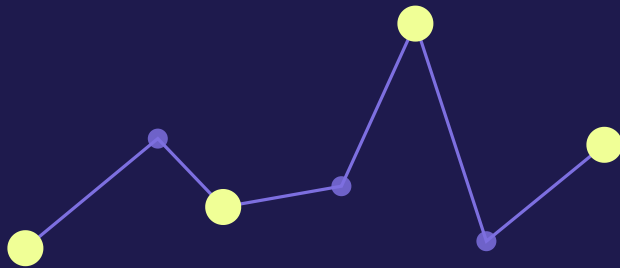


The Executive Authentication Gap

When a familiar voice, face or message is no longer proof of authority



In this briefing

When a familiar voice, face or message is no longer proof of authority

·	Executive Brief
01	What Changed
02	Why This Is a Communications Problem
03	The Executive Authentication Gap
04	The Artefact91 Executive Authentication Chain
05	The Authentication Matrix
06	The Communications Control Layer
07	When Impersonation Becomes a Reputation Incident
08	Do Not Rely on “That Doesn’t Sound Like Them”
09	The Artefact91 Response Sequence
10	Executive Visibility Without Executive Paralysis
11	What to Measure
12	A 30-Day Readiness Sprint
·	Artefact91 Point of View
·	Questions for Leaders
·	Sources & Research Base
·	Research Note

HOW TO READ IT

A briefing, not a report: the executive brief carries the argument, the numbered sections carry the evidence and the method, and every external figure is attributed to its source.

ARTEFACT91 BRIEFING

Executive Brief

A September 2026 financial fraud disclosed by Reuters makes an emerging communications risk harder to dismiss as hypothetical.

Reuters reported that Fideuram, the private-banking arm of Intesa Sanpaolo, lost €95 million after fraudsters impersonated trusted institutional figures across digital communications. More than half of the funds were later recovered; roughly €36 million remained missing at the time of reporting. [1]

The significance is not simply that synthetic media can be convincing. It is that an executive's name, face, voice and familiar communication patterns can increasingly be used to create false authority.

Artefact91's position: executive identity is now part of institutional trust infrastructure. Communications should not own financial authentication or cybersecurity controls, but it should help define the channels, verification norms, escalation paths and public-response architecture that protect trust when a leader is impersonated.

SECTION 01

What Changed

High-value impersonation has moved beyond obvious spoofing. The Fideuram case illustrates a broader pattern in which several familiar trust signals can appear together, making false communication feel credible. [1]

The FBI has repeatedly warned that malicious actors are using AI-generated voice messages, text messages and other impersonation techniques to pose as senior officials. Its guidance emphasizes independent verification through previously confirmed contact information. [2][3]

INTERPOL's 2026 Global Financial Fraud Threat Assessment warns that AI is increasing the scale and sophistication of financial fraud. [4]

Official Hong Kong government reporting also documented a 2024 corporate fraud in which a fabricated video conference was used to support a false executive instruction, resulting in HK\$200 million in losses. [5]

The trajectory is clear: organizations can no longer treat a familiar face, voice, account or communication style as proof of authority.

SECTION 02

Why This Is a Communications Problem

Security, finance and legal teams each control part of the risk. Communications controls something different: institutional meaning.

When an executive is impersonated, four forms of confusion can occur at once:

IDENTITY CONFUSION — Stakeholders may not know whether a message, call, video or post is authentic.

AUTHORITY CONFUSION — People may not know whether the apparent sender is entitled to make the request.

CHANNEL CONFUSION — Employees and external stakeholders may not know which channels the executive actually uses for sensitive matters.

REPUTATION CONTAGION — A false communication can become a real public story about governance, leadership judgment and institutional competence.

The larger failure occurs when an organization has not defined what counts as authentic executive communication, how unusual requests are checked, how impersonation is escalated, and how the institution establishes what is real after trust has been disrupted.

SECTION 03

The Executive Authentication Gap

Many organizations have strong rules for digital account security and weaker rules for authenticating human authority.

The risk is highest where three conditions overlap:

HIGH EXECUTIVE VISIBILITY — There is abundant public audio, video, photography, speech and writing to imitate.

HIGH DECISION AUTHORITY — The executive can legitimately initiate consequential decisions.

HIGH INFORMALITY — The organization relies on familiarity, speed or personal recognition rather than structured confirmation.

This is why “we would know the CEO’s voice” is no longer a sufficient control.

SECTION 04

The Artefact91 Executive Authentication Chain

ARTEFACT91 FRAMEWORK

CLAIM → CHANNEL → IDENTITY → AUTHORITY → INTENT → ACTION → CONFIRMATION

CLAIM — What is being requested?

CHANNEL — Did it arrive through an established and appropriate channel?

IDENTITY — Is the person actually who they appear to be?

