CONSTANGY
Brooks Smith & Prophete

Melissa J. Sachs, Partner
Cybersecurity & Data Privacy Team
1650 Market Street Suite 3600
Philadelphia, PA 19103
msachs@constangy.com
267.219.8332

July 14, 2026

VIA ONLINE SUBMISSION:
Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

Re: **Notice of Data Security Incident**

To Whom it May Concern:

Constangy, Brooks, Smith and Prophete LLP (Constangy) represents The National Association on Drug Abuse Problems, Inc (NADAP), located at 520 Eighth Avenue, Suite 1200, New York, NY 10018, in connection with a recent data incident involving information for Nebraska residents. The purpose of this letter is to notify you, in accordance with Nebraska's data breach notification statute. This notice may be supplemented with any new significant facts learned subsequent to its submission. NADAP hereby reserves all rights and defenses in connection herewith.

1. Nature of Incident

On or about January 10, 2026, NADAP identified suspicious activity within our network, and promptly took steps to secure its environment and launched an investigation. With the support of cybersecurity experts, it learned of information suggesting that an unknown actor gained unauthorized access to its network and accessed files, some of which contained protected personal information. We then worked expeditiously with our NYC program partners to identify all impacted individuals and their most up-to-date contact information. In the interim, we published substitute notice about the incident on our website and reported it to the media on March 30, 2026. We also sent direct notifications to individuals on a rolling basis on March 30 and May 18, 2026, as we identified them and their contact information. On or around June 22, 2026, we identified additional individuals potentially impacted. We confirmed on or around June 29, 2026, that these individuals included 11 Nebraska residents.

2. Number of Nebraska Residents Affected & Information Involved

For these 11 Nebraska residents, the impacted information will vary by individual but may include the residents' names along with Social Security number, Medicaid Client Identification Number, and/or medical, health, or diagnosis information.

3. Notification to Affected Individuals

On July 14, 2026, NADAP notified 11 Nebraska residents by First Class U.S. Mail. NADAP has also set up a toll-free call center to answer questions about the incident and to address related concerns. Impacted callers will have the opportunity to enroll in complimentary 24-months credit monitoring services and proactive fraud assistance.

4. Steps taken relating to the incident

In response to the incident, NADAP conducted an immediate and comprehensive investigation to confirm the scope of the event to secure its network and to determine the source and scope of the compromise. NADAP implemented additional measures to enhance network security and minimize the risk of a similar incident occurring in the future, including enforcing stronger password requirements and implementing conditional access policies. NADAP also notified the U.S. Department of Health and Human Services, the New York State Department of State, the New York State Division of State Police, and the Office of the New York State Attorney General, as well as our partner agencies and the FBI, and we will cooperate with any resulting investigation, providing whatever cooperation may be necessary to hold the bad actors accountable. NADAP continues to review policies and procedures and so it can implement additional measures as appropriate.

5. Contact information

NADAP takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 267.219.8332 or msachs@constangy.com.

Sincerely yours,

[Draft]

Melissa J. Sachs of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Notice Letter Proof

National Association on Drug Abuse Programs, Inc
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2998B

608_0189758

0189758

[redacted]

To Enroll, Please Visit:
[redacted]
Enrollment Code: [redacted]

July 14, 2026

Subject: Notice of Data Security Incident

Dear [redacted]:

We are writing to inform you of a recent data security incident that may have affected your protected health information. The National Association on Drug Abuse Programs, Inc (NADAP) takes the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On or about January 10, 2026, NADAP identified suspicious activity within its network and promptly initiated an investigation of the matter. We engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain NADAP files were accessed by an unauthorized user. We undertook a comprehensive review of those files and, on or about January 27, 2026, learned that some of these files may have contained protected health and/or personal information. We then worked expeditiously with our program partners to identify all impacted individuals and their most up-to-date contact information. We identified your name and contact information on June 22, 2026.

What Information Was Involved. The information that was accessed by the unauthorized user may have included your first and last name, Medicaid Client Identification Number and medical, health, or diagnosis information.

What We Are Doing. As soon as NADAP discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We are also offering you complimentary identity protection services through Cyberscout, a TransUnion company, a leader in consumer identity protection. These services include twenty-four (24) months of credit monitoring that provides you with alerts 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 the event that you become a victim of fraud, and a $1 million identity fraud loss reimbursement policy. The deadline to enroll in these services is 90 days from the date of this letter. We also notified the U.S. Department of Health and Human Services, the New York State Department of State, the New York State Division of State Police, the Office of the New York State Attorney General, and the New York City Human

Resources Administration (HRA), as well as our partner agencies and the FBI, and we will cooperate with any resulting investigation, providing whatever cooperation may be necessary to hold the bad actors accountable.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through TransUnion by going to [redacted] and using enrollment code [redacted].

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-855-522-0352 Monday through Friday from 8:00AM to 8:00PM ET. We take your trust in us and in this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

National Association on Drug Abuse Programs Inc.
520 8th Ave, Suite 1200
New York, NY 10018

0189758

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
1-800-916-8800
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 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

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

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

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

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

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

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

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

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

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

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

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, orunverifiable 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.