RCVD JAN 17 2024

LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Erica Lloyd
601.499.8127 (direct)
Erica.Lloyd@lewisbrisbois.com

January 10, 2023

Via First Class Mail:

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Client : Oak View Group
Matter : Data Security Incident

Dear Attorney General:

We are writing on behalf of Oak View Group ("OVG") with respect to a potential data security incident described in more detail below. OVG takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Iowa residents that were potentially affected, what information has been compromised, and the steps that OVG is taking to secure the integrity of its systems. We have also enclosed hereto samples of the notifications made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On or around November 26, 2023, OVG detected that an unauthorized third party had gained access to parts of its network. Upon detecting the incident, OVG immediately began executing its established cybersecurity protocols, including proactively taking certain of our systems offline to contain the issue. OVG also promptly engaged industry leading outside cybersecurity experts to assist with securing the network environment and investigating the extent of unauthorized activity.

On December 14, 2023, OVG completed a comprehensive review of the data potentially impacted in this incident and determined employee information was potentially compromised.

Therefore, out of an abundance of caution, OVG opted to notify all current and former employees from 2019 to present.

2. What Information Was Involved

OVG found no evidence that personal information had been specifically misused; however, it is possible that the following information was potentially compromised: fist name, last name, and Social Security number.

3. Iowa Residents Notified

Two thousand seven hundred sixty (2,760) Iowa residents were potentially affected by this security incident. Notification letters were mailed to the potentially impacted individuals on January 8, 2024, by first class mail. A sample copy of the notification letter is included with this letter.

4. Steps Taken

Although OVG is not aware of any evidence of misuse of personal information, OVG has extended to the potentially impacted individual an offer for free credit monitoring and identity theft protection through Sontiq. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. OVG has changed passwords, strengthened password requirements, and implemented stricter multi-factor authentication requirements.

5. Contact Information

OVG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Erica.Lloyd@LewisBrisbois.com or 601.499.8127.

Very truly yours,

Lewis Brisbois Bisgaard & Smith LLP

Erica J. Lloyd, Esq.

Enclosures: *Sample Notification Letter*

Oak View Group
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

January 8, 2024

Notice of Data Breach

Dear [redacted],

Oak View Group ("OVG") is writing to inform you of an incident that may have exposed your personal information. You are receiving this letter because you are a current or former employee of OVG. We take the security of personal information seriously. As such, this letter contains details about the incident and resources to help protect your personal information going forward, as well as information on how you can obtain free identity monitoring.

0000101025G0500

P

What Happened:

On or around November 26, 2023, OVG detected that an unauthorized third party had gained access to parts of its network. Upon detecting the incident, we immediately began executing our established cybersecurity protocols, including proactively taking certain of our systems offline to contain the issue. We also promptly notified the FBI of this incident and engaged industry leading outside cybersecurity experts to assist with securing the network environment and investigating the extent of unauthorized activity.

What Information Was Involved:

OVG has found no evidence that your information has been misused. However, on December 14, 2023, we completed a comprehensive review of the data potentially impacted in this incident and determined that your personal information that may have been impacted included: first name, last name, date of birth, and Social Security number.

Please note that your banking information, credit card information, and/or financial information were not involved in this incident.

What We Are Doing:

Data security is among OVG's highest priorities. We have contacted law enforcement and made immediate enhancements to our systems and security. We have also engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward.

Additionally, **although we have no indication at this time of any misuse of your information,** we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/ovg** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires 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.

Please keep this letter as you will need to reference the enrollment code above when calling or enrolling online.

In addition, we encourage you to take the following precautions:

- Remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing your accounts for any signs of unauthorized transactions or activity.
- If you detect any suspicious activity on an online or other account, immediately change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained.
- If you ever suspect you are the victim of identity theft or fraud, you can contact your local police.

For More Information:

We encourage you to take full advantage of these services. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Cyberscout representatives are aware of the incident at OVG and can answer questions or concerns you may have regarding protection of your personal information. Please call 1-844-980-1279 Monday through Friday, 8:00 am – 8:00 pm ET, excluding holidays, for assistance or for any additional questions you may have.

OVG values the security of the personal data that we maintain, and we understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Oak View Group

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:

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

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 listed above.

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.

0000102028000 P

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland 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.

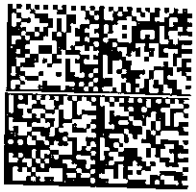
For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or 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 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 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. There are approximately [701] Rhode Island residents that may be impacted by this event.

LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP
1020 Highland Colony Parkway
Suite 310
Ridgeland, Mississippi 39157
Erica J. Lloyd



quadient
FIRST-CLASS MAIL
IMI
$000.87 0
01/11/2024 ZIP 19087
043M31239260

US POSTAGE

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

50319@110 C196