Notice to Individuals regarding Privacy Incident

Colorado Retina Associates ("CRA") recently learned of a breach of part of its secured computer network. CRA deeply regrets this incident occurred. We are providing notice to patients and to individuals who may have been affiliated with CRA to let them know about the incident and what we are doing in response.

On January 12, 2021, CRA first discovered that an unauthorized individual gained access to an employee's work email account when that email account was used to send phishing emails to individuals in the employee's electronic contacts. CRA immediately began investigating, secured that email account, and subsequently secured CRA's entire email environment. CRA hired a national firm with forensic computer expertise to assist in the investigation and to determine the nature and scope of the breach. CRA's forensic investigation concluded on February 24, 2021 and determined that there was unauthorized access to certain CRA email accounts and that two user accounts that had patient information, may have involved "syncing" (copying) of the email account by the unauthorized individual(s) between January 6, 2021 and January 17, 2021. CRA immediately began a detailed analysis and review of all the potentially compromised emails and attachments to identify the names of all individuals who were potentially impacted, as well as the type of information included in these files. Although CRA could not fully determine whether, and to what extent, the unauthorized individual(s) viewed any personal information, regrettably it is possible because of the syncing, that some patients' personal information may have been acquired and could therefore be viewed by the unauthorized individual(s).

Personal information involved may have included any of the following: full name, date of birth, home address, phone number, email address, clinical information such as dates of service, diagnoses and conditions, labs and diagnostic studies, medications, other treatment or procedure information, and certain health insurance, claims, billing, and payment information. For less than 3% of involved individuals social security numbers were involved and for less than 0.2% of individuals, driver's license, financial account, or payment card information was involved.

In response, CRA took immediate steps to enhance the protections that were in place before this incident. CRA made changes to how authorized individuals gain access to accounts and required password changes to all authorized employee accounts. CRA is reinforcing security awareness through reminders to its entire workforce. Additionally, CRA reported this incident to law enforcement for further investigation.

For individuals who may have had information involved in this incident, CRA wants to make them aware of steps they may take to protect against any potential harm. CRA encourage individuals to remain vigilant to the possibility of fraud and identity theft. Individuals should regularly review their financial statements, credit reports, and explanation of benefits (EOBs) from health insurers for any unauthorized activity. If individuals identify services that they did not receive or accounts, charges, or withdrawals that they did not authorize, they should contact and report to the involved company or credit-reporting agency immediately. In addition, individuals can obtain information about placing fraud alerts and security freezes from the Federal Trade Commission and the three national credit reporting agencies at the toll-free numbers, websites, or mailing addresses as follows:

Federal Trade Commission	Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-877-382-4357	1-866-349-5191	1-888-397-3742	1-800-680-7289
600 Pennsylvania Ave., NW	P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

CRA has arranged for individuals with information involved in this incident to be able to enroll, at no charge, in 12 months of identity theft protection services through IDX, a company with data breach and recovery services expertise. To take advantage of this service, an individual will first need to obtain and use the unique enrollment code found in the notice letter mailed on March 12, 2021 to involved individuals for whom CRA had current mailing addresses. For individuals who did not receive a notice letter but whose information may have been involved, they must contact the toll-free number below to determine if their information was involved and if so, to receive a free IDX enrollment code. Please note the deadline to enroll in the identity theft protection services is **June 11, 2021**.

CRA has partnered with IDX to set up a call center to help answer questions and provide additional information to individuals whose information may have been involved. Individuals who have questions, including whether their personal information was involved, should call this toll-free number, **1-833-416-0846**, Monday through Friday between 7 am - 7 pm Mountain Time (closed on holidays). The IDX call center can provide additional information and answers to many questions for individuals whose personal information was potentially involved in this incident.

Recommended Steps to Help Protect Your Information

1. Telephone. Contact IDX at 1-833-416-0846 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. 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 IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help. If you have enrolled and file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft because of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.