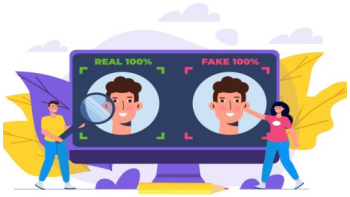
ST. KITTS BRANCH
Financial Services Regulatory Commission

NewsLetter

January 2023
Issue No. 104

THE 411 ON DEEPFAKE: A THREAT TO FINANCIAL INSTITUTIONS



INTRODUCTION

Deepfake Technology has been used in the entertainment industry for decades. Recently, however, there have been a number of reports of this technology being used for illicit purposes. In May 2022, Tesla's Chief Executive Officer (CEO), Elon Musk's face and voice were used by criminals to create a video using deepfake technology to encourage persons to invest in a fake crypto exchange called "BitVex" promising 30% returns to investors. Mr. Musk issued a formal statement indicating that the video was indeed a scam. This is just one example of the many deepfake scams linked to fraud. This Newsletter delves into the world of Deepfake Technology and provides insight as to the risks posed by Deekfake Technology to Financial Institutions (FIs) as well as ways to protect FIs from potential exploitation by cybercriminals and cyberthreats using Deepfake Technology.

WHAT IS A DEEPFAKE?

A Deepfake is a type of Artificial Intelligence (AI) that uses artificial images or sounds along with machine learning algorithms to manipulate visuals and/or other audio content to create fake images. Additionally, a deepfake can be used to make real people appear to say or do things that they neither said nor did. Criminals can use a deepfake to spread misinformation, commit fraud or conduct extortion scams and identify theft.

HOW IS A DEEPFAKE CREATED?

To create a Deepfake, software technology is required. Most Deepfakes are made on high-end desktops however, now with automated computer graphics and machine learning systems, they can be made quickly and cheaply, even on standard computer systems. With enhanced general design software, criminals only now need a handful of photos or videos to create a 'legitimate-looking' Deepfake.

WHY SHOULD FIs BE AWARE OF DEEPFAKE TECHNOLOGY?

Deepfakes can be used for a range of criminal activities within FIs especially as verification procedures, onboarding and communication are becoming increasingly reliant on digital technology. Deepfakes can be used in email scams, phone calls and biometric verification. As a result, employees can be manipulated into believing that their manager or client is requesting them to conduct actions such as the transfer of funds. It is therefore important for FIs to be aware of the risk of Deepfake Technology potentially targeting their institutions and establish appropriate mechanisms and internal controls to mitigate these risks.

- Deepfakes can cause national security concerns when used to commit fraud and steal personally identifiable information; and
- They could also potentially be used in money laundering schemes.

DID YOU KNOW?

According to a report in *The Wall Street Journal* (September 2019), the CEO of an unnamed UK-based energy firm believed he was on the phone with his boss, when he followed the orders to immediately transfer $243,000 to the bank account of a Hungarian supplier. The voice belonged to a fraudster using AI voice technology to fool the CEO. Rüdiger Kirsch of the firm's insurance company explained that the CEO recognized the subtle German accent in his boss's voice and moreover, that it carried the man's "melody." According to Kirsch, the unidentified fraudster called the company three times: the first to initiate the transfer, the second to falsely claim it had been reimbursed and a third time seeking a follow-up payment. It was at this point that the victim grew skeptical. He could see that the purported reimbursement had not gone through and he noticed that the call had been made from an Austrian phone number.

HOW CAN DEEPFAKE TECHNOLOGY BE USED TO EXPLOIT FIs?

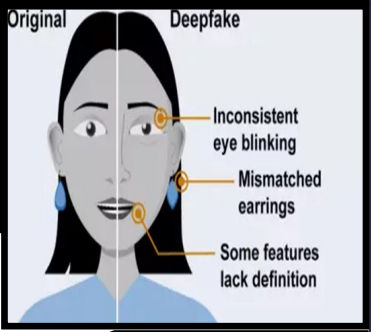
- ◊ Synthetic identity fraud to create a new identity
- ◊ Open bank accounts under false identities to evade sanctions screening or Politically Exposed Person (PEP) requirements
- ◊ Email Hacking
- ◊ Extortion and Blackmail
- ◊ Hide terrorist travel and funding activities
- ◊ Forge passports for human trafficking and smuggling
- ◊ Corruption and Bribery involving political systems and persons
- ◊ Commit fraudulent transactions or steal customer funds
- ◊ Open accounts under fake customer details to launder money through them
- ◊ Evade biometrics

IDENTIFYING SUSPICIOUS ACTIVITY RELATED TO DEEPFAKES

There are various ways to protect an FI from potential exploitation by cybercriminals using Deepfakes. Basic signs to look for when identifying Deepfakes include different intonations in voice, unnatural eye movement or facial expressions, awkward head or body positioning, artificial looking skin, odd lighting or discolouration, bad lip syncing or digital background noise.

In addition to looking for red flags within the manipulated video or image, it is also important to understand the red flags relative to communication. These include the following:

Secrecy: Asking to not disclose requests to others.	Urgency: Asking to take immediate action.	Suspicion: The transaction does not seem normal.



PREVENTING DEEPFAKE ATTACKS

If an FI falls victim to Deepfake attack, it may not only hurt the institution, but it leaves the customers and employees at that institution vulnerable. To protect customer funds and identities and to avoid reputational risk, it is vital to safeguard the institution against cybercriminals using deepfake technologies to exploit systems and manipulate individuals.

Implementing appropriate education and training programs, enhancing customer verification and identity procedures and working with compliance and financial crime analysts are crucial to combatting deepfake activity. CEOs and senior management are most often the targets of attacks since they have access and permission to move large sums of money. It is therefore important to develop and implement cybersecurity protocols as well as to include risks associated with deepfake technology in the institution's risk assessment to enhance its risk-based approach. The institution can:

- ⇒ Download browser extensions to help identify manipulated videos and images;
- ⇒ Use tools to check email breach data to determine if the email address has been compromised; and
- ⇒ Check IP address locations to see if they match known customer locations or addresses.

DID YOU KNOW?

In 2020, a Bank's manager was tricked into transferring US$35 million to an attacker's controlled account because a cybercriminal used deepfake technology to duplicate the voice of the company's Director. The cybercriminal also sent emails from the Director and a lawyer hired to close the acquisition to aid in the fraudulent transaction.

Sources:

1. https://www.acamstoday.org/deepfake-101-a-threat-to-fis/
2. https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=271663aa2241
3. https://www.gao.gov/blog/deconstructing-deepfakes-how-do-they-work-and-what-are-risks
4. https://www.outlookindia.com/business/criminals-use-elon-musk-s-deepfake-video-to-dupe-crypto-investors-crypto-market-rises-news-198403

Happy New Year

To each of our regulated entities, we hope that 2023 brings many successes and achievements.
Our best wishes to you!
May this New Year continue to strengthen the bond of mutual trust and respect
that we have for each other!

From the Board of Commissioners, Management and Staff of the Financial Services Regulatory Commission

Happy New Year

South Independence Square Street, P.O. Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591 Fax: (869) 466-5317
Website: www.fsrc.kn / Email: info@fsrc.kn