IDENTITY THEFT

Kali's Story

OKMM™
OKLAHOMA MONEY MATTERS

Kali didn't have time to wait two hours until her number was called. Nobody ever told her not to keep her kids' Social Security cards in her wallet. They were there for safe keeping, or so she thought. Her cousin had been staying with her for a few weeks and when he left, he took more than he came with, including Kali's children's Social Security numbers. To make things worse, Kali found out the hard way that some of the online sites that offer to help you complete applications for government services aren't always trustworthy. Not only did she get scammed, she paid for a service that's free to the public. And now to add to her misfortune, her cousin shared the children's Social Security information with another party.

"Next, number A37 come to window 14," the overhead speaker blared. Kali looked at her watch and knew there was no way she was going to make it back in time for her shift. Either she had to call in to work or leave without applying for the replacement cards, which meant she couldn't file her taxes. Either way, she was losing time and money.

The Federal Trade Commission's snapshot of 2025 showed the top frauds in the U.S. were reported as:

1	2	3	4	5
Imposters	Online shopping and negative reviews	Investments	Business and job opportunities	Business and wire transfers

Overall, 2.6 million frauds were reported in 2024 and approximately $12.5 billion was reported lost.

Need to report a case of fraud?

Visit **reportfraud.ftc.gov** or **identitytheft.gov**.

Merriam-Webster defines social media as "a form of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos)." A study in 2026 showed there are approximately 5.66 billion social media users around the world, spending 2 hours and 21 minutes daily online.

With so many people sharing their personal information online, the chances that their identity can be comprised is extremely high. This type of malicious activity is known as social engineering. These are a few of the most common types of social engineering attacks:

- **Phishing:** Scammers use targeted email or text messages to trick you into giving them your personal information.
- **Vishing:** Also known as voice phishing, vishing uses the phone to fraudulently steal personal information from its victims.
- **Smishing:** Cybercriminals use this form of identity theft when sending text messages to victims in an effort to mislead them into sharing their personal data.

Kali learned that she should periodically check her credit report to avoid problems with identity theft. She wanted to make sure her cousin hadn't stolen her identity, as well, by opening credit card accounts in her name. Checking your credit report regularly is important and individuals may receive a free credit report every 12 months from **Experian**, **TransUnion** and **Equifax** by visiting **AnnualCreditReport.com**.