RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type Awareness | Watch | **Warning**

Preparing For The Risk of Deepfakes

Deepfakes are digitally-altered images, videos, or audio recordings that when using certain technologies, can convincingly make it appear an individual said or did something they didn't do. Initially used to impersonate politicians, celebrities, and other well-known individuals; the technology has become increasingly available to fraudsters and other bad actors and deepfakes are now being used for fraudulent financial gain.

Details

Artificial intelligence (AI) is enabling new, more sophisticated forms of digital impersonation. And, the next big financial crime might involve deepfakes - video or audio clips - to create false depictions of real people.

Deepfakes - intentionally distorted videos, images, and audio recordings - have developed to be so convincing that bad actors have already employed 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.

Analysts report the cost associated with deepfake scams in 2020 to be more than $250 million. In one instance, a European energy firm's CEO was scammed over the phone when he was instructed to transfer funds by an individual who used audio deepfake technology to mimic the voice of the firm's chairman.

As 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 can use deepfake technologies to successfully bypass these new protocols.

While deepfakes are not the biggest financial deception threat, credit unions may be affected by deepfakes in several ways including the subversion of member onboarding processes, the creation of fraudulent accounts, counterfeit payment or transfer requests, and the impersonations of key credit union personnel.

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.

Date: February 2, 2020

Risk Category: Cybersecurity; Scams; Internal Controls

States: All

Share with:

- ☐ Executive Management
- ☐ IT
- ☐ Members Services / New Accounts
- ☐ Risk Manager

77%

of 100 cyber security decision-makers in the financial services sector are worried about the potential for deepfake technology to be used fraudulently – with online payments and personal banking services.

Source: iProov, Deepfakes: The Threat to Financial Services Report, 2020

Risk Mitigation Tips

Although 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:

- 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.
- 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.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk resources to assist with your loss control. The Protection Resource Center requires a User ID and password. When in the Resource Center, resources related to cyber fraud and scams are typically found within the Cybersecurity, Consumer Payments, and Deposit Account Services section of the Loss Prevention Library.

Attend our **Cybersecurity Office Hours** on **Wednesday, February 17, 2021**, where you'll have the opportunity to hear from Carlos Molina, CUNA Mutual Group Senior Risk Consultant, and Derek Laczniak, Director Cyber Practice from M3 Insurance, as they discuss the latest cyber trends and risks. **Register now** for this no-cost session.

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.

Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.