



August 2026

Fraud Advisory: Claim Hijacking and AI-Enabled Phone Scams

The UI Integrity Center is issuing this Fraud Advisory to alert states to claim hijacking activity and AI-enabled phone scams reported by North Dakota. These schemes are especially concerning because bad actors may target valid unemployment insurance (UI) accounts that have already completed identity verification.

Observed Scheme Activity

Claim hijacking - North Dakota observed an uptick in attempts involving access to valid accounts, often connected to social engineering schemes such as romance scams, fictitious job postings, or AI phone scams as mentioned below. The activity targets legitimate North Dakota residents' identities and wage information, rather than fictitious employment created solely to establish UI eligibility.

AI-enabled phone scam - North Dakota reported an AI-driven fraudulent call operation that contacts residents, tells them they have \$4,000 in unclaimed UI benefits, and attempts to collect personally identifiable information. North Dakota detected the activity after residents reported similar calls through the state fraud email inbox and Benefit Payment Control call queue.

The reported call model can engage in conversation, answer generic questions, and repeatedly redirect callers to provide personal information. It speaks rapidly without natural pauses, appears available at all hours, repeats its initial script consistently, and may use an in-state area code to appear legitimate. North Dakota also recently observed the script shift from "unemployment" to "disability," indicating that scammers may adapt the same impersonation approach across benefit programs.

Recommended Actions

- Monitoring changes in bank accounts. North Dakota conducts bank change audits, including enhanced or daily audits when emerging schemes indicate elevated account takeover risk.
- Ensure front-line staff can recognize suspicious calls, account takeover signs, and scam reports, and know how to document and escalate concerns.
- Remind claimants and stakeholders to be cautious of unsolicited calls promising unclaimed UI benefits or asking for personally identifiable information. Encourage them to hang up, avoid calling numbers provided in suspicious messages, and verify any benefit-related communication through official agency websites and published agency phone numbers.

- Share indicators with sister agencies when the script or impersonation target changes, such as a shift from UI to disability or another public benefit program.
- Review Integrity Data Hub crossmatches that indicate a Social Security Number is in use in multiple states within the last year.
- Monitor repeated demographic or account elements, such as banking information, email addresses, and login IDs, while recognizing that bad actors may reuse these elements sparingly as they adapt to state detection metrics.
- Use employer responses received through the notice of claim process to identify fraudulent claims.
- Issue timely public-facing fraud advisories or social media updates that warn claimants and stakeholders about current fraud trends, suspicious benefit-related calls, and safe ways to verify agency communications. Example: [Unemployment for Individuals | Job Service North Dakota](#)
- Coordinate with appropriate partners when fraudulent phone numbers or impersonation scams are identified. Example: Job Service North Dakota contacted the state Attorney General Consumer Protection Department regarding the AI phone scam. When phone-number takedown or enforcement options are limited, prioritize timely public education and stakeholder alerts.
- Document new tactics, technologies, and indicators observed in each fraud occurrence, then update detection rules, staff guidance, and claimant education materials as schemes evolve.

Resources

The UI Integrity Center encourages states to use Library resources to help staff, claimants, and employers recognize fraud and protect information. Examples include resources on identifying fraudsters, social engineering tactics, protecting UI accounts from cyber fraud, and protecting businesses and employees from UI fraud, some of which can be located here: [Fraud Awareness](#) (login required).

Closing Reminder

Fraud attempts will continue to evolve. States should remain vigilant, avoid complacency, and continuously innovate against fraud schemes to stay ahead of bad actors.