



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED
MAR 07 2022
CONSUMER PROTECTION

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

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

March 4, 2022

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent PracticeMax located at 1440 East Missouri Avenue, Suite C-200, Phoenix, AZ 85014, and are writing to notify your office of an incident that may affect the security of some personal information relating to five (5) New Hampshire residents. The investigation into this matter is ongoing, and 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.

Nature of the Data Event

PracticeMax is a business management and information technology solutions company that provides billing, consulting, and registration services to insurance companies, employers, and physician offices. On May 1, 2021, PracticeMax became aware of technical issues relating to systems in the PracticeMax network. An investigation was promptly commenced, and through that investigation ransomware was identified on certain systems. PracticeMax disconnected its systems and began taking steps to assess the security of its network. PracticeMax also communicated the incident to its 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. Although the investigation did not identify evidence confirming any unauthorized access, acquisition, or disclosure of sensitive information, PracticeMax cannot rule out the possibility of such activity. Additionally, some of the data stored in the network was encrypted as a result of the ransomware. Therefore, PracticeMax reviewed the server and email accounts for sensitive information.

On October 19, 2021, while review of the server continued, PracticeMax began notifying potentially affected individuals on behalf of certain PracticeMax customers. Other notifications include notice to the

Mullen.law

Federal Bureau of Investigation and to the media. PracticeMax also notified the U.S. Department of Health and Human Services.

On or around February 2, 2022, PracticeMax completed the review of the involved server and on February 14, 2022, began updating its customers. 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.

Notice to New Hampshire Residents

As noted above, PracticeMax began notifying potentially affected individuals on or about October 19, 2021. On February 11, 2022, PracticeMax continued with its notification efforts by posting notice of the incident on its website. A copy of the website notice is attached here as *Exhibit A*. On February 18, 2022, PracticeMax issued a national press release and a copy of that notice is attached hereto as *Exhibit B*. On or about March 4, 2022, PracticeMax will continued notifying individuals by mailing written notice to individuals including five (5) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit C*.

Other Steps Taken and To Be Taken

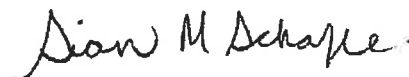
Upon discovering the event, PracticeMax moved quickly to investigate and respond to the incident, assess the security of PracticeMax systems, and identify potentially affected individuals and customers. As previously noted, PracticeMax notified the Federal Bureau of Investigation and has been cooperating with the investigation. PracticeMax continues to assess the security of its systems and to enhance existing policies and procedures, including implementing additional technical and administrative safeguards.

PracticeMax is providing impacted individuals with guidance on how to protect against identity theft and fraud. PracticeMax is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. PracticeMax will provide written notice and supplemental notice to relevant regulators, including the U.S. Department of Health and Human Services.

Contact Information

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

EXHIBIT A

Notice of Data Incident

PracticeMax is notifying individuals of a data incident. To date, we have no evidence of actual or attempted misuse of information as a result of this incident. This notice provides details about the incident, our response, and resources available to help protect information.

Who is PracticeMax? PracticeMax is a business management and information technology solutions company. We provide services including billing, consulting, registration, and other solutions to companies across the United States, including hospitals, insurance companies, employers, and physician offices.

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. PracticeMax reviewed the server and email accounts for sensitive information.

Our investigation revealed some personal information may have been accessed by an unauthorized individual as a result of this incident. On October 19, 2021, while review of the server continued, we began notifying potentially affected individuals on behalf of certain PracticeMax customers. We also notified the FBI, the media, and relevant state and federal regulators.

We recently completed the review for sensitive information and determined the server may have contained some 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, and financial information for individuals associated with our customers. The review of the involved server and email accounts determined that these types of information may have been present in the involved systems at the time of the incident in addition to patient account number, employer and employee identification number, passport number, driver's license/state identification number, prescription information, and in very limited circumstances provider or employee username and password or PIN. The information involved varied by individual.

What We Are Doing? PracticeMax is committed to safeguarding information in its care 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. We have been in communication with our customers throughout the course of the investigation and have notified them of our efforts to date. We remain available to coordinate with our customers and to respond to any further questions they have. 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. As noted above, we notified the FBI and relevant regulators, including the U.S. Department of Health and Human Services. We also notified the media in October of 2021 and will issue an updated media notice now that our investigation has concluded.

