



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

September 13, 2024

Via Email:

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

Re: Preliminary Notice of Cybersecurity Incident

Dear Office of the Attorney General:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents The Maids International, LLC (“TMI”), a residential cleaning services company located at 9394 West Dodge Road, Suite 140, Omaha, NE 68114, with respect to a recent cybersecurity incident that was discovered by TMI on January 22, 2024 (hereinafter, the “incident”). TMI takes the security and privacy of the information within 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 TMI has taken in response to the incident. Sample notification letters, which include an offer of free credit monitoring services, are enclosed hereto.

1. Nature of the Incident

On January 22, 2024, TMI detected unusual activity on its network and discovered that it was the victim of a cybersecurity incident. Upon discovery of this incident, TMI immediately disconnected all access to the network, took non-critical servers offline, and forced password resets across the organization. In addition, TMI promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as conducting a comprehensive forensic investigation to determine the nature and scope of the incident. TMI also proceeded with data mining in an effort to identify a notice population of affected individuals and the personally identifiable information (“PII”) impacted by the incident. On or around April 18, 2024, preliminary data mining results confirmed that PII had been accessed and likely compromised as a result of the incident.

After the data mining process concluded on or around May 24, 2024, TMI began the process of finalizing the notice population of affected individuals, identifying impacted PII data elements for each individual, and collecting sufficient contact information need to mail notification letters. The first wave of notices were mailed to approximately half of the notice population on August 22, 2024. The second and final wave of notices were mailed to individuals on September 12, 2024. Samples of Wave 1 and Wave 2 notification letters are enclosed hereto as **Exhibit A** and **Exhibit B**, respectively.

2. Number of Maryland residents affected.

Based upon the investigation, TMI identified and notified nineteen (19) Maryland residents whose information was impacted as a result of the incident. TMI notified affected individuals by mail on August 22, 2024 and September 12, 2024. Sample notice letters are enclosed.

3. Steps taken in response to the incident.

TMI 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, TMI promptly took steps to contain and remediate its impact by taking appropriate protective and corrective measures to protect the integrity of its systems infrastructure and data. TMI's information technology ("IT") team worked to contain the situation by isolating affected machines and verifying the integrity of backups before bringing systems back online.

In order to prevent similar incidents from occurring in the future, TMI has enhanced a number of security measures and automated protections. Specifically, TMI installed new antivirus and endpoint detection and response tools, implemented 24-hour network monitoring, and validated the use of multi-factor authentication across the organization. TMI has taken steps to mitigate the risk of harm and will continue to do so in the future.

In addition, TMI is offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout, a TransUnion company, to all affected Maryland residents to help protect their identity. Additionally, TMI is providing 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

TMI 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

The Maids International, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

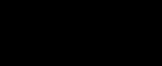


Via First-Class Mail:



August 22, 2024

Re: Cybersecurity Incident Involving The Maids International, LLC

Dear 

The Maids International, LLC (“TMI”) is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. While we are unaware of any fraudulent misuse of your personal information at this time, 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 January 22, 2024, TMI detected unusual activity on its network and discovered that it was the victim of a cybersecurity incident. Upon discovery of this incident, TMI immediately disconnected all access to the network, took non-critical servers offline, and forced password resets across the organization. In addition, TMI promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as conducting a comprehensive forensic investigation to determine the nature and scope of the incident. TMI also proceeded with data mining in an effort to identify a notice population of affected individuals and the personally identifiable information (“PII”) impacted by the incident. On or around April 18, 2024, preliminary data mining results confirmed that PII had been accessed and likely compromised as a result of the incident.

After the data mining process concluded on or around May 24, 2024, TMI used the data mining outputs to finalize a notice population of affected individuals, identify impacted PII data elements for each individual, and collect the contact information required to mail notification letters.

What Information Was Involved?

Although TMI is unaware of any fraudulent misuse of information, it is possible that your full name, date of birth, driver’s license number, passport number, phone number, and private health insurance information were exposed as a result of this incident. Note, impacted data varies based on the individual.

