

May 30, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs & Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Notification of Data Security Incident

Dear Attorney General Hilgers:

Constangy Brooks Smith & Prophete LLP represents Bradford Health Services (“Bradford Health”) headquartered in Birmingham, Alabama, with respect to a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

Nature of the Security Incident

On December 8, 2023, Bradford Health experienced an encryption incident that disrupted access to certain parts of its digital environment. In response, Bradford Health took immediate steps to secure its environment and promptly launched an investigation with the assistance of independent cybersecurity experts. As a result of this investigation, Bradford Health learned that an unauthorized actor acquired certain data stored in its systems. After a thorough review of the data, on May 15, 2025, Bradford Health determined that certain personal and/or protected information may have been impacted by this incident.

The affected information varies by individual, but includes individuals’ names, driver’s license numbers, dates of birth, medical information (including diagnosis and treatment information, physician names, and Medical Record numbers), health insurance information, financial account numbers, passport numbers, payment card numbers plus a means of access to the account, and/or Social Security numbers.

Number of Nebraska Residents Affected

On May 30, 2025, Bradford Health notified forty-six (46) Nebraska residents of this incident via First-Class U.S. Mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

Steps Taken Relating to the Incident

To help prevent something like this from happening again, Bradford Health is implementing additional security protocols. It is also offering complimentary credit and identity protection monitoring services to individuals whose Social Security numbers were involved in the incident.

Contact Information

Bradford Health remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me by email at lfunk@constangy.com.

Regards,

A handwritten signature in black ink, appearing to read 'L. Funk', with a long, sweeping horizontal line extending to the right.

Laura K. Funk
Partner

Enc.: Sample Consumer Notification Letter



Return Mail Processing Center
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

May 30, 2025

Subject: Notice of Data <<Header>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you about a data security incident experienced by Bradford Health Services (“Bradford Health”) that may have involved your personal and / or protected health information. Bradford Health takes the privacy and security of all information within its possession very seriously. That is why we are writing to notify you of the incident, provide complimentary identity monitoring services, and provide you with information about steps you can take to help protect your information.

What Happened. On December 8, 2023, Bradford Health detected unusual activity within its network. Upon discovery, we immediately took steps to secure our network and engaged a leading, independent digital forensics and incident response firm to investigate. Based on that investigation, Bradford Health learned that an unknown actor gained unauthorized access to our network and acquired certain files, some of which contained individuals’ personal and / or protected health information. With the assistance of a third-party data review team, we conducted a comprehensive review of all potentially impacted data to identify the individuals and information involved. On May 15, 2025, we determined that your information was impacted.

What Information Was Involved. The information that was potentially impacted during this incident may have included your name, as well as your <<Affected Data Elements>>.

What Are We Doing. As soon as Bradford Health discovered the incident, we took the steps described above and implemented measures to enhance the security of our network and reduce the risk of a similar incident occurring in the future. Bradford also reported the incident to law enforcement and is cooperating with any resulting investigation. While we have no evidence that any of your information was misused, we are offering you <<CM Length>> months of complimentary identity protection services through IDX, a national leader in identity protection services.

What Can You Do. You can follow the recommendations on the following pages. You can also enroll in the IDX identity protection services, which are offered to you at no cost.

To enroll, please call 1-877-670-4122 or visit <https://app.idx.us/account-creation/protect> and provide the enrollment code at the top of this page. Please note you must enroll by August 30, 2025. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

For More Information: If you have questions or need assistance, please contact 1-877-670-4122 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Andy Seitz
Chief Compliance Officer

Bradford Health Partners
2101 Magnolia Avenue South, Suite 518
Birmingham, AL 35205

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 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

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. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/credit-freeze.

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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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.