October 10, 2022

Robert Walker
601.499.8083 (direct)
601.499.8077 (main)
Robert.Walker@WilsonElser.com

Via Email:

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
Email: DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov

Re: Cybersecurity Incident GEE Group, Inc.
Wilson Elser File # : 16516. 01765

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents GEE Group, Inc. ("GEE Group") with respect to a recent data privacy incident (hereinafter, the "Incident"). GEE Group takes the security and privacy of the information in its control very 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 Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that GEE Group has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of Incident

On February 2, 2022, GEE Group discovered it was subject to a cyber attack when its domain controller and file server were encrypted. Upon discovery of the incident, GEE Group immediately engaged a specialized third-party cybersecurity firm to assist with securing the environment, and to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. After the forensic investigation concluded, GEE Group reviewed files on the impacted servers to determine the specific individuals and personal information impacted by the Incident.

Although GEE Group is unaware of any fraudulent misuse of information, the following data elements may have been exposed as a result of the unauthorized activity: name, address, date

of birth, and Social Security Number. Out of an abundance of caution, GEE Group is reporting the Incident and notifying potentially affected individuals.

As of this writing, GEE Group has not received any reports of related identity theft since the date of the Incident.

2. Number of New Hampshire residents affected.

A total of seventy (70) New Hampshire residents have been potentially affected by this incident. Notification letters to individuals were mailed to potentially impacted individuals on October 7, 2022, by first class mail. A sample copy of the notification letter is included with this letter under *Exhibit A*.

3. Steps taken in response to the Incident.

GEE Group is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, GEE Group moved quickly to respond to the Incident, ensured the security of its systems moving forward, and notified the potentially affected individuals.

Although GEE Group is not aware of any actual or attempted misuse of the affected personal information, GEE Group offered complimentary credit monitoring and identity theft restoration services through a third party vendor to all potentially affected individuals. Additionally, GEE Group provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

GEE Group 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

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Robert Walker, Esq.
RW/ejl

Exhibit A

GEE Group, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

To Enroll Visit:
https://secure.identityforce.com/benefit/geegroup

Enrollment Code: [redacted]

Via First-Class Mail

October 7, 2022

Notice of Data Incident

Dear [redacted],

We are writing in order to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. At this time, we are unaware of any fraudulent misuse of your personal information. However, we take the privacy of your personal information seriously, and want to provide you with information and resources you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

Recently, GEE Group, Inc. (GEE Group) detected and stopped a network security incident. An unauthorized third-party infiltrated our network and encrypted some of our data. We immediately shut off all access to the network and engaged specialized third-party forensic and technical resources to respond to the incident. GEE Group has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the cause and extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused as a result of the incident, an investigation revealed that the following categories of your information may have been exposed to the unauthorized party during the compromise: name, address, date of birth and social security number. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

As of this writing, GEE Group has not received any reports of related identity theft since the date of the incident.

What We Are Doing:

Data privacy is among GEE Group's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, we moved quickly to initiate our incident response, which included fully securing and remediating our network and the data that we maintain. We conducted an investigation with the assistance of third-party forensic specialists, and have reported this matter to law enforcement. We have reviewed and altered our tools, policies, and procedures relating to the security of our systems and servers

0000101102G0500

P

In light of the incident, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twenty-four (24) 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 you become a victim of identity theft. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by accessing the website at the top of this letter. When prompted please provide the unique code also listed. In order to receive monitoring services, 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.

What You Can Do:

We encourage you to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

We value the safety of your personal information, and are offering complimentary credit monitoring and identity theft protection services through Cyberscout. Cyberscout services include: twenty-four (24) months of credit monitoring and fully managed ID theft recovery services. With this protection, Cyberscout will help you resolve issues if your identity is compromised.

We encourage you to remain vigilant against incidents of identity theft and fraud by enrolling in this free identify theft protection and credit monitoring.

Again, at this time, there is no evidence that your information has been taken or misused. However, 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:

We recognize you may have questions not addressed in this letter. If you have additional questions, please contact Cyberscout at 1-844-548-0298 from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Representatives are available for 90 days from the date of this letter.

GEE Group, Inc. values the privacy and importance of your personal data, and we apologize for any inconvenience or concern that this incident has caused.

Sincerely,

Kim Thorpe, Senior VP, CFO
GEE Group, Inc.
(Enclosure)

Steps You Can Take to Help Protect Your 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.

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

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/

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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:*

You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft

North Carolina Office of the Attorney General - Consumer Protection Division**:** 9001 Mail Service Center, Raleigh, NC 27699**;** 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903**;** 1-401-274-4400**;** www riag.ri.gov