An EXTREMELY IMPORTANT letter to the patients of Dr. John Gonzalez:

On the late afternoon of Monday July 25, 2016, my car window was broken out and my briefcase was stolen. In that briefcase was an external hard drive containing two different types of data. First, all office patient records were backed up on the drive, including social security numbers, driver's license numbers, phone numbers, date of birth, physical and email addresses and health insurance information. NO passwords or user names appear in these records. No complete credit card information or bank account information was stored on this drive (only the last four digits of the most recent card used is stored). As a result, your personal information is now potentially accessible to unauthorized individuals. However, the risk of accessibility is extremely low because the data in its format is unreadable. In consulting with my dental soft-ware experts, they assure me it would be incredibly difficult and unlikely for anyone to access your records. However, since the data is not encrypted, I am required by law to notify you. Secondly, pictures of patient cases (teeth only, no faces) that included patient first and last names and phone numbers were saved on the drive. These files of pictures are stored in jpeg format and can be opened easily.

Immediately upon discovery of the theft, I contacted local authorities and reported the theft and filed a police report. You may contact Detective Harris (badge #40215) at 310-444-1580 and reference case number 1608-13548 if you have any questions.

At this point, in order to protect yourself from the risks associated with this breach, you may want to take the following steps:

* Medical records and health insurance information: Regularly review the explanation of benefits statement that you receive from your insurance administrator. If you see any services listed that you did not receive, contact your administrator immediately at the number on your statement. You should also check your credit reports for medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the number on the report.

* Social Security number: Place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. The alert will remain on your accounts for 90 days. You can request a fraud alert through any one of the three credit reporting agencies: Experian 888.397.3742; Equifax 800.525.6285; Trans Union 800.680.7289. You can also request copies of your credit report from any of these agencies, which you should check for suspicious activity. If you find anything, contact local authorities and file a report of identity theft. Ask for a copy of the police report, as you may need to supply this to your creditors. You may also consider placing a credit freeze through these agencies which means no new accounts may be opened without first lifting the freeze.

I am truly sorry to have inconvenienced you, my patients, with this unfortunate event. This theft did not happen in the office. The thief did not break into a medical facility, but rather a car parked in a commercial structure and therefore was not targeting this kind of information. Again, after numerous consultations with the dental software company, I am convinced the risk of any unauthorized person being able to access the medical records information (which is listed above) is incredibly low as the software is HIPPA compliant. We have placed other safeguards with that company which require PIN and caller ID verification to prevent any access to this data by an unauthorized party. All data of patient records is in unreadable format; it cannot be opened without extreme effort, costly purchases, and expert guidance.

If you have further questions, please contact my office either by phone at 310-820-7272 or by email at dr.gonzalezdds@gmail.com.

Sincerely,

John Gonzalez