Hollister Family Dental & Implant Center ("Hollister Dental") is providing notice about an event that may have impacted the sensitive personal information of certain individuals. This notice provides details about the event, measures Hollister Dental has taken in response, and additional steps impacted individuals can take to help protect their sensitive personal information, if they feel it is necessary to do so.

On May 8, 2026, Hollister Dental became aware of a potential issue involving its third-party appointment management platform. Hollister Dental immediately took steps to secure its systems and investigate the extent of this activity. As a result of its investigation, Hollister Dental determined that an unauthorized party accessed the platform between February 12, 2026, and May 8, 2026, via an online account associated with a Hollister Dental team member.

As part of our investigation, Hollister Dental assessed what sensitive personal information may have been impacted in connection with the event. Hollister Dental concluded this assessment on October 8, 2026, and determined that the sensitive personal information of certain individuals may have been affected. Such sensitive personal information may include names, contact information, date of birth, and dental care-related information (e.g., appointment history and type, questions, providers, symptoms, and medications).

Following the event, to help prevent something similar from occurring, Hollister Dental implemented additional safeguards and technical security measures to further protect its systems. While Hollister Dental is not aware of any misuse of the sensitive personal information at issue, out of an abundance of caution, it has secured the services of Kroll to provide two years of identity monitoring services to potentially impacted individuals at no cost. Such individuals have until February 12, 2027, to activate and take advantage of these identity monitoring services.

We encourage impacted individuals, as a best practice, to remain vigilant to the possibility of fraud by reviewing account statements and monitoring free credit reports for any unauthorized activity and reporting any such activity. For questions, call (844) 971-8633, Mon-Fri, 8:00 a.m. to 5:30 p.m. CT, excluding major U.S. holidays.

## ADDITIONAL RESOURCES

### Review Account Statements and Credit Reports

Individuals should remain vigilant, including for incidents of fraud and identity theft, by reviewing account statements and monitoring credit reports. Under federal law, an individual may be entitled every 12 months to one free copy of the individual's 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. Individuals may wish to stagger their requests so that they receive free reports from one of the three credit bureaus every four months.

**Place a Fraud Alert or Credit Freeze/Security Freeze**

Individuals can place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on an individual's credit file. Upon seeing a fraud alert displayed on an individual's credit file, a business must verify the individual's identity before extending new credit. Victims of identity theft may be entitled to an extended fraud alert, which is a fraud alert lasting seven years. To place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, an individual has the right to place a "credit freeze" (also referred to as a "security freeze") on a credit report free of charge, which will prohibit a credit bureau from releasing information in the credit report without the individual's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in the individual's name without the individual's consent. Note that using a credit freeze to control who can access an individual's personal and financial information in the individual's credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application the individual makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a credit freeze on the individual's credit report. You may need the following information to request a credit freeze: (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 to five 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 (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 the individual is a victim of identity theft.

To place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/<br><br>https://www.equifax.com/personal/credit-report-services/credit-freeze/ | https://www.experian.com/help/ | https://www.transunion.com/customer-support/contact-us-consumers |
| 1-888-298-0045 | 1-888-397-3742 | 1-800-916-8800 |
| Equifax Fraud Alert<br>P.O. Box 105069<br>Atlanta, GA 30348-5069 | Experian Fraud Alert<br>P.O. Box 9554<br>Allen, TX 75013 | TransUnion Fraud Alert<br>P.O. Box 2000<br>Chester, PA 19016 |

| | | |
|---|---|---|
| Equifax Credit Freeze<br>P.O. Box 105788<br>Atlanta, GA 30348-5788 | Experian Credit Freeze<br>P.O. Box 9554<br>Allen, TX 75013 | TransUnion Credit Freeze<br>P.O. Box 160<br>Woodlyn, PA 19094 |

**Other Steps For Consideration**

Individuals may educate themselves regarding identity theft, fraud alerts, credit freezes, security breach response, identity theft prevention and protection, and the steps they can take to protect personal information by contacting the individual credit reporting bureaus (as described above), the Federal Trade Commission, or their state Attorney General. In particular, the Federal Trade Commission encourages those who discover their information has been misused to file a complaint. Individuals can obtain further information on filing such a complaint by using the contact information listed below.

An individual can file a police report in the event of identity theft or fraud. Please note that to file a report with law enforcement for identity theft, an individual will likely need to provide some proof of the identity theft. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.

This notification was not delayed as a result of a law enforcement investigation.

*All U.S. Residents*: Individuals may contact and obtain information from the Federal Trade Commission at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580; 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or www.consumer.gov/idtheft.