

Trusted Voice for CxO Fraud

It sounded exactly like your CFO. It wasn't.

How guaranteed number identity closes the gap that voice cloning and caller ID spoofing have opened in executive impersonation fraud.

For CFOs, treasurers, finance directors, internal audit and executive teams

Published by

Trusted Voice a trademark of Trusted B.V.

Stadhuisplein 10, Eindhoven • www.trustedvoice.eu

August 2026

You picked up the phone. It was your CFO. It wasn't.

Your controller gets a call. The caller ID shows the CFO's direct line, the same number saved in their contacts for years. The voice on the line is unmistakable: the same pace, the same slight accent, even the same habit of clearing his throat before getting to the point. He explains, with the usual urgency, that a confidential acquisition requires an immediate wire transfer, and asks the controller to keep it quiet until the deal is announced. The controller, trained to be responsive to leadership and reluctant to question a superior twice, complies.

The CFO never made that call. The number was spoofed. The voice was synthetic, built from a few minutes of audio pulled from an earnings call, a conference keynote, or a video posted online. The money is gone within the hour, routed through accounts that are emptied before anyone thinks to verify.

This is CxO fraud in 2026: not a clumsy email with a typo and a strange sender address, but a phone call, or a video call, that sounds and looks exactly like the person your employees are trained to trust and act on without hesitation.

From a misspelled e-mail to an indistinguishable voice

CxO fraud, also known as CEO fraud, executive impersonation or whaling, is not new. For over a decade, criminals have posed as a company's CEO or CFO by e-mail, asking a finance employee to make an urgent, confidential payment. Traditional CEO fraud already cost Dutch companies dearly: the Rotterdam steel company Jewometaal lost €11 million after a fraudster posing as the director of its German parent company convinced a financial employee to transfer the funds.

What has changed is the wrapping, not the scam. Generative AI has made it possible to clone a voice from as little as three seconds of audio, and to project a convincing, real-time video presence of an executive into a conference call. Earnings calls, investor days, podcast interviews, keynotes and internal town halls are all sitting in the open, ready to be used as training material for a synthetic voice.

The engineering consultancy Arup provided the case that made the threat impossible to dismiss as theoretical. In January 2024, a Hong Kong-based finance employee joined what appeared to be a routine video call with the CFO and several colleagues, and transferred approximately \$25.6 million across fifteen transactions. Every other participant on that call, including the CFO, was an AI-generated deepfake. A comparable attempt targeted WPP CEO Mark Read in 2024, combining a cloned voice, existing video footage and a fake WhatsApp identity to arrange a call with other executives; it was caught before money moved, but the level of coordination signalled a new operational maturity in this type of attack.

The result is a form of fraud that no longer relies on a typo or a suspicious sender domain to give itself away. The channel that finance teams and executive assistants trust most, a phone call or a video call with a familiar voice and face, has become the primary attack surface.

The two-sided problem: fraud against you, and fraud in your name

Fraud against your organization: Criminals impersonate your own CEO, CFO or another executive to instruct your finance team, treasury desk or accounts payable staff to make an urgent transfer, change bank

details, or release confidential information. The caller ID shows an internal or known number. The voice, increasingly, is a synthetic clone of someone your employees have heard speak dozens of times.

Fraud in your organization's name: Criminals impersonate your executives to deceive your customers, suppliers, investors or partners: instructing a supplier to change payment details, convincing an investor of a confidential deal, or pressuring a partner organization into urgent action. Your organization did not place that call, but your name and your executive's identity were used to commit the fraud, and your organization bears the reputational fallout.

In both directions, the underlying vulnerability is identical: nothing in the public telephone network verifies that the person on the other end of the line is actually who the caller ID, or even the voice itself, suggests they are.

