

Associated Eye Care
P.O. Box 3923
Syracuse, NY 13220



July 8, 2022

Via First-Class Mail

Notice of Data Incident

Dear [REDACTED]:

We are contacting you to inform you of a data incident experienced by a third-party vendor for Associated Eye Care Partners, LLC (“AEC”). As this relates to you, Associated Eye Care is a complete vision care and treatment center in Wisconsin and Minnesota. The third-party vendor is Netgain Technology, Inc. (“Netgain”), which offers hosting and cloud IT solutions to various industries. This letter contains additional information about the incident, our response to the incident, and steps you can take to protect yourself. Please be assured that AEC takes the protection and proper use of personal information very seriously, and we sincerely apologize for any inconvenience this may cause.

What Happened

Netgain is a third-party entity that offers hosting and cloud IT solutions primarily for the healthcare and accounting industry. AEC, along with thousands of other healthcare entities, retained Netgain for online hosting of its environment, including cloud services and e-mail. On December 4, 2020, Netgain was the target of a cybersecurity incident. Upon notification by Netgain to AEC, we worked with our information technology (IT) support team and engaged a law firm specializing in cybersecurity and data privacy to investigate further. We have also stayed in close communication with Netgain and its breach counsel regarding Netgain’s incident response and forensic investigation. Netgain provided AEC with the data sets that were potentially impacted. AEC then underwent an extensive data mining project to identify all impacted individuals, which was completed on May 16, 2022.

Please rest assured that this incident only impacted data on Netgain’s environment. Therefore, it did not involve AEC’s network or information systems.

Based on the results of this investigation, we have determined that an unauthorized user had access to information, including your name, address, social security number and medical history. **At this time, AEC does not have any evidence to indicate that any of your personal information has been or will be misused as a result of this incident. Nevertheless, AEC decided to notify you of this incident out of an abundance of caution.**

What We Are Doing

In light of this incident, AEC replaced Netgain as its hosting vendor and migrated our environment and data to another service provider that has assured us the data will be hosted in such a way that it cannot be exposed in a similar attack. Additionally, we are working to improve security and mitigate risk by reviewing and altering our

policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

Further, we value the safety of your personal information and are providing you with access to Single Bureau Credit Monitoring services at no charge. 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have, or in the event your identity is compromised. These services will be provided by Cyberscout through Identity Force, a leading data protection company.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/assoceyecare> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] Please note the deadline to enroll is October 31, 2022.

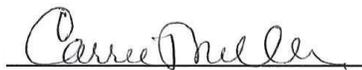
We encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information

If you have additional questions, please call 1-844-514-2125, Monday through Friday, 8:00am – 8:00pm Eastern time, excluding holidays.

Sincerely,



Carrie Miller
Director of Business Operations

* Services marked with an “*” require 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.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

<p style="text-align: center;">Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/</p>	<p style="text-align: center;">Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html</p>	<p style="text-align: center;">TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze</p>
--	--	---

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order 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 generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 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 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 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 at 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 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.