BANKERS' BANK
OF KANSAS

Compliance Corner

Deepfakes

In February 2024, CNN aired a story about a finance worker who paid out nearly $25 million to a fraudster.[1] You may think, "It can't happen to me because I don't have millions of dollars." The problem is fraudsters want money, and it doesn't have to be millions. If you Google "Deepfake" you can find many articles about this phenomenon from Homeland Security, McAfee Security, ID.me Network, and insurance companies.

In this edition of the Compliance Corner, we will focus FinCEN alert and a public service announcement from the FBI.

The FinCEN alert[2] refers to deepfake fraud schemes that create identities and open accounts to use for fraud. Our focus below is on warning signs or red flags for banks. Some of the warning signs to be aware of for new account fraud include:

1. Inconsistencies among multiple identity documents submitted by the customer.
2. Access to an account from an IP address that is inconsistent with customer's profile.
3. High payment volumes to potentially higher-risk payees, such as gambling websites or digital asset exchanges.
4. A customer declines to use multifactor authentication to verify their identity.
5. A reverse image lookup or open-source search of an identity photo matches an image in an online gallery of generative artificial intelligence produced faces.
6. A customer attempts to change communication methods during a live verification check due to excessive or suspicious technological glitches.

The public service announcement from the FBI[3] goes deeper into generative artificial intelligence (AI) and how it is used to create fictitious text, images, audio, and video. Fraudsters then use these to convince people they are communicating with a "real" person who need money, pretend to be a loved one of a person asking for financial help, create misleading promotional materials for investment fraud schemes, and obtain access to bank accounts using AI. Some of the tips to protect yourself include:

1. Create a secret word or phrase with your family to verify their identity.
2. Look for subtle imperfections in images and videos such as irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, or unrealistic movement.
3. Limit online content of your image or voice, make social media accounts private, and limit followers to people you know.

Deepfakes are not going away and will become progressively more realistic. Make sure to keep yourself and your customers aware of the newest trends and safeguards.

---

[1] Finance worker pays out $25 million after video call with deepfake 'chief financial officer' (CNN) | Read More
[2] FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institution (FinCEN) | Read More
[3] Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud (FBI) | Read More