out the possibility of that activity. On or about April 19, 2022, we received further information from Eye Care Leaders that confirmed its investigation would not be able to limit the scope of customer information that was potentially impacted by the event. Therefore, out of an abundance of caution, we are providing notice to all our patients due to the uncertainty of the Eye Care Leaders event. Please note, if you are a new patient that came to us after December 31, 2021, we received no information from Eye Care leaders to suggest your data was potentially affected.

What Information was Involved? Our investigation determined that the Eye Care Leaders systems could have contained patients' full name, date of birth, Social Security number, financial account information, and health insurance information. For patients that joined the practice after 2013, medical information could have been impacted as well. To date, we have not received confirmation from Eye Care Leaders that specific patient information was accessed, deleted, or acquired by the unknown actor.

What We Are Doing. The confidentiality, privacy, and security of patient information are among our highest priorities, and we take the Eye Care Leaders event very seriously. As part of our ongoing commitment to the security of patient information, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Eye Care Leaders to evaluate additional measures and safeguards to protect against this type of event in the future.

What You Can Do. We encourage our patients to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Patients should report any suspicious activity promptly to their insurance company, health care provider, or financial institution. Patients may also review the information in the below *Steps You Can Take to Help Protect Personal Information*.

For More Information. If patients have additional questions, please call our dedicated assistance line at 1-877-566-5206 Monday to Friday between 8am and 8pm CST.

Steps You Can Take to Help Protect Personal Information

Monitor 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 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, military identification, 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 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
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 St. NW, Washington, D.C. 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.

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 event.