AIRNITE

ZERO DAY

ISSUE 19/2026 · AI

The fake CFO on the video call: how deepfakes stole 25 million dollars

An employee of engineering firm Arup in Hong Kong transferred around 25 million US dollars – after a video call with a fake CFO and fake colleagues. How deepfake fraud works and how Germany's BSI advises companies to protect themselves.

Published: 21 November 2026 Reading time: 5 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

HK$200m
amount transferred
around US$25.6 million (Fortune)

15+
transfers
to five bank accounts in Hong Kong (Fortune, CFO Dive)

0
internal systems compromised
according to an Arup spokesperson (Fortune)

Training
key countermeasure
awareness of those at risk according to the BSI; technology offers no complete protection

A video call with the CFO and several colleagues, a confidential transaction, clear instructions: for an employee of British engineering firm **Arup** in Hong Kong, everything looked like a normal working day in early 2024. In the end, he had transferred around **25 million US dollars** to fraudsters. None of the people on the call were real.

// What happened?

According to Fortune and CFO Dive, citing Hong Kong police and the Financial Times, an employee received a message supposedly from the UK-based **CFO** about a "confidential transaction". He then joined a video conference in which the CFO and other colleagues appeared – all **deepfakes**. He subsequently transferred a total of **200 million Hong Kong dollars**, around US$25.6 million, in more than 15 transactions to five accounts in Hong Kong.

He only noticed the fraud when he checked with headquarters. According to CFO Dive, Arup reported the case to police in January 2024; the police made it public in February without naming the company, and Arup was identified as the victim in May 2024. According to Fortune, a spokesperson confirmed that fake voices and images were used; **internal systems were not compromised**.

// How does the attack work?

The attack needs no malware and no network intrusion. It targets people, not systems. AI tools generate deceptively real voices and faces from publicly available material. Combined with time pressure, confidentiality and the authority of superiors, a situation arises in which asking questions becomes difficult.

Germany's BSI describes exactly this scenario as **CEO fraud**: an attacker calls using the cloned voice of a manager to trigger a transfer. According to Fortune, Arup's CIO Rob Greig said attempts to defraud companies had risen sharply; it is an issue for the whole industry, business and society.

// Who is affected?

Every company in which employees can trigger payments is affected – and in which superiors appear publicly with their face and voice, for example in videos, interviews or talks. Finance departments, executive assistants and foreign subsidiaries, where headquarters is often present only by video anyway, are particularly at risk.

// What should you do now?

The BSI names **awareness and training** of those potentially affected as a key measure. According to the BSI, technical detection of deepfakes is not reliable under all conditions, and countermeasures generally offer no complete protection. Processes are therefore decisive: a four-eyes principle for payments, call-backs via known numbers, control questions – and a culture in which double-checking with the boss is allowed and welcome. The checklist below sums up the steps.

// How does Airnite help?

In **training**, Airnite gives management, finance and assistants hands-on practice in recognising deepfakes and CEO fraud. In **consulting**, we review payment approval processes and communication channels with you. With agreed **simulations** as part of security tests, we show where processes are still vulnerable today.

> Note: the information on the Arup case comes from press reports; we were unable to view a primary source from Hong Kong police or Arup directly. Research status: 21 November 2026.

Checklist: what to do now

[+] Define a four-eyes principle for unusual or urgent payments that no one can override by phone or video call.

[+] Make a call-back via a known, internally stored number mandatory before money flows – never via contact details from the request.

[+] Agree on an internal code word or control question for confidential instructions from management.

[+] Train management, finance and assistants specifically on deepfakes and CEO fraud.

[+] Explicitly encourage staff to double-check even “instructions from the boss” – without fear of negative consequences.

[+] If in doubt, immediately inform the bank, the police and internally the management via a second channel.

How Airnite helps

- Training – Your team learns our tools and processes.
- Consulting – An outside view of your plans and projects.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.

Would your team spot a fake boss?

Airnite trains management, finance and assistants on CEO fraud with fake voices and videos and reviews payment approval processes with you. On request, we test the processes with realistic, agreed simulations.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/deepfake-ceo-fraud-video-call/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **BSI · Deepfakes – Gefahren und Gegenmaßnahmen** · PRIMARY SOURCE
   Primary source (authority): CEO fraud with cloned voice, countermeasures, limits of detection
   https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
2. **Fortune · A deepfake 'CFO' tricked the British design firm behind the Sydney Opera House in $25 million scam** · 17 May 2024
   Business press: amount, sequence, statements by Arup
   https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/
3. **CFO Dive · Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'** · 17 May 2024
   Trade press (citing the Financial Times): first contact, accounts, timeline
   https://www.cfodive.com/news/deepfake-scam-engineering-firm-arup-25-million-fraud-hong-kong-cfo/716501/

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de