ERIK NASARENKO
VENTURA COUNTY DISTRICT ATTORNEY
NEWS RELEASE

Follow us @VenturaCountyDA
vcdistrictattorney.com

Contact: Michael Aguilar
Title: District Attorney Investigator
Phone: (805) 662-1756
Email: Michael.Aguilar@ventura.org

Approved: SW
Date: February 15, 2024
Release No.: 24-014

District Attorney Warns of Emerging Fraud Trends

VENTURA, Calif. – The District Attorney's Office is warning Ventura County residents about emerging trends in fraud schemes that coincide with fast-moving technological advances. Several trends include synthetic identity theft, deepfakes, account fraud takeover, cryptocurrency scams, and insider threats. The Association of Certified Fraud Examiners (ACFE) says 2024 is on pace to be another busy year when combating emerging fraud trends. Having knowledge about these new scams and frauds can be your best defense from becoming a victim.

Synthetic identity fraud is a crime where fraudsters piece together your identity by finding your name, social security number, birthdate, and other personal information to open bank accounts, credit card accounts or commit other financial crimes using your identity. In 2020, there was an estimated $20 billion in financial losses attributed to synthetic identity fraud.

Deepfakes are synthetic media that have been fabricated or manipulated, often by artificial intelligence (AI), to impersonate a real person or an event. AI has entered the fraud landscape as fraudsters make deepfake audio recordings, videos, and documents, to make it appear as if the victim approved a transaction. Deepfakes are also seen when impersonating celebrities to endorse products and services. But the deepfake fraud scheme is not limited to celebrity impersonations and can now be used to impersonate everyday citizens to complete a crime.

Account takeover fraud saw an estimated 74 percent increase in 2021, and is the fastest-growing financial crime. Account takeover happens when a victim's online bank accounts, email, or social media profiles are hacked and taken over. Once this occurs, fraudsters can spread malware, solicit money from others, steal the victim's money, or steal their identity.

Cryptocurrency and cryptocurrency scams are not new in 2024, but the growing trend of cryptocurrency scams include fake cryptocurrency exchanges, phishing emails, and fraudulent

scams where investors are tricked into high returns over short periods of time. Unfortunately, money stolen in cryptocurrency scams is seldom recovered.

Insider threats can cause irreparable damage to businesses and can be very difficult to detect. Prevention is key to not becoming victimized by an employee (insider) with access to sensitive information. Investigators say to stay aware of employee activity and monitor those with access to sensitive information.

“Being aware of fraud trends and scams is one of the best ways to prevent becoming a victim of these technological fraud schemes,” Supervising District Attorney Investigator James Espinoza said. “Just a few extra steps can ensure your account security.”

Investigator Espinoza suggests these simple but effective steps as the best defense to prevent scammers from stealing your money:

- Enable two-factor authentication for all accounts.
- Keep a sharp eye on open and active accounts.
- Close inactive accounts
- Monitor your credit report.

If you believe you are the victim of a fraud scam, immediately change passwords to cut off access to the compromised accounts, and report the suspected scam to your local police department or law enforcement agency.