AUTHORITY — Does that person have authority to make this request?

INTENT — Is the request consistent with known institutional context?

ACTION — What consequence will follow if someone complies?

CONFIRMATION — Has the request been independently checked through a separate trusted path?

The critical rule is:

CHANNEL IS NOT IDENTITY.

IDENTITY IS NOT AUTHORITY.

AUTHORITY IS NOT PROOF THAT A SPECIFIC INSTRUCTION IS GENUINE.

SECTION 05

The Authentication Matrix

Artefact91 recommends classifying unusual executive communications by consequence and verification quality.

LOWER CONSEQUENCE + STRONG VERIFICATION — Use normal workflow.

LOWER CONSEQUENCE + WEAK VERIFICATION — Pause and confirm through a known institutional channel.

HIGH CONSEQUENCE + STRONG VERIFICATION — Use established organizational approval controls.

HIGH CONSEQUENCE + WEAK VERIFICATION — Stop the process until the communication has been independently verified.

Urgency should increase verification, not reduce it.

SECTION 06

The Communications Control Layer

Communications should not become the authentication desk. It should own or co-own the parts of the system that define public and internal trust.

CANONICAL EXECUTIVE CHANNELS — Maintain an internal record of official executive contact points, approved messaging channels and known delegate pathways.

EXECUTIVE COMMUNICATION NORMS — Define what leaders will and will not ask people to do through informal channels. High-consequence requests should never depend only on personal recognition.

CANONICAL PUBLIC IDENTITY — For executives with high external visibility, maintain a clear and current owned-source record: executive biography, official role, verified social accounts, leadership page and corporate contact pathway.

IMPERSONATION ESCALATION — Define a standing route that connects communications, security, legal, risk and the executive office. The objective is speed with clear decision rights.

SECTION 07

When Impersonation Becomes a Reputation Incident

Not every attempted impersonation needs a public statement.

Public communication becomes more likely when customers, partners, employees or the public are being targeted; false content is circulating publicly; media are reporting it; the executive's authenticity is actively disputed; or there is a continuing risk that people will act on a false communication.

The first public objective is not image repair.

It is uncertainty reduction.

A strong first response should answer:

WHAT IS REAL? — Which accounts, channels or statements are authentic?

WHAT IS NOT REAL? — What impersonation or false communication has been identified?

WHO MAY BE AFFECTED? — Which stakeholders are most likely to have encountered the false material?

WHAT SHOULD PEOPLE DO? — Where should they verify future communications or report suspicious contact?

WHAT IS STILL UNKNOWN? — Do not fill evidence gaps with confidence.

WHAT HAPPENS NEXT? — Give a clear update path.

SECTION 08

Do Not Rely on “That Doesn’t Sound Like Them”

A May 2026 preprint based on 35,532 human judgments from 1,768 participants found an important pattern: people did not merely struggle with synthetic speech; they became more likely to doubt genuine speech compared with a 2021 baseline. The authors describe a shift toward skepticism of authentic audio. [6]

The study is a preprint and should not be treated as definitive evidence of population-wide behaviour.

But the strategic implication is credible enough to plan for: institutions may face both false acceptance and false rejection.

People may believe a fake executive.

They may also disbelieve the real executive during the correction.

That means detection is not enough. Organizations need authentication infrastructure that does not depend on subjective impressions of a face, voice or speaking style.

SECTION 09

The Artefact91 Response Sequence

ARTEFACT91 FRAMEWORK

DETECT → **PAUSE** → **VERIFY** → **CONTAIN** → **CLARIFY** → **CORRECT** → **RESTORE** → **LEARN**

DETECT — Capture the suspicious communication and establish what is known.

PAUSE — Stop any consequential action connected to the disputed communication until authenticity is established.

VERIFY — Use a previously trusted institutional path rather than the same channel that created the uncertainty.

CONTAIN — Coordinate communications, security, legal, risk and the executive office to limit further exposure.

CLARIFY — If stakeholders are at risk, state which communications are not authentic and which channels are valid.

CORRECT — Push accurate information through owned channels and directly to affected stakeholders. Do not assume one correction post will travel as far as the false content.

RESTORE — Re-establish trusted communication paths and confirm delegated authorities.

LEARN — Document which assumptions made the impersonation credible and update protocols accordingly.

SECTION 10

Executive Visibility Without Executive Paralysis

The answer is not to make leaders invisible.

Executives still need to communicate publicly. Interviews, speeches, podcasts, social media and video can be important to leadership, trust and market presence.

Trying to eliminate all source material is unrealistic.

The better strategy is to separate VISIBILITY from AUTHENTICATION.

Public content should be treated as public.

Sensitive authority should rely on controls that remain trustworthy even when a bad actor can reproduce public-facing characteristics.