The numbers that don't lie

\$25.6M stolen from Arup in a single deepfake video-call incident (Hong Kong, Jan 2024)	\$893M in AI-related fraud losses logged by the FBI's 2025 Internet Crime Report	62% of organizations experienced at least one deepfake attack in the past 12 months (Gartner, 2025)	3 sec. of audio is enough to clone an executive's voice with ~85% accuracy
---	--	--	--

Behind these figures sits a rapid escalation, not a one-off event. Deloitte's Center for Financial Services projects that generative-AI-enabled fraud losses in the United States could rise from roughly \$12.3 billion to \$40 billion annually by 2027. Congressional researchers estimate that fewer than 5% of voice-clone fraud victims ever report their losses, which means the true scale of the problem is materially larger than the reported figures suggest. And this is not a US-only phenomenon: the same synthetic-voice techniques used against Arup and WPP are available, cheaply and at scale, to criminal networks already active against Dutch and European organizations through classic CEO fraud and bank helpdesk fraud.

Perhaps the most sobering figure is a human one: in controlled studies, most people report they cannot reliably tell a cloned voice from a genuine one, and detection accuracy for high-quality deepfakes in live settings is barely better than chance. Training employees to "listen closely" is no longer a credible line of defense.

What this means for your organization

- **Your verification procedures are being reverse-engineered.** Callback protocols, four-eyes principles and "does this sound right" instincts were built for a world where a scammer could fake an e-mail address but not a voice. Attackers now study exactly which procedures your finance team follows, and design the call to satisfy them.
- **Urgency and confidentiality are used as a weapon against your own culture.** The same deference to leadership and discretion around sensitive deals that make an organization function efficiently are precisely what a CxO fraud call exploits. The more your culture trusts a call from the top, the more exposed your finance function is.
- **Your executives are a target whether they know it or not.** Every public appearance, earnings call, keynote, podcast or town hall your CEO or CFO has ever given is potential training data for a

synthetic voice. Executives don't need to be careless with information to be impersonated; they only need to have spoken in public.

- **A single successful call can be catastrophic.** Unlike traditional phishing, which relies on volume, CxO fraud is a single, highly targeted, high-value attack. There is no second chance to catch it after the transfer has cleared.

Why this doesn't go away on its own

The core of the problem is not the sophistication of the criminals, real as it is. The core lies in the architecture of the telephone network itself. The public telephone network (PSTN) was built decades ago with one goal: connect calls. Authenticating the caller was never a design requirement.

To this day, any connected carrier worldwide can send any phone number, and the network accepts it without verification. Caller ID spoofing, the forgery of the number that appears on the recipient's display, is not a security hole that can be patched. It is a property of the network. Combine that unverified number with a synthetic, cloned voice, and every signal an employee historically relied on to trust a call, the number and the voice, can now be fabricated simultaneously.

Detection-based defenses, spam filters, voice-analysis tools, employee awareness training, respond after the call has already reached the employee. As synthetic voices improve and detection tools lose much of their lab accuracy in real-world conditions, that reactive approach is structurally losing ground.

The regulator moves and expects you to move with it

European and Dutch regulation increasingly treats secure communication, and the personal accountability of executives for it, as a demonstrable obligation rather than a best-effort commitment. Three developments are directly relevant for finance and executive functions:

- **Digital Networks Act (DNA), January 2026.** The European Commission requires telecom providers to take harmonised measures against caller ID spoofing. As a Regulation, the DNA is directly applicable in all 27 EU Member States, with BEREC tasked to provide guidance on effective technical measures.
- **Cybersecurity Act (NIS2 / Cyberbeveiligingswet), Spring 2026.** The Dutch implementation of the NIS2 Directive makes digital resilience, including communication security, a legal duty of care for organizations in vital and essential sectors. Directors and executives become personally responsible for demonstrating adequate risk management, including the processes that protect against impersonation fraud targeting their own finance function.
- **DORA, Digital Operational Resilience Act.** For financial institutions and the finance functions of organizations they interact with, DORA sets requirements for the operational resilience of digital systems and communication processes, explicitly including the reliability of the channels used to authorize payments and transfers.

