

Oak View Group
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024



60 1 10067 *****AUTO**ALL FOR AADC 980



June 12, 2026

Notice of Security Incident

Dear [REDACTED],

We are writing to inform you of a cybersecurity incident at Oak View Group (“OVG”) that affected certain of your personal information. OVG collected this information from you in the context of your work as a contractor or vendor at an OVG-managed venue. We are writing to provide you with information about the incident, our response, and additional measures you can take to help protect yourself.

What Happened?

On January 19, 2026, OVG discovered that an unauthorized third party gained access to a subset of OVG's legacy systems. Our investigation determined that the unauthorized third party initially gained access on December 16, 2025, and leveraged that access to remove certain files from OVG’s network. OVG promptly launched an investigation and engaged leading cybersecurity experts.

What Information Was Involved?

We can confirm that your affected personal information was limited to following information: name and tax identification number. To date, we are not aware of fraud or misuse of personal information resulting from this incident. There is also no evidence that this information has been posted for sale on the darkweb or has otherwise been made publicly available.

What We Are Doing.

As part of our response, we took the affected system offline and implemented enhanced security safeguards, including rebuilding the environment with updated security measures. We are continuing to evaluate additional steps we can take to prevent something like this from happening again.

While we are not aware of identity theft or fraud related to this incident, we are offering you two years of complimentary credit monitoring and identity restoration services through Cyberscout, a TransUnion company.

Details about this offer and instructions on how to activate these services are enclosed with this letter. CyberScout/TransUnion is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://bfs.cyberscout.com/activate> to activate and take advantage of your identity monitoring services.

You have until September 12, 2026 to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about CyberScout/TransUnion and your Identity Monitoring services, you can visit <https://bfs.cyberscout.com/activate>.

What You Can Do.

We encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or unexplained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

We have established a dedicated call center to answer questions about this incident. If you have any questions regarding this incident, please call 1-844-507-4260, 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding major U.S. holidays.

We understand and regret any concern this incident may have caused and appreciate your patience and understanding.

Sincerely,

Oak View Group

Steps You Can Take to Help Protect Personal Information

Fraud Alerts: 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 a free credit report, visit www.annualcreditreport.com or call 1-877-322-8228 toll-free. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

- **Equifax:** https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf
 - Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069
- **Experian:** <https://www.experian.com/help/fraud-alert/>
 - Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013
- **TransUnion:** <https://www.transunion.com/fraud-alerts>
 - TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Credit Freeze: As an alternative to a fraud alert, consumers have the right to place a “credit freeze” at no charge 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft. Should consumers wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

- **Equifax:** <https://www.equifax.com/personal/credit-report-services/credit-freeze>; 1-888-298-0045
 - Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5069
- **Experian:** <https://www.experian.com/freeze/center.html>; 1-888-397-3742
 - Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013
- **TransUnion:** <https://www.transunion.com/credit-freeze>; 1-800-916-8800
 - TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Federal Trade Commission: Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit 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). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact

information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For Iowa residents, you are advised to report any suspected identity theft to law enforcement, including local law enforcement or the Iowa Attorney General. The Iowa Attorney General may be contacted at: 1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5926 or (888) 777-4590; iowaattorneygeneral.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, Baltimore, MD 21202; (410) 528-8662 or (888) 743-0023; oag.maryland.gov. Oak View Group's primary address is 5050 S Syracuse Street, Suite 800, Denver, CO 80327.

For Massachusetts residents, under Massachusetts law, individuals 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.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Act by visiting <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>, or by writing Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. NW, 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; (800) 771-7755; ag.ny.gov.

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

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. The Oregon Attorney General may be contacted at 1162 Court St. NE Salem, OR 97301-4096; (877) 877-9392; doj.state.or.us. For more information on security freezes, you can visit the Oregon Department of Consumer and Commercial Services website at <https://dfr.oregon.gov/financial/protect/pages/place-credit-freeze.aspx>.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, RI 02903; (401) 274-4400; www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately **53** Rhode Island residents that may be impacted by this event.