



Robert Bender
Constangy, Brooks, Smith & Prophete, LLP
bbender@constangy.com
445.308.1588
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

July 21, 2025

VIA ONLINE SUBMISSION

Re: Notification of Data Security Incident

Dear Attorney General Hilgers:

Constangy, Brooks, Smith & Prophete, LLP represents Upper Dublin Family Dentistry (UDFD), located at 3515 W. Moreland Road, Willow Grove, PA 19090 in conjunction with their response to a recent data event involving information for a Nebraska resident. The purpose of this letter is to notify you of the incident in accordance with Neb. Rev. Stat. §§ 87-801 - 808. UDFD does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of Neb. Rev. Stat. §§ 87-801 - 808, or personal jurisdiction by providing this notice.

1. Nature of the Security Incident

On May 13, 2025, UDFD discovered that an unauthorized party gained access to its computer systems and deployed malicious software that encrypted data. UDFD immediately engaged a leading cybersecurity and forensic firm to investigate the incident, to contain the threat, and to restore system functionality. The investigation determined the individuals responsible for the attack may have accessed or viewed network locations that included patient information.

2. Number of Affected Nebraska Resident & Information Involved

On July 17, 2025, UDFD confirmed the incident involved information for one Nebraska resident. The information involved in the incident includes name and Social Security number. At this time, there is no evidence that any of this information has been misused.

3. Notification to Affected Individuals

On July 21, 2025, UDFD notified one Nebraska resident by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in complimentary identity protection services.

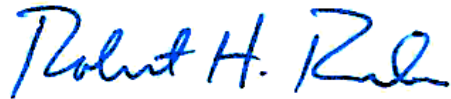
4. Measures Taken to Address the Incident

Upon discovering this incident, UDFD conducted an immediate and comprehensive investigation to confirm the scope of the event to secure its network and to notify affected individuals. UDFD also improved its web server infrastructure and implemented enhanced safeguards to reduce the risk of future incidents. UDFD reported the event to the U.S. Department of Health & Human Services. UDFD also notified established a toll-free call center to answer questions about the incident and to address related concerns.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at bbender@constangy.com or 445-308-1588.

Sincerely,



Robert Bender
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

July 21, 2025

Notice of Data Event

Dear [REDACTED]

Upper Dublin Family Dentistry ("UDFD") values the privacy and security of our patients' information. We are providing notice of a recent data security incident that may have involved patient information. This letter provides an overview of the event, steps taken in response, and resources available to individuals to protect their information.

On May 13, 2025, we discovered that an unauthorized party gained access to our computer systems and deployed malicious software that encrypted our data. We immediately engaged a leading cybersecurity and forensic firm to investigate the incident, to contain the threat, and to restore system functionality. The investigation determined the individuals responsible for the attack may have accessed or viewed network locations that included patient information. This data may have included names, Social Security numbers, dates of birth, home addresses, phone numbers, and dental medical records that would contain treatment dates and summaries and claim information. At this time, we have no evidence that any of this information has been misused.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We have taken immediate steps to improve our system security, including strengthening our web server infrastructure and implementing enhanced safeguards to prevent future incidents. We recommend patients review and monitor their accounts for suspicious activity, including reviewing any explanation of benefits. We value the trust our patients place in us and are happy to address any questions. If you have questions or need assistance, please call (866) 910-0429 Monday through Friday from 9:00am - 7:00pm Eastern Time.

Sincerely,

Upper Dublin Family Dentistry

DUBLIN_1-ADT-CM12

Steps You Can Take to Help Protect Your Personal 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 (the “FTC”).

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 www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

Additional Free Resources: You also have the right to obtain any police report filed in this matter. 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. You can contact the Federal Trade Commission at 600 Pennsylvania Ave, NW, Washington, DC 20580; consumer.ftc.gov; 877-438-4338. Residents of the below states can obtain additional information about the steps you can take to avoid identity theft:

- **District of Columbia residents:** District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; oag@dc.gov; 202-727-3400.
- **Maryland residents:** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; <https://www.marylandattorneygeneral.gov>; 1-410-528-8662 or 1-888-743-0023.
- **New York residents:** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov>; or 1-800-771-7755.
- **North Carolina residents:** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; <https://ncdoj.gov>; and toll-free at (877) 566-7226 or (919) 716-6000.
- **Rhode Island residents:** Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag.ri.gov or 401-274-4400. There are approximately two Rhode Island residents potentially impacted by this incident.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf