Arup deepfake video-call fraud

IMPLEMENTED 2024 · PROFESSIONAL SERVICES · HONG KONG · BAND F · PARTLY PROVED
VERSION 1.0 · PUBLISHED 17 NOVEMBER 2026 · UPDATED 17 NOVEMBER 2026 · FACTS CHECKED 17 NOVEMBER 2026

Fraudsters used AI-generated faces and voices of senior Arup staff on a video call to persuade a finance employee in Hong Kong to make 15 transfers. Arup confirmed in May 2024 that it was the company involved.

ABOUT THIS SYNOPSIS

This is MarLuc's summary and grading of publicly available sources, for information only. It is not investment, legal, financial or professional advice, and should not be relied on for any decision. Readers must validate it against the original sources and, where appropriate, challenge its conclusions.

Facts and figures are as reported by the sources listed below, which may be incomplete, self-reported or out of date. Check the original source before relying on any figure.

The impact band, proof marker and SEAM view are MarLuc's opinion. The organisation is not a MarLuc client and has not reviewed or endorsed this synopsis. Names and trademarks belong to their owners.

NOTICE WORDING LAST UPDATED 16 NOVEMBER 2026

AT A GLANCE

What went wrong: Fraud; Weak oversight or controls.

AI used: Generative AI used against the organisation: deepfake video and voices of senior staff on a multi-person video conference.

Implemented: 2024. Grade: band F, Failure, Partly proved.

Headline result, as reported: A finance employee in Hong Kong transferred HK$200 million after a video call with deepfakes of senior staff, per Hong Kong police; Arup confirmed it was the victim in May 2024

1 · The case

The facts, as reported by the 5 sources listed at the end. Where a source is silent, the field says "Not reported".

Organisation

Arup. Design and engineering consultancy based in London, with about 18,500 employees in 34 offices, per CNN. The fraud targeted a finance employee in its Hong Kong office. Canvas block: 8. Governance and risk. Also 4. Operations and process, 5. People and skills.

Business challenge

The challenge. Arup's global chief information officer said its operations are subject to regular attacks, including invoice fraud, phishing scams, WhatsApp voice spoofing and deepfakes, and that their number and sophistication had been rising sharply.

Who implemented it

Not an AI deployment by Arup: the deepfakes were made and used by the fraudsters.

Technology (SEAM pillar E)

SEAM types: not established; the sources do not say how the system works. Deployment: Not reported. Vendors and products: Not reported.

Where it was built in: Not an Arup deployment: fraudsters used fake voices and images of senior staff on a video conference call to instruct payments.

What changed

Before: a finance employee acted on payment instructions given in what appeared to be a video call with senior colleagues. After: Arup reported the fraud, told staff to stay alert to such attacks and spoke publicly to raise awareness. Changes to payment approval or verification: Not reported. [1] [2] [3] [4] [5]

Cost of failure

HK$200 million (about US$25.6 million, or £20 million) transferred to fraudsters, per Hong Kong police as reported by CNN and The Guardian. Arup did not give details, citing the ongoing investigation, and said its financial stability and business operations were not affected. Recovery of funds: Not reported.

What it saved

Not reported [1] [2] [3] [4] [5]

Governance and control

Arup notified Hong Kong police and said none of its internal systems were compromised. Its East Asia regional chairman told staff in a memo to stay alert to scammers' techniques. Its chief information officer later said Arup checked whether systems, clients or data were at risk and found none compromised. Owner of payment controls and changes made after the incident: Not reported.

S2 · Accountable owner · Not reported

Not reported. Arup's global chief information officer spoke for the company after the incident; ownership of payment controls is not reported. [2]

A1 · Safe use · Evidenced

After the incident, a memo from Arup's East Asia regional chairman, seen by CNN, told staff to stay informed and alert about how to spot scammers' techniques. [1]

A2 · Human in the loop · Missing (independent source shows it was absent)
Per Hong Kong police, the employee made 15 transfers after the call, and the fraud was discovered only when the employee later checked with head office. [2] [3]

A3 · Monitoring and assurance · Claimed
Arup said none of its internal systems were compromised; its chief information officer later said it assessed whether systems, clients or data were at risk and found none compromised. [2] [5]

A4 · Vendor AI · Not reported
No AI vendor involved; the AI was used by the fraudsters.

A5 · Agent controls · Not reported
No agents described.