Your social security number was not impacted by this incident.

As of this writing, TMI has not received any reports of related identity theft since the date of the incident (January 22, 2024 to present).

000010103G0400

P

What We Are Doing

TMI 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, TMI promptly took steps to contain and remediate its impact by taking appropriate protective and corrective measures to protect the integrity of its systems infrastructure and data. TMI's information technology ("IT") team worked to contain the situation by isolating affected machines and verifying the integrity of backups before bringing systems back online. In addition, TMI also engaged a specialized cybersecurity firm to conduct a forensic investigation into the nature and scope of the incident and assist in remediation efforts.

In order to prevent similar incidents from occurring in the future, TMI has enhanced a number of security measures and automated protections. Specifically, TMI installed new antivirus and endpoint detection and response tools, implemented 24-hour network monitoring, and validated the use of multi-factor authentication across the organization. TMI has taken steps to mitigate the risk of harm and will continue to do so in the future.

In response to the incident, 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 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, a TransUnion company that specializes in fraud assistance and remediation services. Details on how to enroll in these complimentary services can be found 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.

How do I Enroll for the Free Services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> 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. 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-833-566-7679 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

TMI 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,



Ashley Williams
CFO and General Counsel
The Maids International, LLC



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



000010303000000

P

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

EXHIBIT B

The Maids International, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



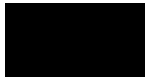
Via First-Class Mail:

PKMJ1H00100676



September 12, 2024

Re: Cybersecurity Incident Involving The Maids International, LLC

Dear ,

The Maids International, LLC (“TMI”) is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. While we are unaware of any fraudulent misuse of your personal information at this time, 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 January 22, 2024, TMI detected unusual activity on its network and discovered that it was the victim of a cybersecurity incident. Upon discovery of this incident, TMI immediately disconnected all access to the network, took non-critical servers offline, and forced password resets across the organization. In addition, TMI promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as conducting a comprehensive forensic investigation to determine the nature and scope of the incident. TMI also proceeded with data mining in an effort to identify a notice population of affected individuals and the personally identifiable information (“PII”) impacted by the incident. On or around April 18, 2024, preliminary data mining results confirmed that PII had been accessed and likely compromised as a result of the incident.

After the data mining process concluded on or around May 24, 2024, TMI used the data mining outputs to finalize a notice population of affected individuals, identify impacted PII data elements for each individual, and collect the contact information required to mail notification letters.

What Information Was Involved?

Although TMI is unaware of any fraudulent misuse of information, it is possible that included your name as well as your Date Of Birth and Social Security Number were exposed as a result of this incident. Note, impacted data varies based on the individual.

As of this writing, TMI has not received any reports of related identity theft since the date of the incident (January 22, 2024 to present).

PKMJ1H0010067600676010290400

What We Are Doing

TMI 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, TMI promptly took steps to contain and remediate its impact by taking appropriate protective and corrective measures to protect the integrity of its systems infrastructure and data. TMI's information technology ("IT") team worked to contain the situation by isolating affected machines and verifying the integrity of backups before bringing systems back online. In addition, TMI also engaged a specialized cybersecurity firm to conduct a forensic investigation into the nature and scope of the incident and assist in remediation efforts.

In order to prevent similar incidents from occurring in the future, TMI has enhanced a number of security measures and automated protections. Specifically, TMI installed new antivirus and endpoint detection and response tools, implemented 24-hour network monitoring, and validated the use of multi-factor authentication across the organization. TMI has taken steps to mitigate the risk of harm and will continue to do so in the future.

In response to the incident, 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 twenty-four 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, a TransUnion company that specializes in fraud assistance and remediation services. Details on how to enroll in these complimentary services can be found 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.

How do I Enroll for the Free Services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> 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. 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call 1-833-566-7679 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

TMI 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,

A handwritten signature in black ink, appearing to read "Ashley Williams", with a stylized flourish at the end.

Ashley Williams
CFO and General Counsel
The Maids International, LLC



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.