PERKINSCOIE

700 13th Street, NW
Suite 800
Washington, D.C. 20005-3960

T +1.202.654.6200
F +1.202.654.6211
PerkinsCoie.com

November 30, 2023

David C. Aaron
DAaron@perkinscoie.com
D. +1.202.654.1723
F. +1.202.624.9520

BY EMAIL: IDTHEFT@OAG.STATE.MD.US
Hon. Anthony G. Brown
Attorney General
State of Maryland

Re: Notification of Data Security Breach - MD² International

Dear Attorney General Brown,

This letter contains supplemental detail regarding a data security breach we are reporting today. In addition to the information in the notification letter we will send to affected consumers, MD² International, LLC (MD² International) provides the following information. MD² International does not waive, and expressly reserves, all applicable privileges and other legal protections, including protection from disclosure to third parties, that may apply to the contents of this letter.

The incident related to a Microsoft 365 account of an employee of Grateful Doctors Medical of New York, PLLC, doing business as MD² Madison Avenue, a medical practice in New York, New York that is part of the MD² network of internal medicine practices. MD² International supports a network of concierge medical practices that are each owned by the practice physicians. MD² International is making this report to your office on behalf of MD² Madison Avenue. The incident affected approximately two (2) Maryland residents.

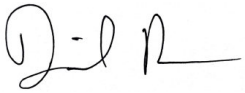
The intrusion into the MD² Madison Avenue employee account was initially learned of on or about July 17, 2023. Investigation determined that the account was accessed by an unauthorized actor or actors between May 23, 2023 and June 13, 2023. We are unable to determine whether any specific information of Maryland residents was accessed or obtained.

MD² International decided in abundance of caution to notify all individuals whose personal information was present in the MD² Madison Avenue employee account. MD² International initiated a process to identify all such individuals. MD² International received preliminary results of that process on October 31, 2023, but required additional time to assess the nature and scope of the breach. We began the process of providing required notice once that data analysis process was completed. The attached template letter was used for Maryland residents. MD² International has taken steps such as enhancing authentication protocols to protect its email systems from further compromise.

Please note that MD^2 International and MD^2 Madison Avenue are not Covered Entities or Business Associates under the Health Insurance Portability and Accountability Act (HIPAA).

If you have any questions, please contact me.

Sincerely,



David C. Aaron

Return to IDX:
[redacted]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

MD²

Enrollment Code: <<XXXXXXXX>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

[redacted]

November 30, 2023

<<Header>>

Dear <<First Name>> <<Last Name>>:

We are honored that you have chosen an MD² practice for your health care. As your trusted partner, MD² takes the privacy and security of patients' information seriously. Unfortunately, we recently became aware of a data security incident, which may have affected the security of some of your information.

You are receiving this notice because of the possibility that your information was accessed during the incident. We know that this causes concern. We cannot confirm that any information of yours was accessed or taken, but are notifying you out of an abundance of caution. Below we have provided notice about the event, our response, and additional measures you can take to help protect your information.

What Happened? We detected unauthorized access to the Microsoft 365 account of a non-physician employee in the MD² Madison Avenue practice. That access terminated before it was detected. We initiated an investigation into the nature and scope of the incident. The investigation determined that the unauthorized access to that Microsoft 365 account occurred between approximately May 23, 2023 and June 13, 2023, and information within the account could have been viewed or downloaded within that time. Because we were not able to determine whether specific items were viewed or downloaded, we are notifying you out of an abundance of caution.

The Microsoft 365 system is not the same as our electronic medical records (EMR) system or our billing system. We have no evidence that the EMR system or the billing system were accessed.

What Information Was Involved? <<Lead in>> determined that email messages and files in the affected Microsoft 365 account included the following types of your information: <<Potential PI Fields>>.

We cannot confirm whether any of this information was accessed, viewed, or taken, but it was present within email messages and files in the staff member's account.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this incident, we took steps to prevent the unauthorized access from occurring again. We have investigated the potential scope of the incident, are assessing the security of our systems more broadly, and are issuing notifications to potentially affected individuals. We are also reviewing and enhancing our information security and have already implemented new security measures to help avoid future incidents.

In addition, we are offering <<12/24>> months of identity theft protection services through IDX and have included materials and a list of steps recommended by IDX to further protect your information. Please use the IDX link and Enrollment Code provided above and note the deadline to enroll in the identity theft protection services is February 28, 2024.

What You Can Do. In addition to enrolling in the services described above, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity.

For More Information. If you have additional questions, please contact me or your MD^2 doctor. To contact me, please call me at [redacted] or send an email to [redacted] And, if you have questions about the IDX identity theft protection service, please contact IDX using the information above or on the attached document.

We sincerely regret that this incident occurred. MD^2 remains committed to providing our patients with access to unparalleled health care, protecting their information, and advocating for their health and well-being.

Sincerely,

_____

Sean Kell
Chief Executive Officer
MD^2 International, LLC

IDX
A ZEROFOX COMPANY

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at 1-800-939-4170 Monday through Friday 6 am to 6 pm Pacific Time to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free (1-877-322-8228), or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies, including:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without

your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

If you are a California Resident, you may visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

If you are a Connecticut resident, you may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, calling 410-576-6491, or writing to Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a New York resident, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, www.doj.state.or.us, Telephone: 877-877-9392, and to the FTC.

If you are a Washington, D.C. resident, you may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001; Telephone: 202-727-3400; oag@dc.gov.