



March 5, 2024

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

Via Email:

Attorney General Anthony G. Brown

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

IDTheft@oag.state.md.us

Re: Data Security Incident Involving Consulting Testing Services, Inc. (“CTSI”)

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Consulting Testing Services, Inc. (“CTSI”), an environmental safety consultant located at 237 W 35th St #1004, New York, NY 10001, with respect to a recent data privacy incident that was first discovered by CTSI on November 6, 2023 (hereinafter, the “Incident”). CTSI 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 Maryland residents being notified, and the steps that CTSI 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 the Incident

On November 6, 2023, CTSI detected unusual activity on its network. Upon discovery of this incident, CTSI immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation was completed on January 2, 2024. The forensic investigation found evidence that some of CTSI files were accessed by an unauthorized actor.

On January 11, 2024, CTSI finalized the list of individuals to notify.

Although CTSI is unaware of any fraudulent misuse of information, it is possible that individuals’ full name, date of birth, Social Security Number, Drivers’ License Number or other government-issued form of identification, and email with username and password. It has come to CTSI’s attention that some employees may have been storing their own personal information on company servers against CTSI policy which may include other types of data such as health information.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

As of this writing, CTSI has not received any reports of related identity theft since the date of the incident (November 6, 2023 to present).

2. Number of Maryland residents affected.

CTSI identified 94 individuals potentially affected by this Incident. A total of one (1) Maryland resident may have been potentially affected by this incident. Notification letters to these individuals will be mailed on March 6, 2024, 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.

CTSI 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, CTSI moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, CTSI has taken additional steps to secure its network including isolating the affected areas, blocking malicious traffic, deploying threat detection tools across all critical endpoints, monitoring all network activity, removing all malicious software and the cause of the breach, installing new firewalls, changing all network passwords and security keys, implementing multi-factor authentication, and individualized cyber security training for all employees. Additionally, CTSI engaged a cybersecurity firm to assist with ensuring that individuals were notified as a result of the incident.

Although CTSI is not aware of any actual or attempted misuse of the affected personal information, CTSI is offering 12 months of complimentary credit monitoring and identity theft restoration services through TransUnion to all individuals to help protect their identity. Additionally, CTSI 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

CTSI 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

Consulting and Testing Services, Incorporated
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08440



Via First-Class Mail

<First Name> <Last Name>
<Address>

March 6, 2024

Re: Data Security Incident

Dear <First Name> <Last Name>,

Consulting and Testing Services, Inc. ("CTSI") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive personal information. We are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On November 6, 2023, CTSI detected unusual activity on its network. Upon discovery of this incident, CTSI immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation was completed on January 2, 2024. The forensic investigation found evidence that some of CTSI files were accessed by an unauthorized actor.

On January 11, 2024, CTSI finalized the list of individuals to notify.

What Information Was Involved?

Although CTSI has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, employee information that may have been compromised as a result of the underlying incident may include one or more of the following types of data maintained by CTSI in its normal course of business: Name, date of birth, Social Security Number, Drivers' License Number or other government-issued form of identification, and email with username and password. It has come to CTSI's attention that some employees may have been storing their own personal information on company servers against CTSI policy which may include other types of data such as health information.

What We Are Doing

Data privacy and security is among CTSI'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. Since the discovery of the incident, CTSI moved quickly to investigate, and respond to the incident. Specifically, CTSI has taken additional steps to secure its network including isolating the affected areas, blocking malicious traffic, deploying threat detection tools across all critical endpoints, monitoring all network activity, removing all malicious software and the cause of the breach, installing new firewalls, changing all network passwords and security keys, implementing multi-factor authentication, and individualized cyber security training for all employees. Additionally, CTSI engaged a cybersecurity firm to assist with ensuring that individuals were notified as a result of the incident.

In light of the incident, we are also 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 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. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

What You Can Do

We encourage 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, 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.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is June 5, 2024.

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/ctsinc>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **NQQA889NN9**

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.

For More Information

If you have any questions regarding this incident, representatives are available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and be prepared to supply the fraud specialist with your unique code listed within.

CTSI sincerely regrets any concern or inconvenience this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



Frank Selamie
President
Consulting and Testing Services, Inc.

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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

www.experian.com/fraud/center.html www.transunion.com/fraud-alerts <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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

www.experian.com/freeze/center.html www.transunion.com/credit-freeze <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 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. 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 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
