Steven Yang, DDS
6670 Reseda Blvd., Suite 106
Reseda, CA 91335

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Notice of Data Breach

Dear <<Name1>>:

Protecting the security and confidentiality of patient information is of the utmost importance. Regrettably, we are writing to inform you about an incident involving some of that information.

What Happened
On the morning of January 6, 2018, our dental office was burglarized and two laptops were stolen. Once discovered, the matter was immediately reported to the Los Angeles Police Department and an internal investigation was started to determine what, if any, health information may have been stored on those devices.

What Information Was Involved
Our investigation has determined that files contained on those devices may have included your name, address, social security number, health insurance number and other information regarding your dental care. We have been working with law enforcement but, to date, they have been unable to locate the stolen devices.

What You Can Do
We have no evidence that the information on the laptop has been misused or even accessed; however, as a precaution, we wanted to notify you regarding this incident and assure you that we take it very seriously. We also recommend that you regularly review the explanation of benefits (EOB) statements that you receive from your health insurer. If you identify services listed on your EOB statements that you did not receive, you should contact the insurance company immediately.

What We Are Doing
Maintaining information security is part of our commitment to providing high quality and safe dental care and we deeply regret any concern or inconvenience that this may have caused you. To help ensure that a similar issue does not happen in the future, we are re-enforcing education regarding safeguarding patient information. We have also implemented enhancements to our existing technical safeguards and initiated a review of our systems to further protect patient information.

For More Information
If you have any questions, please call 1-818-881-2731, Monday through Thursday between 10:00 a.m. and 4:00 p.m. Pacific Time.

Sincerely,
Steven Yang, D.D.S.

Additional Steps You Can Take

We recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity.

We also recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or charge your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit www.annualcreditreport.com or call toll free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

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

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

If you believe that you are the victim of identity theft or have reason to believe that your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.