

**North Texas Behavioral Health Authority  
Notice Regarding Data Security Incident**

North Texas Behavioral Health Authority is committed to protecting the privacy and security of the personal information in our possession. On or about October 15, 2025, North Texas Behavioral Health Authority detected unauthorized access to our network that resulted in the exposure of certain data we maintain. Upon learning of the issue, we commenced a prompt and thorough investigation.

As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following the completion of our investigation, it was determined that some of our files may have been accessed and removed by the unauthorized individual(s) between October 13, 2025, and October 15, 2025. We conducted a thorough review of the potentially impacted data, and on January 7, 2026, we determined that the impacted files may have contained personal information.

While we have no indication that there has been any fraud as a result of this incident, out of an abundance of caution, commencing on March 6, 2026, North Texas Behavioral Health Authority notified individuals whose information was included in the files that may have been accessed and removed by the unauthorized individual(s). Notified individuals have been provided with best practices to protect their information, and individuals whose Social Security numbers were contained in the impacted files have been offered complimentary credit monitoring.

North Texas Behavioral Health Authority understands the importance of safeguarding individual personal information. North Texas Behavioral Health Authority remains fully committed to maintaining the privacy of personal information in our possession, and upon learning of the incident, North Texas Behavioral Health Authority took immediate action to protect the individual personal information it maintains. North Texas Behavioral Health Authority continually evaluates and modifies its practices to enhance the security and privacy of personal information and is taking measures to augment its existing cybersecurity practices. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements, including resetting passwords, expanding multi-factor authentication, and deploying advanced endpoint detection and response tools and services.

For further questions or additional information regarding this incident, please contact the dedicated toll-free response line at 1-833-289-1629. The response line is available for 90 days, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

**– OTHER IMPORTANT INFORMATION –**

**1. Placing a Fraud Alert on Your Credit File.**

We recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance  
Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

**2. Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

***Equifax Security Freeze***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888)-298-0045

***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

***Security***

***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

**3. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at [www.annualcreditreport.com](http://www.annualcreditreport.com). Once you receive your credit reports,

review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

#### **4. Protecting Your Medical Information**

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

#### **5. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

\* \* \* \* \*

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: 515-281-5164.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov), Telephone: 888-743-0023.

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**New Mexico residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit [www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; [ag.ny.gov/consumer-frauds-bureau/identity-theft](http://ag.ny.gov/consumer-frauds-bureau/identity-theft); Telephone: 800-771-7755.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us](http://www.doj.state.or.us), Telephone: 877-877-9392.