



FOR IMMEDIATE RELEASE

May 2, 2024

Contact: Jacqueline Ortiz, Attorney Supervisor, Office of General Counsel

Email: Jacqueline.Ortiz@osi.nm.gov

NEW MEXICO SUPERINTENDENT OF INSURANCE URGES CONSUMERS TO PROTECT THEMSELVES AGAINST IDENTIFY THEFT AFTER CYBERATTACKS

Santa Fe, NM – The Office of the Superintendent of Insurance (“OSI”) is urging consumers to take action to protect their personal information from identity theft following Change Healthcare’s cyberattack on February 21, 2024.

On February 21, 2024, Change Healthcare, a company which handles 50% of all medical claims across the county, experienced a cyberattack on February 21, 2024. Change Healthcare confirmed that consumer’s personally identifiable information was accessed during the attack. For more information about the cyberattack please visit Change Healthcare’s website at [Change Healthcare Cyberattack Support - UnitedHealth Group](#).

Given that personally identifiable information was accessed, OSI urges consumers to protect their information and reduce the risk of identity theft by:

- **Immediately checking your accounts.** Review each of your financial accounts and identify any suspicious activity that may have already occurred.
- **Monitoring your financial accounts and credit reports.** Identity thieves might not use your compromised information right away. Continue to monitor your credit report for signs of suspicious activity. Each of the three nationwide credit bureaus, Equifax, Experian, and TransUnion, provide one free credit report per year.
- **Signing up for free credit monitoring.** Some businesses or government agencies offer free credit monitoring services. Remember, never provide private information without verifying that the service is legitimate.
- **Requesting a fraud alert from one of the credit bureaus.** A fraud alert notifies banks and other creditors to take extra steps to verify your identity before issuing credit in your name. A fraud alert is free and will last 90 days. You can request a fraud alert with one of the three nationwide credit bureaus.
- **Avoiding use of the same password across various accounts.** If your username and password are compromised in a breach, using the same password on other accounts could help a criminal gain access to other accounts that use the same password.
- **Freezing your credit.** A credit freeze or a security freeze blocks a criminal from opening any new accounts or accessing credit in your name. To freeze your credit, you have to contact each of the three credit bureaus individually. A credit freeze is free for you and your children. You can remove the freeze temporarily ahead of a big purchase.

The OSI encourages consumers experiencing healthcare service delays, pharmacy changes or payment issues to contact the OSI at 855-427-5674, option 3.

###