This dental practice belongs to an affiliation of dental practices called Professional Dental Alliance. Professional Dental Alliance's culture is driven by a desire to provide our patients with the highest level of dental care. Because we value our patients', team members' and others' need for confidentiality in all aspects of our work, we are proactively making the following information available regarding a data security incident at a vendor. The investigation is ongoing, and we will update this page as additional information becomes available.

What happened?

Professional Dental Alliance ("PDA") was recently notified that a few email accounts of its vendor, North American Dental Management, containing some limited patient information were accessed by an unauthorized person between March 31 and April 1, 2021 as the result of an email phishing incident. At this time, the identity of some individuals is known, but the vendor's investigation is ongoing. This notice will be updated with additional information as the investigation continues. Our vendor has confirmed that access to information was limited to a few email accounts. There is no current evidence of any actual misuse of personal information and current information indicates that the attack was limited to email credential harvesting.

What has been done?

We are very serious about protecting the personal information of our patients and have confirmed that immediate action was taken to secure the email accounts and information in the accounts, information in the vendor's network and information in the PDA network. We are

continuing to take actions to confirm the security and privacy of all personal information including providing complimentary identity theft protection services, enhancing email security, providing email security training to staff and email phishing tests. Monitoring of the dark web is being conducted to determine if any malicious use of information has occurred and as of this date, there is no indication of malicious use of personal information.

Who is potentially affected?

Because personal information may have been potentially exposed, we are providing notice so that potentially affected individuals may take precautions to protect themselves. We are continuing to identify potentially affected persons. Additional individual notice will be provided at such time that potentially affected individuals are identified. If you were a patient or patient guarantor at our dental practice prior to April 2, 2021, your personal information may have been impacted.

What information was affected?

There was no access to PDA's patient electronic dental record or dental images; however, some discreet personal information may have been present in the email accounts. The full extent of the potentially affected personal information is not yet known and will vary between persons, but it may include the following: name, address, email address, phone number, dental information, insurance information, Social Security Number, and/or financial account numbers.

How can you protect yourself?

To help provide protection, PDA will offer complimentary credit monitoring and identity theft services for two (2) years for potentially affected persons. Information regarding this service will be in the notice letter mailed to you.

We encourage you to call the toll-free numbers of any of the three major credit bureaus to place a fraud alert on your credit report and order your free credit report:

- Experian: 1-888-397-3742; P.O. Box 9532, Allen, TX 75013
- Equifax: 1-800-525-6285; P.O. Box 740241, Atlanta, GA 30374-0241
- TransUnion: 1-800-680-7289; P.O. Box 6790, Fullerton, CA 92834-6790.

We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call (888) 397-0067 toll-free Monday through Friday from 6am to 8pm Pacific Time or 8am to 5pm Pacific time on Saturday and Sunday – excluding major holidays.

RECOMMENDED NEXT STEPS IF YOU RECEIVE A NOTICE:

1. **Activate the credit monitoring.** Follow the instructions for enrollment using your Enrollment Code provided at the top of your Notice letter and contact Experian at the number provided in the Notice if you have questions.

2. Telephone. Contact Experian at the toll-free number in your Notice to gain additional information about this Notice and speak with Experian about the appropriate steps to take to protect your credit identity.

3. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in Experian identity protection, notify them immediately by calling or by logging into the Experian website and filing a request for help.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You will need to contact Experian or the three national credit reporting bureaus listed above to place the freeze and provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. If you are a victim of identity theft, include a copy of either the police report, investigative

report, or complaint to a law enforcement agency concerning identity theft. The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including 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. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) 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 make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

6. State Resources. Review the state resources available in your state to assist in protecting you from identity theft. A list of available resources by state follows:

ADDITIONAL RESOURCES:

All US Residents: Visit the Federal Trade Commission, Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW Washington, DC 20580, on its website at www.consumer.gov/idtheft, or by phone at 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261. for additional information on protection against identity theft.

Alabama Residents: Visit the Office of Information Technology (https://cybersecurity.alabama.gov/) for additional information on protection against identity theft.

Arizona Residents: Visit the Office of the Attorney General of Arizona (https://www.azag.gov/consumer/data-breach/identity-theft) for additional information on protection against identity theft.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Colorado Residents: Visit the Office of the Attorney General of Colorado (https://coag.gov/resources/data-protection-laws/faqs-for-consumers/) for additional information on protection against identity theft.

Connecticut Residents: Visit the Office of the Attorney General of Connecticut (https://portal.ct.gov/AG/Departments/Privacy/The-Privacy-and-Data-Security-Department) for additional information on protection against identity theft at

Florida Residents: Visit the Office of the Attorney General of Florida (http://myfloridalegal.com/pages.nsf/Main/53D4216591361BCD85257F77004BE16C) for additional information on protection against identity theft.

