



— BRIEFING / 007 · JULY 2026

THE VOICE IS NOT YOUR CFO.

The wrench attack and the deepfake call are the same attack. Both bypass the cryptography entirely and go at the one control every architecture shares: a human authorized to approve. One does it with proximity and fear. The other does it with a familiar voice and time pressure, from anywhere on earth.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don't have to.

info@executiveriskservices.com · referral or invite only

THE SAME TERMINAL CONTROL, ATTACKED REMOTELY

This series has argued that every custody and treasury architecture terminates in a person who can approve. Physical coercion reaches that person through their body and their family. Synthetic-media fraud reaches the same person through their ears and their inbox, and it scales in a way proximity never can. A voice model of a public executive is built from material the executive published on purpose: earnings calls, podcasts, conference keynotes. The more senior the principal, the larger the training set, and the more weight their voice carries in exactly the moments an approver is being asked to break procedure.

The attack pattern is stable across the public cases: an urgent, plausible scenario; a familiar voice or face; a reason the normal channel is unavailable; and a narrow window to act. Every element is aimed at the same target, which is not a system. It is an employee's willingness to help a superior under pressure.

WHY VOICE VERIFICATION IS ALREADY DEAD

The uncomfortable premise to plan from: recognizing a voice, or a face on a video call, is no longer authentication. It was never designed to be. It was a social habit that happened to be reliable for a century, and it stopped being reliable. Organizations that still allow a recognized voice to move money or change signing arrangements are running an authentication control that has been publicly broken.

The equally uncomfortable corollary for protective work: this is not only a treasury problem. The same technique books travel, changes an itinerary, redirects a school pickup, or manufactures the crisis that a physical approach then exploits. Synthetic media is how a remote attacker creates the urgency; the seam between that call and the physical world is where our discipline meets the fraud team's.

VERIFICATION AS ARCHITECTURE, NOT VIGILANCE

Training people to "listen for artifacts" is a losing strategy against improving models. The durable answer is the same one this series gave for physical duress: design the process so that one deceived person cannot complete the loss.

Four properties do most of the work. Out-of-band verification for any request that moves value or changes authority, over a channel the requester did not choose. Call-back to numbers on file, never to numbers provided in the request. Dual authorization with genuinely independent approvers, so urgency has to defeat two people on two channels. And a cultural rule stated by leadership in plain terms: no one in this firm will ever be penalized for verifying, and any request that resists verification is treated as hostile. The last one matters most, because every one of these frauds is, at bottom, a bet that hierarchy beats procedure.

ERS provides executive protection, insider-risk advisory, and custody-governance review for principals in digital assets, finance, and technology. Engagements begin with a conversation: info@executiveriskservices.com.

This briefing describes a fraud pattern at the level already established in public reporting, names no tooling, and provides no methodology. It centers verification design, which is the protective takeaway. We publish the pattern. We omit operational detail. © 2026 Executive Risk Services, LLC.