Deepfakes Are Increasing – Top Three Scams To Watch

cyber security risk management social media

Summary: Deepfakes have been around for a while, but they are now increasing dramatically with costly effects. Deepfakes are fabricated pictures, videos, or audio using advanced technologies to replace a person in an image or alter a person's voice. Let's explore the latest insights from industry experts, how much damage deepfakes are causing, and how to protect your institution from three related scams.

The word "fake" with its meaning of bogus or counterfeit, first surfaced around 200Ys ago. Believe it or not, it was captured in a dictionary of criminal slang, which was put together by James Hardy Vaux in 1819. Interestingly, Vaux was a former criminal that became familiar with this type of slang, while spending time in British penal colonies in Australia.

Deepfakes are the latest in criminal wrongdoing and they are spreading quickly. We explore what they are, the monetary damage they can cause, what the experts are saying, and give you three deepfake scams to steer clear of.

What are deepfakes?

According to SentinelOne, a cybersecurity startup, "*A Deepfake is the use of machine ("deep") learning to produce a kind of fake media content – typically a video with or without audio – that has been 'doctored' or fabricated to make it appear that some person or persons did or said something that in fact they did not.*" So basically, a deepfake is an existing image, video, or audio recording where a person is replaced by someone else.

Even before the pandemic and urgent move to digital, there were 15K deepfake videos online in 2019. According to Deeptrace, a cybersecurity company, the number of deepfake videos increased twofold from 2018 to 2019. As consumers and businesses alike have become more dependent on technology, the risk of deepfakes increases.

Cybercriminals use a plethora of technologies, including artificial intelligence, to mimic specific people in video, pictures, or audio in deepfakes and convince customers to fall for a scam. The effect can be severe for many businesses. These types of misinformation have been estimated to cost businesses $78B annually. The use of this highly-believable, counterfeit audio, pictures, and video to enable financial fraud is not only growing — it is becoming increasingly difficult to spot and root out.

What the industry experts say

David Blaszkowsky, head of strategy and regulatory affairs for Helios Data, says that deepfakes are really a "worst-case" scenario, because virtually all protection dependent on visual or audio metrics can be cracked. "*One by one, all the 'unique' metrics that protect access to data and accounts are being wiped out, like*

antibiotics against ever-mutating infectious diseases," he says. "*It has always been easy to fool human 'gate-keepers'. But with deepfakes it is easier than ever to fool the computers, too.*"

Indeed, the rapidly increasing sophistication of today's financial deepfake scams suggests that community financial institutions (CFIs) and their customers need a more heightened awareness of the threats these bad actors could pose. "**It is not outlandish to think that it will be used in ways for cyberattacks that we're not even expecting right now,**" according to Nick Santora, CEO of security awareness training solution, Curricula.

With that warning, it is critical to continue with robust governance processes and cyber hygiene, such as layered security, rigorous staff training, and careful monitoring of people, networks, and data sources for anomalies. Continuing with these procedures and practices ensures well-drilled security teams can swing into action quickly, when necessary.

Here are **three deepfake-related scam areas** that CFIs might face and how to fight them:

1. **Selfie identification.** The use of selfies for identification is rising, especially with online account opening. However, this is an area vulnerable to deepfake photos, with cybercriminals posing as someone else to open accounts for money laundering or even access current accounts. Make sure that your institution's know-your-customer (KYC) procedures are updated with extra controls, if selfie IDs are accepted.
2. **Voice authentication.** Voice authentication is one way to use biometrics for multifactor authentication. While this can be a very effective way to authenticate a customer, with deepfakes, audio can be altered to sound like a customer's voice. Make sure that your security systems are reinforced to uncover any anomalies or red flags in voice authentication measures.
3. **Social media videos.** For some CFIs with high-visibility CEOs or other executives, there may be deepfake danger through social media. If a cybercriminal wanted to create chaos and damage a financial institution's reputation, it could post a video with an executive making a fake announcement about branches closing or mismanagement of funds. Technologent Senior Solutions Architect Jason DeJong brought up the former example in an article last year for ATM Marketplace. Diligently use "watching" and "listening" tools on social media to flag any fraudulent activity and allow you to promptly shut it down.

Deepfakes will become more sophisticated as technology advances. So, stay on top of the latest scams and fraud ploys, while ensuring your cybersecurity is at its optimal level.

FLEXIBLE SOLUTION TO FIT YOUR CECL NEEDS TODAY AND TOMORROW

We know that not every banker has the same needs. So CECL FIT® is flexible to adapt to fit your portfolio. Start small with CECL FIT at the basic tier and you can grow into a larger tier, if you need to later. Learn more about our CECL FIT solution.

ECONOMY & RATES

Rates As Of: 02/28/2022 06:38AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.33	0.11	0.27
6M	0.71	0.22	0.52
1Y	1.05	0.27	0.67
2Y	1.48	0.32	0.77

5Y	1.78	0.19	0.54
10Y	1.90	0.13	0.40
30Y	2.23	0.14	0.34
FF Market		**FF Disc**	**IORB**
0.08		0.25	0.15
SOFR		**Prime**	**OBFR**
0.05		3.25	0.07