NOTICE OF DATA EVENT

Keep Smiling Dental Group (“KSDG”), a privately owned, family dental practice located in Beavercreek, Ohio, is providing notice of an event that may involve information related to certain individuals. Although KSDG is not aware of any identity theft or fraud in relation to the event, KSDG is taking steps to provide notifications directly to potentially involved individuals. This notice includes information about what happened, the steps taken since learning of the event, and the resources related to individuals to better protect against potential misuse of their personal information, should they feel it appropriate to do so.

What Happened? KSDG recently experienced a network disruption involving certain computer systems and files. In response, KSDG promptly took steps to confirm the security of our systems and began a thorough investigation to determine the nature and scope of the event. The investigation confirmed the disruption was the result of a cybersecurity incident and that certain files were accessed or taken from the KSDG network between August 29, 2026 and September 5, 2026. KSDG first identified activity related to the event on September 7, 2026. As a result, KSDG undertook a comprehensive review of the files involved to determine what information was involved in this event and to whom it belonged. This review recently completed, and KSDG is working to assess which individuals are involved and to locate address information for them to effectuate direct notifications.

What Information Was Involved? The information involved varies by individual, but may include: name, patient ID, date of birth or age, contact information (such as address, phone number, or email address), dental insurance information, dental account and billing information (such as account balances and treatment charges), dental records (including X-rays, treatment plans, and clinical notes), medical history, and appointment or schedule information. For a limited number of individuals, Social Security number may also have been involved; KSDG is notifying all individuals identified as being involved directly if they can locate complete address information.

What We Are Doing. Protecting the information KSDG patients and team members trust us with is a responsibility we take very seriously. Our response included promptly securing our network, completing an investigation into how this happened and what information was involved, and taking action on preventing future cyber threats. We implemented additional cybersecurity measures, including server-wide security enhancements and additional phishing-awareness training for our staff, and reviewed existing security policies to further protect against similar events moving forward. We also reported this event to the Federal Bureau of Investigation and are cooperating with their investigation.

For More Information. If you have additional questions, please call our dedicated assistance line at 1 833-918-1289 from 9:00 a.m. ET to 9:00 p.m. ET, Monday through Friday, excluding major U.S. holidays, and reference Engagement Number B175906. You may also contact our office directly at 1 (937) 426-5340. Thank you for your patience and for the trust you place in us.

What You Can Do. KSDG encourages all individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity and to detect errors. Additionally, we encourage individuals to check their explanations of benefits regularly to ensure that there has not been any unexpected activity. Unexpected activity should be promptly reported to relevant parties including an insurance company, healthcare provider, and/or financial institution. Please also be cautious of unexpected emails, text messages, or phone calls that claim to be from KSDG or that reference this event. KSDG will never ask you for your Social Security number, banking information, or passwords by email or text message. If you receive a suspicious message that appears to come from us, please do not click any links or reply, and instead call our office directly at 1 (937) 426-5340.

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus: Equifax, Experian, and TransUnion. To order a free credit report, visit https://www.annualcreditreport.com or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three (3) major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help/
1 (888) 298-0045	1 (888) 397-3742	1 (833) 799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; https://www.identitytheft.gov; 1 (877) ID-THEFT (1 (877) 438-4338); and TTY: 1 (866) 653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and http://oag.dc.gov. KSDG is located at 4090 Indian Ripple Rd. Ste. 101, Beavercreek, Ohio 45440.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1 (410) 576-6300 or 1 (888) 743-0023; and https://oag.maryland.gov. KSDG is located at 4090 Indian Ripple Rd. Ste. 101, Beavercreek, Ohio 45440

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1 (800) 771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1 (877) 566-7226 or 1 (919) 716-6000; and https://www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; https://www.riag.ri.gov; and 1 (401) 274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Whether any residents of Rhode Island are involved is not confirmed as of the date of this notification.