

1/2

NEW YORK STATE SECURITY BREACH REPORTING FORM
Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa; State Technology Law §208)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
University Dental Associates, L.L.P.
Street Address: Maimonides Medical Center/Division of Dentistry 4802 Tenth Avenue
City: Brooklyn State: New York Zip Code: 11020

Submitted by: Alvin D. Fried, D.D.S. Title: Partner Dated: 12/23/12
Firm Name (if other than entity):
Telephone: 718-283-7428 Email: afried@mairmonidesmed.org
Relationship to Entity whose information was compromised: Partner

Type of Organization (please select one): [] Governmental Entity in New York State; [] Other Governmental Entity;
[] Educational; [X] Health Care; [] Financial Services; [] Other Commercial; [] Not-for-profit

Number of Persons Affected:
Total (Including NYS residents): 2400 NYS Residents: 2400
If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [] Yes; [] No.

Dates: Breach Occurred: 11/21/12 Breach Discovered: 11/21/12 Consumer Notification: 12/20/12

Description of Breach (please select all that apply):
[X] Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[] Internal system breach; [] Insider wrongdoing; [] External system breach (e.g., hacking); [] Inadvertent disclosure;
[] Other (specify):

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[X] Social Security Number
[] Driver's license number or non-driver identification card number
[] Financial account number or credit or debit card number, in combination with the security code, access code,
password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO
AFFECTED NYS RESIDENTS:
[X] Written; [] Electronic; [] Telephone; [] Substitute notice.
List dates of any previous (within 12 months) breach notifications: N/A

Identify Theft Protection Service Offered: [] Yes; [X] No.
Duration: Provider:
Brief Description of Service:

University Dental Associates, L.L.P.
Maimonides Medical Center
Division of Dentistry
4802 Tenth Avenue
Brooklyn, New York 11219

December 11, 2012

Dear University Dental Associates, L.L.P. patients:

We are writing to inform you that a laptop on which we stored billing information was stolen from our office on November 21, 2012. While the computer was password protected, your name, social security number, address, date of birth, and billing codes related to services you have received at our office were stored on the computer.

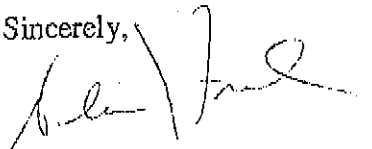
At this time, we have no evidence that your personal information has been or will be accessed or misused. Nonetheless, we want to alert you to the incident and make you aware of some precautions you can take to protect yourself against the possibility of becoming a victim of identity theft. Please see the enclosures to learn more about these precautions. We strongly encourage you to actively monitor your financial accounts and the free credit reports that are available to you. You should report any suspected identity theft to us and to appropriate law enforcement officials.

Please be assured that we reported the theft of the computer to the New York City Police Department on November 26, 2012. We are also providing notice of this incident to other appropriate government agencies and to the three major credit bureaus, and taking steps to prevent any similar incidents in the future.

If you have any questions about this incident please contact our office at (718) 283-7428 or email us at afried@maimonidesmed.org.

We deeply regret any difficulties that this may cause you, and hope the information we are providing will be helpful.

Sincerely,



Alvin D. Fried, D.D.S.
Julius R. Berger, D.D.S.
University Dental Associates, L.L.P.

IMPORTANT STEPS TO HELP PREVENT FRAUD

1. **Carefully review your banking, credit card and other account statements and report any unauthorized transactions.** You should regularly review your accounts to look for unauthorized or suspicious activity. You may also want to notify your financial institution(s) and credit card companies that you received this notice. This will tell them that your information may have been viewed or accessed by an unauthorized party. You may want to request a new debit or credit card from these institutions if one has not already been issued to you.
2. **Contact the fraud department at the three major credit bureaus listed below and ask them to place a "fraud alert" on your credit file.** A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. To place a fraud alert on your credit file, contact one of the three national credit bureaus at the numbers provided below.

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241

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

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834-6790

3. **Obtain a copy of your credit report from each of the three major credit reporting agencies and review them to be sure they are accurate and include only authorized accounts.** You are entitled to one free copy of your report every 12 months. To order your report, visit www.annualcreditreport.com, or call toll-free (877) 322-8228, or complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the request form at <http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtml>). Carefully review your credit reports to verify that your name, address, account, and any other information are accurate and notify the credit reporting agencies of any errors you detect, and about any accounts you did not open or inquiries from creditors you did not initiate. In addition to your free credit report, you can also purchase a copy of your credit report by contacting one of the three national credit reporting companies listed above.
4. **Contact the Federal Trade Commission ("FTC") to obtain additional information about how to protect against identity theft.** The FTC is a good resource for general questions about identity theft. You can call the FTC's identity theft hotline at 1-877-IDTHEFT (438-4338), or visit their website at www.ftc.gov/bcp/edu/microsites/idtheft/.
5. **You may also put a "credit 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 a freeze. Please note that placing a credit freeze may delay your applications for credit, mortgage, employment, housing, insurance, utilities or even cellular telephone service.** Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit bureaus using the information provided below to find out more.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

6. **We recommend that you remain vigilant over the next 12 to 24 months and report any suspected identity theft or other misuse of personal information immediately to the proper law enforcement authorities.** You have the right to obtain a police report if you are the victim of identity theft.