

<<Date>>

<<FirstName>> <<LastName>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Re: Notification of Data Security Incident

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a data security incident experienced by PracticeLink, Ltd. ("PracticeLink") that may have affected your personal information. As explained below, we recently learned that an unauthorized individual gained access to two PracticeLink employee email accounts, at least one of which contained your personal information. We are writing to notify you of this incident and to inform you about steps that can be taken to help protect your information.

What Happened? On September 17, 2020, we detected unusual activity relating to one PracticeLink employee's email account. Upon discovering this activity, we immediately took steps to secure our email system and launched an investigation. In connection therewith, we engaged a leading, independent forensics firm to determine what happened and whether sensitive information was accessed or acquired without authorization as a result. As a result of this investigation, we learned that two PracticeLink employee email accounts were accessed without authorization. We then took steps to identify the personal information contained within the accounts and, on or about January 26, 2021, confirmed that at least one of the accounts contained some of your personal information which may have been accessed or acquired by an unauthorized individual. We then worked diligently to identify current address information required to provide notification of this incident.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems. In addition, PracticeLink is not aware of the misuse of any potentially affected information.

What Information Was Involved? The following information may have been contained within the email account: your <<Variable Text>>.


What We Are Doing. As soon as we discovered this incident, we took the steps referenced above. We also applied enhanced security measures to our email system in order to help prevent a similar incident from occurring in the future. In addition, we reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrator(s) of this incident accountable.

What You Can Do. You can follow the recommendations included with this letter for steps you can take to protect your personal information.

For More Information. If you have questions about this letter, please contact us at 1-800-776-8383 x4427 Monday through Friday from 8:00 am – 3:00 pm EST excluding major US holidays. You may also consult the resources included on the following page which provides information about steps you can take to protect your personal information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Bruce Reed, CFO
PracticeLink, Ltd.

Steps You Can Take to Further Protect Your Information

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 www.annualcreditreport.com/, calling toll-free 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 this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.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 90 days. 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 www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. 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. There is no charge to place, lift or remove the security freeze. 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 respective state Attorney General about 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission

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

**Maryland Attorney
General**

200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

**Rhode Island
Attorney General**

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.