For finance, treasury and executive teams, this means in concrete terms: relying on informal trust in a familiar voice or a recognized number is no longer a defensible control. "We trained our staff" will not, on its own, satisfy a regulator, an auditor or a board asking how a seven-figure transfer was authorized on the basis of a phone call that was never actually made by the person it appeared to come from.

The solution: guaranteed number identity for executive communication

Trusted Voice is designed around one principle: every organization deserves the certainty that a call from its executives is genuinely from its executives, not because the recipient has to trust it, but because the network guarantees it.

Trusted Voice operates as a closed, telecom-grade network completely separate from the public telephony infrastructure. Every call placed by an executive, or received by finance and treasury staff through the Trusted Voice network, is cryptographically verified before the connection is established. The identity of the caller is authenticated to the network itself. A call that fails this verification is not accepted.

The result: when a call from your CEO or CFO arrives through Trusted Voice, it is provably your CEO or CFO. Not because the voice sounds convincing, and not because the number on the display looks right, but because the network mathematically guarantees it before the call ever connects. Caller ID spoofing and voice cloning attack the two signals a human being can perceive; Trusted Voice authenticates the one signal a human being cannot fake.

What this means for your day-to-day operations

- **A verifiable channel for high-risk instructions.** Payment instructions, changes to banking details, and confidential deal communications from executives can be required to route through a verified channel, closing the gap that callback procedures and "just call them back" advice leave open when the callback itself can be spoofed.
- **No new burden on your executives.** Executives keep using their phone as normal. There is no app to install, no behavioural change, and no friction added to legitimate, time-sensitive communication.
- **A hard control finance teams can point to.** Instead of asking staff to detect a deepfake by ear, a skill that studies show is close to unreliable, the organization can point to a technical control: verified calls are accepted, unverified calls are not.
- **Compliance file out of the box.** Every verified call is logged with a full audit trail: who called, when, verified by the network. This is exactly the evidence NIS2, DORA and internal audit expect to see when a high-risk payment process is reviewed.
- **Integration in weeks, not months.** Trusted Voice connects to existing communication platforms, treasury systems and identity providers through a straightforward API integration, without an infrastructural overhaul.

Comparison: without vs. with Trusted Voice

Characteristic	Executive calling today	Executive calling with Trusted Voice
Number identity	Unverified: caller ID and the voice itself can both be faked	Cryptographically verified before the call connects
Voice-clone resilience	None: verification depends on a human recognising a familiar voice	Irrelevant: identity is confirmed by the network, not by ear

High-risk payment calls	Authorised on trust in caller ID and voice	Authorised only once network verification succeeds
Compliance	Not demonstrably safe	Audit trail per call, NIS2, DORA-ready
Implementation	N/A	API integration, up and running in weeks

Conclusion: from a familiar voice to a verified identity

CxO fraud has always exploited the same weakness: an employee's instinct to trust and act on instructions from the top. What has changed is that criminals no longer need to fake that trust convincingly through text alone. They can now fake the voice, the face, and the number, simultaneously and at very low cost, using nothing more than audio and video that your own executives have made public.

That problem cannot be solved with better training, stricter callback policies, or listening more carefully. The weakness is structural: the public telephone network was never built to verify who is actually calling, and the human ear was never built to reliably detect a synthetic voice.

Trusted Voice offers a fundamentally different approach: guaranteed number identity, verified at the source, within a closed network where spoofing and impersonation are technically excluded, not merely made harder to pull off. For your finance and executive functions, this means a channel where a call from the CEO or CFO is provably genuine before a single euro moves.

"Your controller shouldn't have to decide, in the moment, whether that voice is really the CFO's. The network should already know."

The choice in front of you

Keep authorising high-value instructions on the strength of a familiar voice and a recognisable number, and accept that both can now be fabricated convincingly and cheaply. Or move high-risk executive communication onto a network that verifies identity before the call ever connects, and remove the guesswork from the moment it matters most.

Contact us for a no-obligation consultation: www.trustedvoice.eu • Stadhuisplein 10, Eindhoven