NMRLD
NEW MEXICO
REGULATION &
LICENSING DEPARTMENT
Securities Division

ARTIFICIAL INTELLIGENCE, REAL CONSEQUENCES

KEY DEFINITIONS

Deepfakes
Videos or photos that artificially replicate a person doing or saying something

Voice Cloning/Audio Deepfakes
Artificially replicate someone's voice

Caller ID Spoofing
Changing the caller ID information to deceive recipient

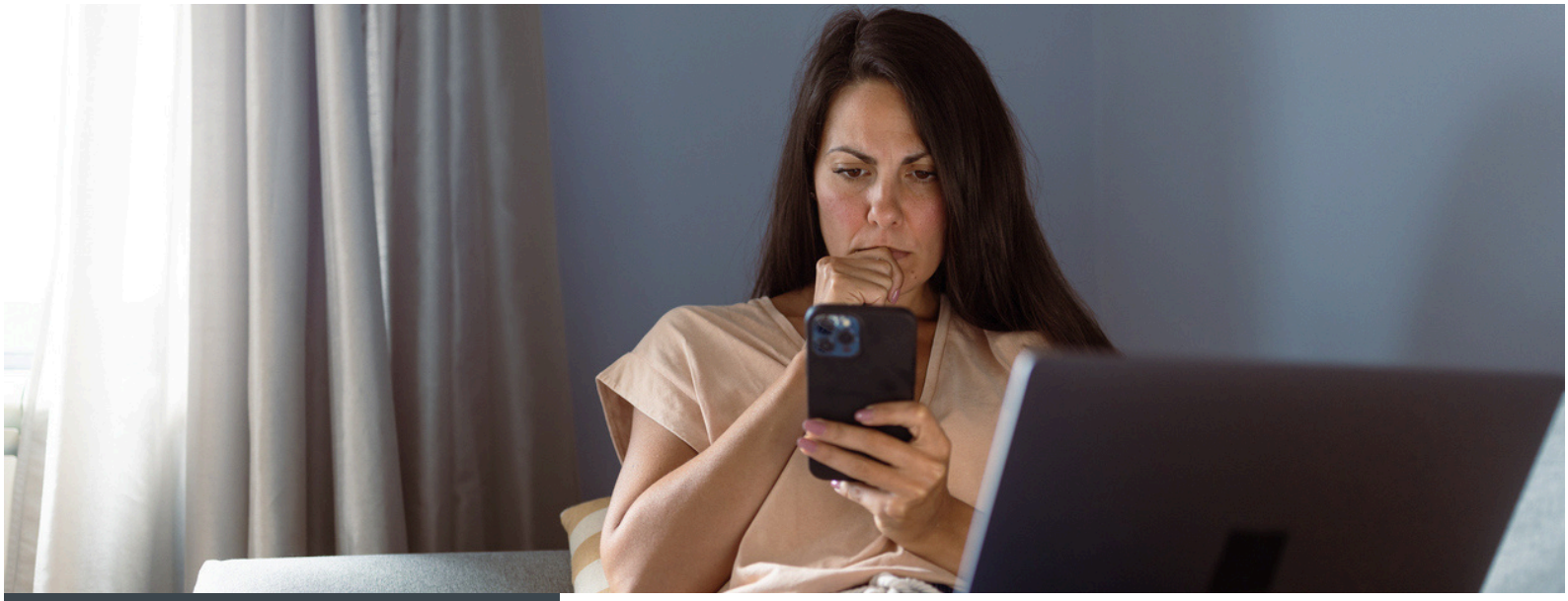
AI IS USED IN SCAMS TO

- Impersonate celebrities, relatives, and friends.
- Impersonate businesses like UPS, FedEx, banks, and Amazon.
- Create fake strangers to con people out of money through romance scams, including the one known as Pig Butchering.
- Impersonate government officials with the IRS, Social Security, and law enforcement.

TYPES OF SCAMS

Audio Deepfakes:
Scammers use voice cloning to impersonate family members ("grandparent scams"), government officials (IRS, police), or friends to demand money. They may also record a target's voice to access accounts with voice recognition. This manipulation is based in psychology and plays off people's fear instinct to reduce good judgment.

Video Deepfakes:
Scammers might use video deepfakes to impersonate family or friends in trouble, just like with the audio version of the scam. They may impersonate celebrities to advertise a fraudulent investment. People have shown to be less likely to suspect fraud when they see a celebrity.



REPORT THE SCAM OR CRIME

Your local police department

New Mexico Department of Justice
https://nmdoj.gov/get-help

U.S. Securities and Exchange Commission
https://www.sec.gov

Internet Crime Complaint Center
https://complaint.ic3.gov

NEW MEXICO SECURITIES DIVISION

Assists with the investigation or referral of cases involving investment fraud

Education on financial fraud prevention

Phone:
1-800-704-5533

Online:
RLD.nm.gov/redflags

HELPFUL TIPS FOR AI SCAM AWARENESS

Verify Identity

Be skeptical of unsolicited calls or messages. Don't trust caller ID, as it can be faked. Look up the official contact details and reach out to confirm the legitimacy.

Establish a "Safe Phrase"

Create a secret phrase with close contacts to confirm their identity during an emergency. Avoid things that can be researched online about you or your family: street names, towns, schools, etc. Always ask for the safe word (or phrase) before transferring any money.

Hang Up and Call Back

If you receive a call requesting payment, hang up and call the person or institution back directly using a number you independently verified.

Be Aware of Red Flags

- Requests for payment via cryptocurrency or cash couriers
- Pressure to act quickly
- Unregistered or unlicensed individuals making claims of high returns with AI
- Glitches in video or audio or other signs of tampering

Protect Yourself

- Let unknown calls go to voicemail to prevent voice cloning
- Keep social media private to limit information scammers can use
- Do research to confirm a celebrity endorsement before buying into it

NMRLD
NEW MEXICO
REGULATION &
LICENSING DEPARTMENT
Securities Division

The federal Securities and Exchange Commission (SEC) maintains a free online database of registered investment advisers. You can look up an investment adviser firm and view the form filed with the SEC containing information about the firm, including information about certain disciplinary events involving the adviser and its key personnel. Finally, check with the New Mexico Securities Division to find out whether an individual is a licensed financial professional in New Mexico and whether he or she has been subject of a past disciplinary action.

Do business only with licensed brokers and financial advisers and report any suspicion of investment fraud to the New Mexico Securities Division. One call can protect your financial security and might prevent others from becoming victims.