

May 16, 2022

Ryan M. Cook, Esq.
601.499.8087 (direct)
Ryan.Cook@WilsonElser.com

Via electronic-mail: Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re:	Our Client	:	Strategic Management Solutions LLC
	Matter	:	Data Security Incident
	Wilson Elser File #	:	16516.01812

Dear Attorney General Frosh:

We represent Strategic Management Solutions LLC (“SMSI”), headquartered in Albuquerque, New Mexico, with respect to a potential data security incident described in more detail below. SMSI 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 Maryland residents being notified, what information has been compromised, and the steps that SMSI is taking in response to the incident. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

It appears that on or around March 2, 2022, some items were stolen from an SMSI leased office space. Among the missing items were thumb drives which contained sensitive employee information. The information stored on the thumb drives may have including full name, home address, dates of birth and social security numbers. SMSI was able to identify individuals whose information may have been on the drive on April 5, 2022.

SMSI, however, is not aware of any evidence that information has been misused. SMSI has not received any reports of related identity theft since the date of the incident (March 2, 2022 to present).

2. Number of Maryland Residents Affected

A total of eight (8) residents of Maryland were potentially affected by this security incident. Notification letters to these individuals will be mailed on May 12, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

1400 Meadowbrook Road, Suite 100 • Jackson, MS 39211 • p 601.499.8077 • f 601.499.8078

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

3. Steps Taken

Upon learning of this incident, SMSI moved quickly to institute a response plan, which included conducting an investigation of the incident to determine whose information may have been compromised. SMSI immediately reported this incident to law enforcement. SMSI has reviewed, altered and enhanced its policies and procedures relating to data access management.

4. Contact Information

SMSI 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 Ryan.Cook@WilsonElser.com or 601.499.8087.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in black ink, appearing to read "Ryan Cook", written in a cursive style.

Ryan M. Cook, Esq.

Enclosure: *Sample Notification Letter*



[REDACTED]

May 12, 2022

[REDACTED]

We are writing in order to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive 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, Strategic Management Solutions, LLC (“SMSI”) experienced a theft during which several pieces of hardware were stolen. The full scope of potentially exposed information was determined on April 5, 2022.

Although we have found no evidence that your information has been specifically misused as a result of the theft, an investigation of the incident revealed that the following categories of your information may have been exposed to the unauthorized party as a result: name, mailing address, date of birth, and social security number. We maintained this information for employment record retention requirements, as you are a former SMSI employee, or a family member of a former SMSI employee. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

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

What We Are Doing:

Data privacy is among SMSI’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 an investigation into what data may have been compromised, and securing our information against further thefts. We have reported this matter to law enforcement. We have reviewed and altered our tools, policies, and procedures relating to data access and management.

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

* Services marked with an “*” require 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.

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.

In light of this incident, we are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. If you sign up for our credit monitoring services, we will provide 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, a 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.

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

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

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed above. To extend these services, enrollment in the monitoring services described above is required.

SMSI 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,



David K. O'Flynn
President, Strategic Management Solutions, LLC

* Services marked with an "*" require 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.

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

www.experian.com/fraud/center.html

TransUnion

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

www.transunion.com/fraud-alerts

Equifax

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

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

www.experian.com/freeze/center.html

TransUnion

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

www.transunion.com/credit-freeze

Equifax

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

* Services marked with an "*" require 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.

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

* Services marked with an “*” require 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.