What You Can Do. We do not have any evidence of misuse of personal information at this time. However, we encourage individuals to remain vigilant by reviewing documents for suspicious activity, including health insurance statements, explanation of benefits of letters, medical records, account statements and credit reports. If you find unfamiliar activity on statements you receive from your health insurance company, you should immediately notify your health insurance company immediately. Additionally, any suspicious activity on your credit report should be reported immediately to law enforcement.

For More Information

Patients with questions may contact PracticeMax's dedicated call center at 1-855-568-2073 (toll free), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. You can also contact PracticeMax at incidentresponse@practicemax.com.

STEPS YOU CAN TAKE TO 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 security 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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. PracticeMax is located at 1440 East Missouri Avenue, Suite C-200, Phoenix, AZ 85014.

For New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <http://www.riag.ri.gov/>; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

EXHIBIT B

Notice of Data Incident

Phoenix, Arizona, February 18, 2022: PracticeMax is notifying individuals of a data incident. To date, we have no evidence of actual or attempted misuse of information as a result of this incident. This notice provides details about the incident, PracticeMax's response, and resources available to help protect information.

Who is PracticeMax? PracticeMax is a business management and information technology solutions company. It provides services including billing, consulting, registration, and other solutions to companies across the United States, including hospitals, insurance companies, employers, and physician offices.

What Happened? On May 1, 2021, PracticeMax became aware of technical issues relating to systems in the PracticeMax network. It promptly commenced an investigation and identified ransomware on certain systems. It disconnected its systems and partnered with subject matter specialists to assist with the investigation and to confirm the security of its network. PracticeMax began restoring the network and business operations, and it implemented additional security policies and controls. It also communicated the incident to its 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. PracticeMax reviewed the server and email accounts for sensitive information and determined that some personal information may have been accessed by an unauthorized individual as a result of this incident. Additionally, some of the data stored in the network was encrypted as a result of the ransomware.

What Information Was Involved? In general, PracticeMax collects 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, and financial information for individuals associated with its customers. The review of the involved server and email accounts determined that these types of information may have been present in the involved systems at the time of the incident in addition to patient account number, employer and employee identification number, passport number, driver's license/state identification number, prescription information, and in very limited circumstances provider or employee username and password or PIN. The information involved varied by individual.

What is PracticeMax Doing? PracticeMax is committed to safeguarding information in its care and has strict security measures in place to protect information in its care. Upon learning of this incident, it moved quickly to investigate and respond and to confirm the security of its systems. PracticeMax notified the FBI, the media, its customers, and relevant state and federal regulators. While the investigation was ongoing, PracticeMax also began notifying potentially impacted individuals. As part of its ongoing commitment to the privacy of information in its care, PracticeMax also reviewed its existing policies and procedures and implemented additional safeguards to further its already stringent security policies and procedures and to secure the information in its systems.

What You Can Do. PracticeMax does not have any evidence of misuse of personal information at this time. However, in general PracticeMax encourages individuals to remain vigilant by reviewing documents for suspicious activity, including health insurance statements, explanation of benefits forms, account statements and credit reports and to report unfamiliar activity to relevant entities immediately. Individuals may also consider the resource information below.

For More Information. Individuals with questions may contact PracticeMax's dedicated call center at 1-855-568-2073 (toll free), Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Additional information may also be found at <https://www.practicemax.com/notice-of-data-incident/>.

Monitor 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 security 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, PracticeMax encourages 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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. PracticeMax is located at 1440 East Missouri Avenue, Suite C-200, Phoenix, AZ 85014.

For New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <http://www.riag.ri.gov/>; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

EXHIBIT C



<<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.

What You Can Do. We encourage you to remain vigilant by reviewing documents for suspicious activity, including health insurance statements, explanation of benefits of letters, medical records, account statements and credit reports. If you find unfamiliar activity on statements you receive from your health insurance company, you should immediately notify your health insurance company. Additionally, any suspicious activity on your credit report should be reported immediately to law enforcement. You can also review the enclosed *Steps You Can Take To Help Protect Personal Information* for more information.

If you have additional questions, please call our dedicated assistance line at (855) 568-2073 (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. holidays).

Sincerely,

Michael Johnson
CEO
PracticeMax

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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-576-6300 or 1-888-743-0023; and www.oag.state.md.us. PracticeMax is located at 1440 East Missouri Avenue, Suite C-200, Phoenix, AZ 85014.

For New Mexico residents, 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 bureaus 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 violator. 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 by visiting 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.