An executive's face or voice can support communication, but should not by itself authenticate consequential authority.

SECTION 11

What to Measure

TIME TO AUTHENTICATE — How long does it take to confirm or reject a suspicious executive communication?

VERIFICATION COVERAGE — What proportion of high-consequence requests pass through an independent confirmation step?

CHANNEL INTEGRITY — Are executive contact records, delegated authorities and public account lists current?

ESCALATION LATENCY — How long does it take for a suspicious impersonation to reach communications and the relevant decision owner?

EXPOSURE — How many internal or external stakeholders encountered the false communication?

CORRECTION REACH — Did verified information reach the same audiences and channels as the impersonation?

RECOVERY TIME — How long did it take to restore trusted communication and normal decision flow?

SECTION 12

A 30-Day Readiness Sprint

WEEK 1 — MAP — Inventory the organization's most visible executive identities, high-consequence decision types, informal communication channels and delegated-authority practices.

WEEK 2 — DEFINE — Create the executive authentication chain, canonical channel register and cross-functional escalation path.

WEEK 3 — SIMULATE — Run three scenarios: a false executive message, a synthetic voice or video, and a publicly circulating fake statement attributed to a leader. Measure where uncertainty persists and where staff feel unable to challenge apparent authority.

WEEK 4 — INSTITUTIONALISE — Publish the protocol internally, brief executive assistants and relevant control teams, establish a correction-page template, and add executive impersonation to the crisis simulation calendar.

ARTEFACT91 BRIEFING

Artefact91 Point of View

The next executive reputation crisis may begin with something the executive never said.

That is why executive communications can no longer stop at message discipline, media training and social monitoring.

Organizations need to know how authority is authenticated.

The strongest response is not better deepfake detection alone. It is a trust architecture in which no single face, voice, account, message or intermediary can independently turn familiarity into consequential authority.

Artefact91 Executive Authentication:

ARTEFACT91 FRAMEWORK

CLAIM → CHANNEL → IDENTITY → AUTHORITY → INTENT → ACTION → CONFIRMATION

The question for leaders is no longer only, “What happens if someone fakes me?”

It is:

“What could someone make the organization believe or do if enough people think the fake is me?”

ARTEFACT91 BRIEFING

Questions for Leaders

Could an employee receive a high-consequence instruction from an executive through an informal channel today?

Would that employee know exactly how to verify it without relying on the apparent sender?

Can staff challenge an urgent executive instruction without fearing that they are obstructing leadership?

Do we have a current internal record of official executive channels and delegated authorities?

If a fake CEO video or voice note circulated publicly this afternoon, where would stakeholders go to establish what is real?

Could our communications, security, legal and risk teams agree on a fact-floor statement quickly?

Do our crisis exercises include impersonation of a senior leader — not merely compromise of an account?

ARTEFACT91 BRIEFING

Sources & Research Base

- [1] Reuters, “AI messaging scam costs Italy’s top bank Intesa millions, sources say,” 25 September 2026. Reuters reporting syndicated by WHBL. The report states that Fideuram lost €95 million; more than half was recovered and approximately €36 million remained missing at the time of publication. <https://whbl.com/2026/09/25/ai-messaging-scam-costs-italys-top-bank-intesa-millions-sources-say/>
- [2] Federal Bureau of Investigation, “Senior U.S. Officials Impersonated in Malicious Messaging Campaign,” 15 May 2025. <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign>
- [3] Federal Bureau of Investigation, “Senior U.S. Officials Continue To Be Impersonated in Malicious Messaging Campaign,” 19 December 2025. <https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-continue-to-be-impersonated-in-malicious-messaging-campaign>
- [4] INTERPOL, “INTERPOL report warns of increasingly sophisticated global financial fraud threat,” 16 March 2026. <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
- [5] Government of the Hong Kong Special Administrative Region, “LCQ9: Combating frauds involving deepfake,” 26 June 2024. <https://www.info.gov.hk/gia/general/202406/26/P2024062600192.htm>
- [6] Nicolas M. Müller and Wei Heng Choong, “Eroding Trust in Real Speech: A Large-Scale Study of Human Audio Deepfake Perception,” arXiv preprint, 21 May 2026. Study of 35,532 judgments from 1,768 participants; cited here as emerging research, not peer-reviewed evidence. <https://arxiv.org/abs/2605.26136>

ARTEFACT91 BRIEFING

Research Note

This briefing synthesises current reporting, law-enforcement guidance, official government documentation, emerging academic research and Artefact91 analysis. The Fideuram incident remains subject to investigation and public reporting may evolve. The academic audio-perception study cited is a preprint and should not be generalized beyond its methodology. The Artefact91 frameworks are decision aids designed to strengthen communications governance; they do not replace cybersecurity controls, authorization procedures, legal advice or forensic investigation.