MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 10, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent PracticeMax located at 1440 East Missouri Avenue, Suite C-200, Phoenix, AZ 85014, and are writing to supplement our March 4, 2022, notice to your Office. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PracticeMax does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

PracticeMax continues to coordinate with its customers, review its records, and undertake address locator efforts for purposes of providing notification to potentially affected individuals. On or about June 10, 2022, PracticeMax will continue mailing written notice to individuals on its own behalf, including notice to forty-six (46) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. While the information is not the same for each entity and individual involved, the potentially impacted personal information as defined by N.H. Rev. Stat. Ann. § 359-C:19 includes name and Social Security number.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M. Schafle of
MULLEN COUGHLIN LLC

PracticeMax
Smart Solutions. Maximum Results.

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

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

<<b2b_text_1(NOTICE OF DATA INCIDENT / NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

PracticeMax is a business management and information technology solutions company. We provide services including billing, consulting, registration, and other solutions to companies, including hospitals, insurance companies, employers, and physician offices, and as a result we are in possession of some information related to you. This letter contains information about a data incident at PracticeMax. The letter also provides information about our response and resources available to help protect information, should you feel it is appropriate to do so.

What Happened? On May 1, 2021, PracticeMax became aware of technical issues relating to systems in the PracticeMax network. We promptly commenced an investigation and identified ransomware on certain systems. We disconnected our systems and partnered with subject matter specialists to assist with our investigation and to confirm the security of our network. We began restoring the network and business operations, and we implemented additional security policies and controls. We also communicated the incident to our customers.

The investigation determined the PracticeMax network was subject to unauthorized access beginning on April 17, 2021 until May 5, 2021 and during that time one server was accessed and certain files may have been removed. The investigation also identified unauthorized access to a limited number of company email accounts. We reviewed the server and email accounts for sensitive information and determined these systems may have contained sensitive information at the time of the incident. Although the investigation did not identify evidence confirming any unauthorized access, acquisition, or disclosure of sensitive information, we cannot rule out the possibility of such activity. Additionally, some of the data stored in our network was encrypted as a result of the ransomware.

What Information Was Involved? In general, we collect demographic and health information, including but not limited to name, address, Social Security number, date of birth, treatment and/or diagnosis information, health insurance information and, in some cases, financial information for individuals associated with our customers. The information varies depending on what was provided to PracticeMax, however, it is possible these types of information may have been present on the involved systems at the time of the incident. Importantly, our investigation did not identify evidence of unauthorized access, acquisition, or disclosure of your information, however, the review of the involved systems identified information including your <<b2b_text_2(name, data elements)>><<b2b_text_3(data elements cont.)>>.

What We Are Doing. PracticeMax is committed to safeguarding information and has strict security measures in place to protect information in our care. Upon learning of this incident, we moved quickly to investigate and respond and to confirm the security of our systems. As part of PracticeMax's ongoing commitment to the privacy of information in our care, we reviewed our existing policies and procedures and implemented additional safeguards to further our already stringent security policies and procedures and to secure the information in our systems. We also notified law enforcement, our customers, and relevant regulators of this incident.

Steps You Can Take to Help Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a general practice, we encourage individuals to frequently reset online account passwords, to use complex password combinations, and to not share passwords or use identical passwords for multiple online accounts. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.