WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

March 9, 2022

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Mail

Attorney General John Formella
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Cybersecurity Incident Involving TOPS Staffing

Dear Attorney General Formella,

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents TOPS Staffing, LLC and its affiliates eStaff Search Group, Inc., AccountStaff, Inc., AllTek Staffing & Resource Group, Inc., and Sterling Office Professionals LLC (collectively, "TOPS Staffing"), a staffing services and employee placement provider, located at 600 Davidson Rd, Pittsburgh, PA 15239 with respect to a recent cybersecurity incident that was first discovered by TOPS Staffing on June 7, 2021 (hereinafter, the "Incident"). TOPS Staffing 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.

A first wave of letters was mailed to the potentially impacted individuals and applicable regulators on November 5, 2021. At that time, TOPS Staffing had no notice of potentially impacted individuals resident of New Hampshire. On January 26, 2022, TOPS Staffing received notification of undelivered mail to 497 individuals. After further investigation, which ended on March 3, 2022, TOPS Staffing obtained updated addresses for the 497 individuals. Of those, one (1) is a resident of New Hampshire. Thus, TOPS Staffing sent an additional wave of notification letters to the 497 individuals on March 9, 2022 and it is now notifying your Office.

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 TOPS Staffing 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.

Please note that the information contained herein is deemed to be confidential, non-public, and privileged. By sharing this information with your Office, TOPS Staffing does not intend to waive any such confidentiality or privilege that may attach. TOPS Staffing respectfully requests that your Office designate and treat this information as confidential and refrain from sharing this information with any third parties. TOPS Staffing trusts the confidential information contained in this response demonstrates that TOPS Staffing has taken prompt and effective action to address this incident.

1. Nature of the Incident

Between June 7, 2021 and June 13, 2021, TOPS Staffing discovered that an unauthorized individual accessed and encrypted its computer environment. Upon detecting the unauthorized access, TOPS Staffing immediately terminated the unauthorized access, and promptly started an investigation to obtain contact information of the potentially affected individuals. TOPS Staffing promptly engaged a team of cyber security professionals to assist with the recovery of its business services, and to conduct a forensic investigation to fully determine the scope and the overall impact of the incident. The investigation was unable to rule out that sensitive personal information from its systems may have been accessed by an unauthorized actor, so TOPS Staffing started an internal investigation to determine what personally identifiable information may have been impacted. The internal investigation concluded on October 5, 2021, and revealed that sensitive information has been potentially impacted by this incident. This investigation was necessary to provide accurate information and notice the potentially impacted individuals.

2. Number of New Hampshire residents affected.

TOPS Staffing identified and has notified 7,118 individuals potentially affected by this Incident. Of those, one (1) was a resident of New Hampshire. Notification letters to these individuals were mailed on November 5, 2021 and March 9, 2022, by first class mail. A sample copy of the March 9, 2022 notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

TOPS Staffing 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, TOPS Staffing moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, TOPS Staffing engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, TOPS Staffing has greatly enhanced its security, including changing passwords and installing additional security on its systems. Lastly, TOPS Staffing informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although TOPS Staffing is not aware of any actual or attempted misuse of the affected personal information as a result of this Incident, TOPS Staffing offered 12 months of complimentary credit monitoring and identity theft restoration services through Kroll to all individuals to help protect their identity. Additionally, TOPS Staffing 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

TOPS Staffing 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 Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Out of an abundance of caution, TOPS Staffing, LLC and its affiliates eStaff Search Group, Inc., AccountStaff, Inc., AllTek Staffing & Resource Group, Inc., and Sterling Office Professionals LLC (collectively, "TOPS Staffing") are writing to inform you of a recent data security incident that may have resulted in an unauthorized access of your sensitive personal information. While TOPS Staffing is unaware of any evidence suggesting that any individual's information was misused as a result of this Incident, TOPS Staffing is providing you with details about the event, steps that TOPS Staffing is taking in response, and resources available to help you protect against the potential misuse of your information. On November 5, 2021, TOPS Staffing mailed a notification letter to you. Recently, TOPS Staffing received notice that the letter originally sent to you was returned due to an invalid address, and may not have reached you. Upon further investigation, TOPS Staffing has obtained an updated address for you, and it is now mailing this notice in case you did not receive the initial notification letter mailed on November 5, 2021.

What Happened?

Between June 7, 2021 and June 13, 2021, TOPS Staffing discovered that an unauthorized individual accessed and encrypted its computer environment. Upon detecting the unauthorized access, TOPS Staffing immediately terminated the unauthorized access, and promptly started an investigation to obtain contact information of the potentially affected individuals. TOPS Staffing promptly engaged a team of cyber security professionals to assist with the recovery of its business services, and to conduct a forensic investigation to fully determine the scope and the overall impact of the incident. The investigation was unable to rule out that sensitive personal information from its systems may have been accessed by an unauthorized actor, so TOPS Staffing started an internal investigation to determine what personally identifiable information may have been impacted. This investigation concluded on March 3, 2022, and revealed that your information has been potentially impacted by this incident. This investigation was necessary to provide accurate information and notice the potentially impacted individuals.

What Information Was Involved?

Based on the investigation, the unauthorized individual may have had access to one or more of the following data elements pertaining to TOPS Staffing employees: names, dates of birth, Social Security numbers, tax ID numbers, driver's licenses/ state-issued identification card numbers, passport numbers, military identification numbers, electronic signatures and financial account numbers. TOPS Staffing provided notice of this incident to you out of an abundance of caution.

What We Are Doing

TOPS Staffing values the privacy of your information and will continue to do everything it can to protect it. Upon detecting this incident, TOPS Staffing promptly engaged an independent firm to conduct an investigation of the incident. Since the incident, TOPS Staffing has greatly enhanced its security, including changing passwords and installing additional security on its systems. Out of an abundance of caution, TOPS Staffing is also providing you with 12 months of complimentary identity monitoring services. While TOPS Staffing is covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information.*

What You Can Do

TOPS Staffing encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity.

Additionally, 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. There, you will also find more information about the credit monitoring and identity theft restoration services that TOPS Staffing is offering to you, and how to activate. Again, TOPS Staffing is making these services available to you at no cost; however, you will need to activate yourself in these services. The deadline to enroll is <<b2b_text_6(activation deadline>>.

At this time, TOPS Staffing is not aware of any evidence suggesting that any individual's information was misused as a result of this Incident. However, TOPS Staffing encourages you to take full advantage of the services offered and to remain vigilant against incidents of identity theft and fraud. Such vigilance includes reviewing account statements and credit reports for suspicious activity.

More Information:

The protection of your information is a top priority, and TOPS Staffing sincerely regrets any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call 1-855-912-1238, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Susan C. Dietrich
For TOPS Staffing, LLC, eStaff Search Group, Inc.,
AccountStaff, Inc., AllTek Staffing & Resource Group, Inc.,
Sterling Office Professionals LLC

Steps You Can Take to Help Protect Your Information

Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 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 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 residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon,* and *West Virginia*: It is required by state laws to inform you that 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.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a 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 residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

***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