



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

September 16, 2021

Michael J. Waters

312-463-6212

312-819-1910

mwaters@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)

The Honorable John Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Data Security Incident

Dear Attorney General Formella:

Please allow this to follow up my December 23, 2020 letter regarding a data incident that occurred at Metabolic Maintenance Products, Inc. (“Metabolic”), 601 N. Larch Street, Sisters, OR 97759. This letter is being submitted to you pursuant to N.H. REV. STAT. ANN. § 359-C:20.

NATURE OF THE INCIDENT

As discussed in my prior letter, in September, 2020, Metabolic was notified that an unauthorized third party may have acquired payment card information transmitted through Metabolic’s website. On December 22, 2020, Metabolic notified all customers who conducted credit card transactions on Metabolic’s website between October 1, 2019 and August 20, 2020, including fifty-six (56) New Hampshire residents.

Following the discovery of the incident, Metabolic undertook a number of steps, in conjunction with its third-party website provider, to confirm the security of its website and reduce the risk of a similar incident. Metabolic and its website vendor continued to encrypt and mask credit card data, ran a PCI scanner, and installed a third-party service that scans the website every 30 minutes and identifies any changes made to the site. Metabolic’s vendor removed a file that contained certain unencrypted credit card data and removed certain WordPress functions as a precaution. Metabolic removed several files from its website identified by a forensic security firm as being suspicious, limited access to the WebMin configuration tool based on IP Address, and it changed all of the user passwords to complex 12-digit passwords. Metabolic’s website vendor confirmed that it did

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California

79887579.1



The Honorable John Formella
Office of the Attorney General
September 16, 2021
Page 2

not see any further suspicious activity and configured the website such that once it publishes a file to the server it is encrypted and cannot be decoded.

Unfortunately, despite these efforts, Metabolic has discovered that malicious code remained on its website until July 9, 2021. On June 23, 2021 and June 24, 2021, Metabolic received notice from its merchant services provider requesting that Metabolic investigate whether payment card data collected through Metabolic's website between February 4, 2021 and April 27, 2021 may have been subject to unauthorized access. Metabolic engaged a forensic security firm to conduct a further forensic investigation and review of Metabolic's website. The investigation ultimately determined that an unknown, unauthorized third party installed code on the Metabolic website that transmitted transaction data to the third party. The sophisticated code was designed to evade detection and required specialized analysis to identify and remove it. The code captured and transmitted transaction information, including names, addresses, transaction details, and payment card information, for transactions processed through the Metabolic Maintenance Products and the MethylPro websites from approximately May, 2020 until July 9, 2021.

Metabolic is notifying all customers who conducted credit card transactions on Metabolic's website from the end of the last notification window on August 20, 2020 until the forensic security firm confirmed removal of the malicious code on July 9, 2021.

NOTIFICATION TO THE NEW HAMPSHIRE RESIDENTS

On or about August 20, 2021, Metabolic determined that sixty-seven (67) New Hampshire residents conducted credit card transactions on Metabolic's website between August 20, 2020 and July 9, 2021. A number of these individuals may have been previously notified by Metabolic on December 22, 2020. Metabolic notified the residents of the situation by letter on September 16, 2021. Metabolic has established a confidential telephone inquiry line to assist the individuals with any questions they may have regarding the incident. Attached is a sample of the notification letter that is being sent to the affected New Hampshire residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon receiving the notice from its merchant services provider, Metabolic promptly commenced an investigation and engaged a forensic security firm to confirm the security of its systems and website. Upon identifying the unauthorized code, the forensic security firm removed the code from Metabolic's website and Metabolic began identifying potentially affected customers. Metabolic is nearing completion of a new, state-of-the-art website to ensure that its customers' data is secure. Metabolic has also taken significant steps to secure its existing website, including implementing an updated firewall configuration, increased logging, and traffic detection. Metabolic has notified



The Honorable John Formella
Office of the Attorney General
September 16, 2021
Page 3

the credit card brands and law enforcement regarding the incident. Finally, as discussed above, Metabolic is notifying potentially affected individuals and providing them with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in black ink, appearing to read "Michael J. Waters".

Michael J. Waters

Enclosure



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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

RE: NOTICE OF DATA BREACH

Metabolic Maintenance Products, Inc. (“Metabolic”) values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information.

What Happened? We were recently notified that an unknown third party may have gained unauthorized access to names and payment card numbers processed through our website. Upon discovering the potential incident, we engaged a forensic security firm to conduct an in-depth investigation of the incident to confirm the security of our website and systems. The investigation ultimately determined that an unknown, unauthorized third party installed code on our website that transmitted transaction data to the third party. The sophisticated code was designed to evade detection and required specialized analysis to identify and remove it. The code captured and transmitted transaction information for transactions processed through the Metabolic Maintenance Products and the MethylPro websites from approximately May 2020 until July 9, 2021.

What Information Was Involved? After discovering and removing the code, we compiled a list of all transactions that took place during the relevant timeframe. On August 20, 2021, we determined that your name, address, transaction details, and payment card information for your payment card(s) ending in <<b2b_text_1(LastFourDigits)>> may have been acquired by the third party as a result of the incident.

What We Are Doing. Upon learning of the incident, we promptly commenced an investigation and hired a leading forensic security firm to confirm the security of our systems and website. Upon identifying the unauthorized code, we removed the code from our website and we began identifying potentially affected customers. We are nearing completion of a new, state-of-the-art website to ensure that our customers’ data is secure. We have also taken significant steps to secure our existing website, including an updated firewall configuration, increased logging, and traffic detection. We have notified the credit card brands and law enforcement regarding the incident.

What You Can Do. If you detect any suspicious activity on your credit card, you should promptly notify your financial institution or credit card company. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. For further information and assistance, please call 1-855-551-1490 from 6:00 A.M. – 3:30 P.M. PST, Monday through Friday, excluding major U.S. holidays.

We value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause.

Sincerely,

Dan Young

General Manager
Metabolic Maintenance

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected 55 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any 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.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.