TruStage™

RISK Alert

Actionable insights for bond policyholders

Awareness | Watch | **Warning**

Deepfake imposter scams introduce new fraud risks

By obtaining images and voice samples from social media, videos, or cold-calling to record a voice, fraudsters can make convincing deepfakes that look and/or sound like someone an individual or employee knows. Combining generative AI's language processing abilities with visual deepfake and voice recreation technologies, there are significant risks for financial institutions due to the heightened level of sophistication to fraud attempts.

Alert details

A significant challenge facing financial institutions today is that methods commonly used to prevent fraud, such as phone or video calls, are now being used by criminals to perpetrate fraud using deepfakes. Advanced applications and technology allow the fraudster to be off camera while the app fully animates the deepfake image on screen.

Deepfakes – often intentionally distorted videos, images, and audio recordings – have been so convincing that bad actors have already used them in social engineering attacks for financial gain. Social engineering frauds using deepfake technology are a new challenge for credit unions as conventional security technologies and member identification protocols are designed to identify impostors - not recognize altered or recorded voices or digitally enhanced and manipulated videos .

Even though some credit unions have pivoted to the use of photographs or "selfies" with government-issued ID's as well as the adoption of voice recognition software for member identification purposes; impostors have been able to use deepfake technologies to successfully bypass these new protocols.

Credit unions may be affected by deepfakes in several ways:

- exploiting member onboarding processes
- creating fraudulent accounts, counterfeit payment or transfer requests
- impersonating key credit union or third-party personnel
- mimicking job candidates

Unfortunately, it appears that every time risk mitigation techniques are tightened up, fraudsters seem to find a workaround.

Date:
December 19, 2023

Risk category:
Fraud; scams; deepfakes; artificial intelligence (AI); social engineering

States:
All

Share with:

- Branch operations
- Executive management
- Front-line staff/tellers
- Human resources
- IT
- Member services/new accounts
- Risk manager
- Transaction services

Facing risk challenges?:
Schedule a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

As credit unions continue to widen digital capabilities, offerings, and online presence to cater to a more diverse membership and distributed workforce; it is equally important to consider mitigating strategies against the financial and reputational damages deepfakes pose as an emerging threat.

Detection tools are improving, but so are deepfakes themselves. Likely solutions will blend technology, internal controls/business practice changes, and broad public awareness.

Risk mitigation

At this early-stage complete mitigation against the threat of deepfakes is unlikely, early detection can minimize the impact to your organization. Credit unions should consider:

- Deploy multifactor authentication across financial institution networks and consider enhanced measures for authentication. Examples could include issuing tokens or physical devices for authentication.
- Consider the use of biometrics (or physical characteristics) for authentication. Biometrics can be a fast and convenient solution to verify customers as this type of data is unique, nontransferable, and hard to fake or steal. However, financial institutions should also be aware of the increasing number of state laws regulating the use of biometrics and ensure they are complying with those regulations.
- Ensure a clearly-defined and distributed response protocol is in place. Much like an incident response plan, individual responsibilities and required actions should be defined in this plan to minimize the financial and reputational impact.
- Explore artificial intelligence (AI) and liveness detection software to identify and alert your staff to potential attacks.
- Implement employee training and awareness as a critical component and an additional line of defense in a credit union's deepfake mitigation strategy.

  Training programs should be centered on how the technology is leveraged in various malicious attempts, detection techniques, and enable reporting protocols for employees to bring forth concerns related to a deepfake-based social engineering attempt.
- Inform members of potential scams. If a member suspects they are being targeted by a deepfake scammer, ask the member to stand up and move around or wave their hand in front of their face.

Risk prevention resources:

Access the Business Protection Resource Center for exclusive risk and compliance resources (User ID and Password required).

- Call center fraud risk overview
- Fraud & scams eBook
- Common member scams risk overview
- New account fraud risk overview
- Business email compromise & fraudulent instruction
- For additional RISK Alerts related to fraud and scams, go to the RISK Alerts Library and enter the keyword "scams" or "fraud" into the search field.

For additional support, call 800.637.2676 or email riskconsultant@trustage.com