

Privacy Breach Incident FAQ

January 2025



TEXAS
Health and Human
Services

Frequently Asked Questions

1. What is the privacy breach incident?

The Texas Health and Human Services Commission (HHSC) discovered that protected health, personal identifying or sensitive personal information may have been inappropriately accessed, used or disclosed.

2. What did HHSC do after learning about the privacy breach?

When the incident was discovered, system access for the employees suspected of involvement was promptly revoked, and their employment was subsequently terminated.

HHSC referred the matter to the Texas Health and Human Services Office of Inspector General (OIG) for a thorough investigation, which remains ongoing.

To safeguard individuals affected by the breach, HHSC is offering two years of free credit monitoring and identity theft protection services from Experian.

Services provided to adults impacted include:

- **Experian Credit Report at Sign-Up:** Users can see what information is associated with their credit file. Daily credit reports are available.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Services provided to minors affected include:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security number (SSN) on the Experian credit report.

- **Internet Surveillance:** Technology searches the web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the dark web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Furthermore, HHSC is strengthening internal security controls and working to implement additional fraud prevention measures, including enhanced monitoring and alerts to detect suspicious activity.

3. Has HHSC notified the authorities?

Yes. HHSC referred the incident to the Texas Health and Human Services Office of Inspector General (OIG) for investigation and coordination with law enforcement to pursue criminal charges. The investigation remains ongoing.

4. Will the employees go to jail because you said criminal charges are being pursued?

Because this is an ongoing investigation, additional information is not available.

5. What kind of information was inappropriately accessed, used or disclosed?

The data that may have been inappropriately accessed, used, or disclosed was not the same for everyone. But the information may have included:

- **Contact** (such as full name, address, phone number, and email address).
- **Financial** (such as employment, income, asset, eligibility, financial and banking information).
- **Benefit** (such as benefit type, amount and payment information).
- **Insurance** (such as health plan or policy, life insurance plan or policy, insurance company, member or group ID number, and Medicaid or Medicare payer ID number).
- **Health** (such as medical records, diagnosis, treatment and care, and disability status).
- **Other personal or sensitive identifying information** (such as Social Security number, date of birth, driver license, state or other

government-issued ID, license or certificate numbers, education and court records or other information related to your eligibility record).

Some Lone Star Cards containing Supplemental Nutrition Assistance Program (SNAP) funds may have been improperly accessed or used.

6. How will I know if I was affected?

HHSC is notifying individuals affected by the breach via first-class regular mail. Letters were mailed no later than Jan. 17, 2025, and include next steps on how to sign up for two years of free credit monitoring and identity protection services, and how to request SNAP funds reimbursement due to fraudulent activity.

The agency will notify any additional individuals it determines were affected by the breach.

7. What should I do?

You should carefully review your accounts and statements sent from health care providers, insurance companies and financial institutions to make sure all account activity is correct.

If you identify charges that you don't recognize, you should report the questionable charges promptly to the provider or company. You should report any suspected fraudulent activity to law enforcement.

You should also consider signing up for the two years of free credit monitoring and identity protection services.

Also, if you are a recipient of SNAP benefits, you should check your Lone Star Card to make sure there hasn't been any fraudulent activity. You can do this by calling the Lone Star Help Desk at 800-777-7328, or logging into your account at YourTexasBenefits.com or on the Your Texas Benefits mobile app.

If there are purchases that you do not recognize, you should take immediate action by calling 2-1-1, and after selecting a language choose Option 3 to report the fraud to OIG. You should also call local law enforcement.

To learn more about how to keep your Lone Star Card safe, you can visit the [Lone Star Card Fraud Awareness and Prevention page](#).

8. Can I be reimbursed if my SNAP funds were affected by the incident?

Yes. You should go to [your local HHSC benefits office](#) if you have identified fraudulent charges on your Lone Star Card.

If you can't go to a local HHSC benefits office because of age, disability, distance or the inability to appoint an authorized representative, you may call your local HHSC benefits office and

request [Form H1854, Affidavit for Unauthorized Use of Electronic Benefit Transfer \(EBT\) Benefits](#), by mail.

9. How much time do I have to report that my SNAP funds were stolen because of this incident?

You must return the completed and signed [Form H1854, Affidavit for Unauthorized Use of Electronic Benefit Transfer \(EBT\) Benefits](#), to HHSC within 30 days from when you discovered your benefits were stolen.

If you request Form H1854 to be mailed to you, you must complete, sign and return it to HHSC by the date printed on the form.

10. Is it safe for me to continue to use my Lone Star Card and access my Your Texas Benefits account?

Yes. It is safe to use your Lone Star Card and access your account.

HHSC recommends monitoring account activity regularly and immediately reporting any unauthorized transactions. Visit the [Lone Star Card Fraud Awareness and Prevention page](#) for more information.

11. What number can I call to get more information about my benefits or Lone Star Card?

You should call 2-1-1. After selecting a language, choose Option 2.