

## **Notice of Data Security Incident**

TOMS RIVER, NEW JERSEY: December 22, 2023 – ProSmile Holdings, LLC (“ProSmile”) is a dental service organization which experienced a data security incident that may have impacted personal and protected health information belonging to certain individuals who received dental services from various dental practices that ProSmile supports. ProSmile takes the protection of personal and protected health information very seriously.

On July 7, 2022, ProSmile learned of a potential data security incident involving its email environment. In response, ProSmile promptly engaged an independent digital forensics and incident response firm to investigate. On December 1, 2022, ProSmile received confirmation that numerous email accounts within its email environment had been accessed without authorization and began working to identify the personal / protected health information contained therein that may have been impacted. On January 27, 2023, a vendor engaged to assist with this process advised that the incident likely resulted in unauthorized access to personal / protected health information. Thereafter, ProSmile continued with its comprehensive review, and on November 29, 2023, ProSmile identified all potentially impacted individuals for purposes providing notification thereto. Notably, to date, ProSmile has no evidence to suggest that any potentially impacted information has been misused as a result of this incident.

This incident may have involved information belonging to individuals who may have received dental treatment from clinics that use ProSmile for administrative and support services, and may have included names, dates of birth, Social Security numbers, driver’s license or other state identification card numbers, financial account numbers, payment card numbers, medical treatment information, diagnosis or clinical information, provider information, prescription information, and health insurance information.

On December 22, 2023, ProSmile sent notification of this incident by way of the United States Postal Service to potentially impacted individuals with identifiable address information and provided resources to assist them. In addition, ProSmile has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives are available between the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday, excluding holidays, and can be reached at 1-888-817-4969, or you can go to <https://app.idx.us/account-creation/protect>.

The privacy and protection of personal and protected health information is a top priority for ProSmile, which deeply regrets any inconvenience or concern this incident may cause.

***While ProSmile has no evidence of the misuse of any potentially affected individual’s information as a result of this incident, ProSmile is providing the following information about steps that individuals can take to help protect their information:***

### **ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION**

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.consumer.ftc.gov](http://www.consumer.ftc.gov), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, [www.equifax.com](http://www.equifax.com).
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com).
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, [www.transunion.com](http://www.transunion.com).

**Fraud Alerts:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

**Credit or Security Freezes:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

**IRS Identity Protection PIN:** You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

**Additional information:**

**District of Columbia:** The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [oag@dc.gov](mailto:oag@dc.gov)

**California:** California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

**Massachusetts:** Massachusetts Attorney General can be reached at: 1 Ashburton PI Boston, MA 02108; 617-727-8400; <https://www.mass.gov/orgs/office-of-the-attorney-general>

**Maine:** Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

**Maryland:** Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; [oag@state.md.us](mailto:oag@state.md.us) or [IDTheft@oag.state.md.us](mailto:IDTheft@oag.state.md.us)

**North Carolina:** North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; [www.ncdoj.gov](http://www.ncdoj.gov)

**New York:** New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

**Rhode Island:** Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

**Texas:** Texas Attorney General can be reached at: 300 W. 15<sup>th</sup> Street, Austin, Texas 78701; 800-621-0508; [texasattorneygeneral.gov/consumer-protection/](http://texasattorneygeneral.gov/consumer-protection/)

**Vermont:** Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; [ago.info@vermont.gov](mailto:ago.info@vermont.gov)