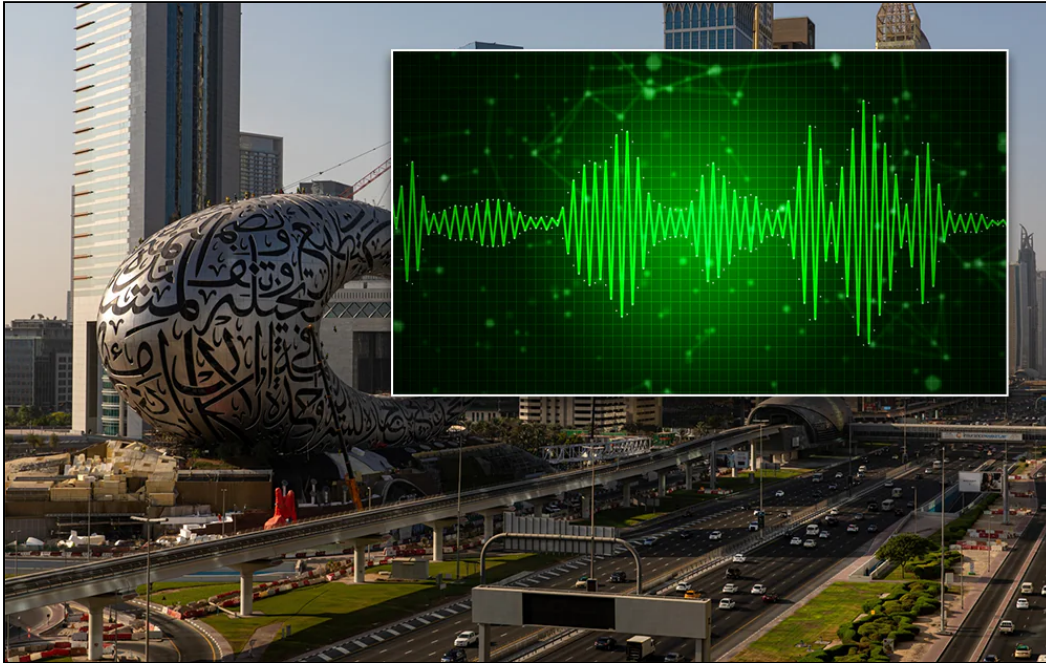


Deepfaked Voice Enabled \$35 Million Bank Heist in 2020

Originally published at <https://www.unite.ai/deepfaked-voice-enabled-35-million-bank-heist-in-2020/>



An investigation into the defrauding of \$35 million USD from a bank in the United Arab Emirates in January of 2020 has found that deepfake voice technology was used to imitate a company director known to a bank branch manager, who then authorized the transactions.

The crime took place on January 15th of last year, and is outlined in a [request](#) (PDF) by UAE to American state authorities for aid in tracking down a portion of the siphoned funds that were sent to the United States.

The request states that the branch manager of an unnamed victim bank in UAE received a phone call from a familiar voice, which, together with accompanying emails from a lawyer named Martin Zelner, convinced the manager to disburse the funds, which were apparently intended for the acquisition of a company.

The [request](#) states:

'According to Emirati authorities, on January 15, 2020, the Victim Company's branch manager received a phone call that claimed to be from the company headquarters. The caller sounded like the Director of the company, so the branch manager believed the call was legitimate.'

'The branch manager also received several emails that he believed were from the Director that were related to the phone call. The caller told the branch manager by phone and email that the Victim Company was about to acquire another company, and that a lawyer named Martin Zelner (Zelner) had been authorized to coordinate procedures for the acquisition.'

The branch manager then received the emails from Zelner, together with a letter of authorization from the (supposed) Director, whose voice was familiar to the victim.

Deepfake Voice Fraud Identified

Emirati investigators then established that deepfake voice cloning technology had been used to imitate the company director's voice:

'The Emirati investigation revealed that the defendants had used "deep voice" technology to simulate the voice of the Director. In January 2020, funds were transferred from the Victim Company to several bank accounts in other countries in a complex scheme involving at least 17 known and unknown defendants. Emirati authorities traced the movement of the money through numerous accounts and identified two transactions to the United States.'

'On January 22, 2020, two transfers of USD 199,987.75 and USD 215,985.75 were sent from two of the defendants to Centennial Bank account numbers, xxxxx7682 and xxxxx7885, respectively, located in the United States.'

No further details are available regarding the crime, which is only the second known incidence of voice-based deepfake financial fraud. The first took place nine months earlier, in March of 2020, when an executive at a UK energy company was harangued on the phone by what sounded like the employee's boss, demanding the urgent transfer of €220,000 (\$243,000), which the employee [then transacted](#).

Voice Cloning Development

Deepfake voice cloning involves the training of a machine learning model on hundreds, or thousands of samples of the 'target' voice (the voice which will be imitated). The most accurate match can be obtained by training the target voice directly against the voice of the person who will be talking in the proposed scenario, though the model will be 'overfitted' to the person who be impersonating the target.

The most active legitimate online community for voice cloning developers is the [Audio Fakes](#) Discord server, which features forums for many deepfake voice cloning algorithms such as Google's [Tacotron-2](#), [Talknet](#), [ForwardTacotron](#), [Coqui-ai-TTS](#) and [Glow-TTS](#), among others.

Real-Time Deepfakes

Since a phone conversation is necessarily interactive, voice cloning fraud cannot reasonably be effected by 'baked' high-quality voice clips, and in both cases of voice cloning fraud, we can reasonably assume that the speaker is using a live, real-time deepfake framework.

Real-time deepfakes have come into focus lately due to the advent of DeepFaceLive, a real-time implementation of popular deepfake package DeepFaceLab, which can superimpose celebrity or other identities [onto live webcam footage](#). Though users at the Audio Fakes Discord and the DeepFaceLab Discord are intensely interested in combining the two technologies into a single video+voice live deepfake architecture, no such product has publicly emerged as yet.

Writer on machine learning, domain specialist in human image synthesis. Former head of research content at Metaphysic.ai, until its dissolution into DNEG's Brahma.ai.

Portfolio site: martinanderson.ai

Contact: martin@martinanderson.ai

