

December 29, 2023

Notice of Data Security Incident

We are posting this notice to provide important information regarding a recent security incident involving personal information maintained by Knowles, Smith & Associates d/b/a/ Village Family Dental (“Village Family Dental”), including protected health information as defined by the Health Insurance Portability and Accountability Act. We want to provide patients with details about the incident and let patients know that we continue to take significant measures to protect their information.

On November 17, 2023 Village Family Dental detected an intrusion to its network. Immediately upon detecting this activity, we took steps to mitigate the threat, including taking certain systems offline. We also quickly engaged professionals experienced in handling these types of incidents to assist us with an investigation and to assess the full scope of information impacted. Village Family Dental has notified and is cooperating with law enforcement in connection to our ongoing forensic investigation. On November 23, 2023, the investigation revealed that personal information, including protected health information of some patients, was accessed and acquired by an unauthorized party as early as November 16, 2023.

The investigation is ongoing, including with respect to identifying specific persons impacted and the type of patient data that was impacted. We will notify all known impacted individuals as quickly as possible, and in accordance with applicable laws. This means that if we learn that your personal information or protected health information was impacted, we will provide notice consistent with our legal obligations.

Out of an abundance of caution, all Village Family Dental patients and personnel are encouraged to take steps to protect themselves. This includes protecting themselves against identity fraud, including placing a fraud alert/security freeze on their credit files, obtaining free credit reports, and remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Village Family Dental is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of the information we maintain, and we are taking significant steps to mitigate the risk to persons impacted by this incident.

If you have any questions regarding this incident, please call our dedicated and confidential toll-free response line at **888-723-2015**. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available 9:00am to 9:00pm ET, Monday through Friday, excluding holidays.

The privacy and security of the personal information we maintain is of the utmost importance to us, and we sincerely regret any inconvenience this incident may cause you.

Sincerely,
Village Family Dental

Steps Individuals Can Take to Protect Personal Information

1. Protecting Your Medical Information.

The following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Freeze	Security	Experian Freeze	Security	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (800) 349-9960 (888) 298-0045		P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742		P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC

20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.