A6 · Standards and regulation · Outside scrutiny (a regulator, court, auditor or similar body acted)
Hong Kong police investigated the case as obtaining property by deception; in May 2024 they said no arrests had been made and the investigation was ongoing. [2]

What worked, what did not, what is unproven

WORKED

– Arup reported the incident to police in January 2024 and later spoke publicly to raise awareness, by its account.

– No internal systems were compromised and business operations were not affected, by Arup's account.

DID NOT

– The employee's early suspicion of phishing was set aside after a video call in which other participants looked and sounded like colleagues, per Hong Kong police.

– The fraud was discovered only when the employee later checked with head office, per Hong Kong police as reported by CNN.

– No arrests in the case had been made by May 2024, per Hong Kong police.

UNPROVEN

– Whether any of the money was recovered: Not reported.

– What Arup changed in its payment controls after the incident: Not reported.

– Whether anyone has since been charged: Not reported.

Timeline

Jan 2024 Arup notifies Hong Kong police of the fraud [1]

Feb 2024 Hong Kong police describe the deepfake video-call fraud without naming the company [3]

May 2024 Arup confirms it was the company involved and that fake voices and images were used [2]

May 2024 Police say no arrests so far and the investigation is ongoing [2]

Aug 2025 FM magazine relays Arup's chief information officer: the company reviewed the incident and found no systems, clients or data compromised [5]

2 · Grade and SEAM assessment

MarLuc's opinion, made on the evidence above. How cases are graded: marluc.co.uk/case-studies/how-we-rate

Level of change and impact

Claimed: Not applicable. Grade: F, Failure. Proof: Partly proved. Level of change: Not graded.

No level assessed: band F, a fraud in which AI-generated faces and voices were used against the organisation. The harm came from deception exploiting a payment process, not from AI the organisation deployed.

Band F: money was lost to a fraud carried out with deepfake video and voice. Marked Partly proved because the Hong Kong police and Arup both confirm the fraud and the use of fake voices and images, but there is no court finding and Arup has not confirmed the amount.

The SEAM view and lessons learnt

Per the police account, an employee made 15 transfers on instructions given in a video call, and the check with head office came only afterwards. The AI here was the attackers' tool, and its effect cannot be separated from the payment process it exploited: trust in familiar faces and voices replaced an independent check. Before relying on calls or video for payment approval, a leadership team should ask which payments need confirmation through a separate, known channel, and who can release large sums without it.

1. Require confirmation through a separate, known channel before any large or unusual payment.
2. Train finance staff that faces and voices on a call can be faked.
3. Report incidents to police quickly and share the lessons across the organisation.

Evidence

Score 3 of 4. Independent: Hong Kong police statements reported by CNN and The Guardian, with Arup's own confirmation; no court finding.

Evaluation method. Police account and company statement: the police briefing of February 2024 and Arup's statement of May 2024, as reported by the press.

Sources disagree. Reports give the loss as US$25 million, US$25.6 million or £20 million, each converting the police figure of HK$200 million. CNN's reports of the police briefing refer to the employee as 'he'; the Hong Kong police statement quoted by The Guardian says 'she'.

Status. Open: in May 2024 Hong Kong police said no arrests had been made and the investigation was ongoing. Later outcome: Not reported.

3 · Original sources

Read these in full. To challenge a fact or a grade, use the contact form at marluc.co.uk or the link on https://marluc.co.uk/case-studies/arup-hong-kong-deepfake-video-call-fraud

[1] CNN: British engineering giant Arup revealed as $25 million deepfake scam victim (May 2024)
https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

[2] The Guardian: UK engineering firm Arup falls victim to £20m deepfake scam (May 2024)
https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video

[3] CNN: Finance worker pays out $25 million after video call with deepfake 'chief financial officer' (February 2024)
https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

[4] Building: Arup named as victim of £20m deepfake scam (May 2024)
https://www.building.co.uk/news/arup-named-as-victim-of-20m-deepfake-scam/5129479.article

[5] FM magazine: How accountants can combat the rising threat of deepfake fraud (August 2025)
https://www.fm-magazine.com/issues/2025/aug/how-accountants-can-combat-the-rising-threat-of-deepfake-fraud/

Arup website: https://www.arup.com

Version 1.0 · Published 17 November 2026 · Updated 17 November 2026 · Facts checked against sources 17 November 2026 · Downloaded 26 November 2026. This PDF may be out of date: the latest version, and a way to report an error or a better source, is at https://marluc.co.uk/case-studies/arup-hong-kong-deepfake-video-call-fraud

VERSION HISTORY

v1.0 17 November 2026 First published