



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

August 30, 2016

Re: Notice of Data Breach

Dear John Sample:

Southwest Portland Dental (SPD) is deeply committed to the security and confidentiality of our patients' information, including any such information maintained by our third-party vendors. Regrettably, we are writing to inform you of an incident involving some of that information. We believe we have taken every step necessary to address this incident and prevent future incidents. Please read the following for more information.

I. What Happened

Patterson Dental Supply Inc. (PDSI) is a trusted third-party vendor that provides software to dentists to help manage dental practice information. On July 1, 2016, we determined that between April 2012 and January 2016 one or more unauthorized individuals gained access to a network resource site used by SPD and PDSI in 2010 to exchange data between software systems.

II. What Information Was Involved

The software provided by PDSI to dentists was not, nor were any networks or systems maintained by SPD, involved in this incident. However, we have confirmed that the affected site used to make the 2010 data transfer included electronic files containing SPD dental practice information. Based on our investigation, with the cooperation of PDSI, we determined that the files located on the site included limited information related to some of our patients, possibly including you. The information contained data fields and scattered information within a file such that a person who obtained access to this information would need to take further action to be able to assemble a record about any particular patient. However, because of our knowledge and experiences with the file, we can confirm that, if successfully manipulated, the information involved included patient names, dates of birth, and Social Security numbers. We have no information suggesting that any of the unauthorized individuals successfully assembled a record about any particular patient nor do we have any evidence suggesting that any person intends to use any of this information for malicious purposes.

III. What We Are Doing

PDSI reported the unauthorized access to law enforcement and acted immediately to restrict any further external access to the site. PDSI also hired outside experts to help determine what occurred and to evaluate the risk of harm posed by this event. Law enforcement investigators required that PDSI and SPD delay any public



announcement or notification to potentially affected individuals while they were conducting their investigation. On May 26, 2016, law enforcement gave PDSI permission to notify. SPD began this notification as quickly as possible once SPD had completed its own independent investigation.

IV. What You Can Do

We are notifying you about this incident so you may take appropriate steps to protect your information. We recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your account statements for any unauthorized activity. If you find any unauthorized or suspicious activity, you should contact your credit card company or financial institution immediately. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (see the attached document for more information).

Additionally, we are offering you a complimentary 12-month membership to AllClear ID identity repair and credit monitoring services. These services help detect possible misuse of your personal information and provide you with superior identity protection services focused on immediate identification and resolution of identity theft. AllClear ID identity protection services are completely free to you and enrolling in this program will not hurt your credit score. The AllClear Identity Repair service is available to you with no enrollment required. Unfortunately, privacy laws prevent us from enrolling you directly into monitoring services. **For more information on identity theft prevention and AllClear ID, including instructions on how to enroll into your complimentary 12-month membership, please see the additional information provided in this letter.**

V. For More Information

We regret any inconvenience caused by this incident. To help prevent this type of incident from happening again, SPD is working with PDSI to ensure that it takes appropriate steps to enhance its existing safeguards to protect patient information. If you have questions regarding this incident, please feel free to contact 1-855-303-6662, Monday through Saturday, 6 a.m. to 6 p.m. PST (closed on U.S. observed holidays) and provide your redemption code when calling.

Sincerely,

A handwritten signature in black ink, appearing to read "H R Jarvis".

Howard R. Jarvis

ACTIVATE ALLCLEAR ID SERVICES NOW:

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-303-6662 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-303-6662 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

IDENTITY THEFT PREVENTION GUIDE

Remain Vigilant and Monitor Your Credit. Even if you do not take advantage of the AllClear ID credit monitoring services, we encourage you to remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, every twelve (12) months. To request a free credit report, call 1-877-322-8228 or visit www.annualcreditreport.com. You may also obtain a credit report directly from each of the three nationwide credit reporting agencies (see below for contact information).

Sign up for free "fraud alert" and/or security/freeze: At your request, the three major credit bureaus will place a free "fraud alert" on your file letting creditors know that they should take extra steps to confirm your identity before granting credit in your name. You also can request a security freeze on your accounts if you wish. (Please note that these steps may make it more complicated for you to get new credit or make certain purchases.) A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. If you would like to place a fraud alert or security freeze, contact any one of the following credit reporting agencies, and that agency will inform the others:

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax PO Box 740241 Atlanta, GA 30374 www.equifax.com 1-800-465-7166	Experian PO Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	TransUnion PO Box 2000 Chester, PA 19016 www.transunion.com 1-800-916-8800
---	--	--

Inform Law Enforcement. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can report potential identity theft or file a complaint with the FTC using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, DC 20580. For more information, you may also visit <https://www.identitytheft.gov/>.



ADDITIONAL INFORMATION FOR RESIDENTS OF CERTAIN STATES

If you are an Oregon resident, for more information on consumer protection and identity theft, you may visit the web site of the Oregon Department of Justice at <http://www.doj.state.or.us>.

If you are a Massachusetts resident, you have a right to obtain a copy of a police report if one is filed in connection with this situation. If a police report is filed with Massachusetts authorities (one has not been filed at this time), we will let you know. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that this freeze may delay approval of any requests you (or others) make for information about your credit.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. To request a freeze, send a written request to each credit reporting agency at the address listed above.

You will need to provide your personal information including your full name, social security number, date of birth, addresses for the past five years, proof of current address (such as a copy of a utility bill), and a photocopy of your government-issued ID card. If you are a victim of identity thief, provide a copy of the police report or compliant to a law enforcement agency concerning the incident. If you are not a victim of identity theft, include a check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a Maryland resident, you also may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending an email to idtheft@oag.stat.md.us, or calling 1-410-576-6491.

If you are a North Carolina resident, for more information about preventing identity theft, you may contact the North Carolina Attorney General office at 9001 Mail Service Center, Raleigh, NC 27699-9001, or by calling 1-919-716-6400, or visit the Attorney General website at <http://www.ncdoj.com/>.

If you are a California resident, for more information on identify theft, you may visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.