Georgia Residents: Visit the Georgia Office of the Attorney General - Consumer Protection Division (https://consumer.georgia.gov/consumer-topics/cybersecurity-georgia) for additional information on protection against identity theft.

Illinois Residents: Visit the Office of the Attorney General of Illinois (https://www.illinoisattorneygeneral.gov/consumers/idtheft.html) for additional information on protection against identity theft.

Indiana Residents: Visit the Office of the Attorney General of Indiana Consumer Protection Division (https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/ or call (800) 382-5516) for additional information on protection against identity theft.

Kentucky Residents: Visit the Office of the Attorney General of Kentucky (www.ag.ky.gov, by mail: 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, or phone: Telephone: 1-502-696-5300) for additional information on protection against identity theft.

Maryland Residents: Visit the Office of the Attorney General of Maryland, Consumer Protection Division (www.oag.state.md.us/Consumer, by mail: 200 St. Paul Place Baltimore, MD 21202, or phone:: 1-888-743-0023) for additional information on protection against identity theft.

Massachusetts Residents: You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may also place a security freeze on your credit reports, free of charge, as described earlier. Visit the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, on its website

(https://www.mass.gov/info-details/protecting-your-privacy or call (888) 283-3757) for additional information on protection against identity theft.

Michigan Residents: Visit the Office of the Attorney General of Michigan (https://www.michigan.gov/ag/0,4534,7-359-81903_20942_30997-487726--,00.html) for additional information on protection against identity theft.

Minnesota Residents: Visit the Office of the Attorney General of Minnesota (https://www.ag.state.mn.us/consumer/Publications/PersonalInformationBreaches.asp) for additional information on protection against identity theft.

Missouri Residents: Visit the Office of the Attorney General of Missouri (https://ago.mo.gov/civil-division/consumer/identity-theft-data-security/data-breaches) for additional information on protection against identity theft.

New Jersey Residents: Visit the New Jersey Office of the Attorney General Department of Law and Public Safety (https://www.njsp.org/tech/identity.html) for additional information on protection against identity theft.

Nevada Residents: Visit the Office of the Attorney General of Nevada Bureau of Consumer Protection (https://ag.nv.gov/About/Consumer_Protection/Bureau_of_Consumer_Protection/) for additional information on protection against identity theft.

New York Residents: Visit the Office of the Attorney General (https://ag.ny.gov/; by mail: The Capitol, Albany, NY 12224-0341; or phone: 1-800-771-7755) for additional information on protection against identity theft.

North Carolina Residents: Visit the Office of the Attorney General Carolina Consumer Protection Division (https://ncdoj.gov/protecting-consumers/protecting-your-identity; by mail: 9001 Mail Service Center, Raleigh, NC 27699-9001, or call: 1-877-566-7226 or 1-919-716-6000) for additional information on protection against identity theft.

Ohio Residents: Visit the Ohio Attorney General's Office (https://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Identity-Theft or phone: 800-282-0515) for additional information on protection against identity theft.

Pennsylvania Residents: Visit the Pennsylvania Office of the Attorney General (https://www.attorneygeneral.gov/protect-yourself/identity-theft/) for additional information on protection against identity theft.

South Carolina Residents: Visit the South Carolina Department of Consumer Affairs (https://consumer.sc.gov/identity-theft-unit) for additional information on protection against identity theft.

Tennessee Residents: Visit the Tennessee Bureau of Investigation (https://www.tn.gov/tbi/crime-issues/crime-issues/identity-theft.html) for additional information on protection against identity theft.

Texas Residents: Visit the Office of the Attorney General of Texas (https://www.texasattorneygeneral.gov/consumer-protection/identity-theft) for additional information on protection against identity theft.

Virginia Residents: Visit the Office of the Attorney General of Virginia (https://www.oag.state.va.us/programs-initiatives/identity-theft) for additional information on protection against identity theft.

Washington Residents: Visit the Office of the Attorney General of Washington (https://www.atg.wa.gov/recovering-identity-theft-or-fraud) for additional information on protection against identity theft.

West Virginia Residents: Visit the Office of the Attorney General of West Virginia (https://ago.wv.gov/consumerprotection/pages/identity-theft-prevention.aspx) for additional information on protection against identity theft.

Wisconsin Residents: Visit the Bureau of Consumer Protection (https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx, by mail: 2811 Agriculture Drive, Madison, WI 53708-8911 or by phone: (800) 422-7128) for additional information on protection against identity theft.