People Verification for Finance: Stopping Wire Fraud, Vendor BEC, and Executive Impersonation

People & In-Person / Last updated 2026-06-11 / https://www.scrambleid.com/learn/people-verification-for-finance

> **Status (June 2026):** Early access. The People verification family is live with early-access customers and isn't generally available yet. The patterns in this article describe the shipped design as it stands today; talk to your ScrambleID account team about access and timelines before building them into finance procedure.

In one sentence: Wire-transfer fraud, vendor banking changes, and executive sign-off impersonation have become the dominant high-loss attack class in enterprise finance, and the only verification primitive that defeats them deterministically (regardless of how convincing the AI-generated voice or video) is cryptographic people verification at the moment of the high-trust decision.

TL;DR (canonical)

- **The threat is now operational.** BEC and APP fraud rank among the top reported cyber-loss categories targeting enterprises. Single-incident losses in the $10-100M+ range are common. The Arup Hong Kong deepfake fraud (~$25.6M, 2024) is one of many.
- **Procedural defenses are no longer sufficient on their own.** Callback-to-known-good is defeated by voice cloning. Manager confirmation is defeated by deepfake. Knowledge-based questions to the vendor are defeated by social-engineering preparation.
- **The cryptographic anchor is people verification.** A signature from the legitimate executive's, AP partner's, or vendor's hardware-bound device, against a server-issued single-use challenge with a 60-second TTL, defeats the impersonation regardless of fidelity.
- **Three load-bearing patterns.** people verification at wire approval. people verification at vendor banking change. people verification at executive sign-off for high-value commitments.
- **Layered with dual control** for wires above thresholds. Lockstep (in development) is ScrambleID's dual-control design, described in Lockstep: Dual Control.
- **Compliance posture.** FFIEC 2021 guidance, NYDFS Part 500, SOX, GLBA, and PSD2 SCA all support and increasingly expect this layered cryptographic approach.

The threat landscape for enterprise finance

The pattern is well-documented. An attacker establishes a context (compromised email account, pretexted phone call, scheduled video meeting) in which a finance employee is asked to authorize a wire, change vendor banking details, or process an urgent payment. The sophistication ranges from text-only BEC ("hey, can you send a wire to this account, I'll explain in person later") to multi-participant deepfake video conferences with cloned voices, prepared OSINT, and real-time coaching.

The attackers target finance because:

1. **The blast radius is the wire.** A successful authorization moves money irrevocably. There is no "accept" button that can be retroactively unclicked.
2. **Time pressure is built in.** Wire deadlines, end-of-quarter pressure, end-of-day cutoffs, and "the executive is on a plane and needs this now" all serve the attacker.
3. **The verification controls have historically been procedural.** Callback. Manager confirmation. Email reply confirmation. All of these are now defeatable by AI capability.
4. **Insurance complications.** Cyber and crime insurance increasingly carve out social-engineering losses from BEC, leaving the loss on the company's balance sheet.
5. **Executive carve-outs.** "Trust the CFO's email/call/text" remains a cultural default in many organizations. The attacker exploits that.

The traditional defenses (procedure, training, segregation of duties) remain necessary. They are not sufficient in the deepfake era.

Three load-bearing people-verification patterns for finance

Pattern 1: people verification at wire authorization

The threat: Finance receives an apparent executive instruction to authorize a wire transfer. The instruction may arrive by email (BEC), phone (voice clone), video call (deepfake), or chat. The amount is large enough to be material; the urgency is engineered.

The pattern:

1. Finance receives the wire instruction.
2. Before authorizing, finance initiates a people verification with the apparent executive's enrolled identity.
3. The executive's enrolled device prompts. The executive approves on their phone. The cryptographic round trip completes in a few seconds, versus the 30 to 90 seconds typical of knowledge-based questions.
4. For wires above an organizational threshold, the authorization additionally requires dual-control approval (a second authorized approver completes their own cryptographic ceremony before the

wire releases). This is the control Lockstep (in development) is designed to enforce.
5. The wire is released only on successful completion of all required ceremonies. Audit captures every event.

What this defeats:

- BEC: the email is from a compromised executive account; without people verification, finance acts on the email; with people verification, the verification fails because the attacker doesn't hold the executive's private key.
- Voice clone: the phone call sounds like the executive; without people verification, finance trusts the voice; with people verification, the cryptographic round trip cannot be completed by the cloned voice.
- Deepfake video: the video shows the executive (Arup-style); without people verification, finance trusts the video; with people verification, the deepfake on the call cannot complete the verification.
- Insider misuse: a legitimate finance employee initiating a fraudulent wire still has to pass dual control; both ceremonies must be executed by authorized parties.

What this does not solve: Coercion (an executive under duress can complete the verification). Mitigations include duress codes, very-high-amount thresholds requiring additional friction, and well-publicized "no urgency exception" policy.

Pattern 2: people verification at vendor banking change

The threat: A vendor's apparent contact emails, calls, or messages AP to change the vendor's banking details before the next payment cycle. The instruction may come from a compromised vendor email, a voice-cloned vendor representative, or a social-engineered vendor portal account.

The pattern:

1. AP receives the banking change instruction (email, call, portal, in-person).
2. Before processing, AP initiates a people verification with the vendor's enrolled contact.
3. Verification completes in a few seconds. AP sees the verified vendor identity card.
4. AP confirms the new banking details over a separate channel (typically a callback to the vendor's known-good number from the corporate vendor record, not from the change request itself).
5. The change is processed only after both verification and channel-separated confirmation succeed.

What this defeats:

- Compromised vendor email: the change request is from the legitimate-looking inbox; without people verification, AP processes the change; with people verification, the attacker doesn't hold the vendor contact's private key.
- Voice-cloned vendor call: the call sounds like the legitimate contact; without people verification, AP trusts the voice; with people verification, the verification fails.

- Vendor portal account compromise: the portal request looks legitimate; without people verification, AP processes it; with people verification, the cryptographic verification confirms the legitimate vendor contact is requesting the change in real time.

What this does not solve: Vendor-side compromise where the attacker has both the legitimate vendor contact's email and their enrolled device. This is a compound compromise (the attacker has had to reach the vendor's hardware-bound device, which is materially harder than email account takeover) and is mitigated by the channel-separated confirmation step.

Pattern 3: people verification at executive sign-off for high-value commitments

The threat: Various: M&A approvals, contract signatures, strategic communications, board commitments, public statements. An attacker who can impersonate an executive's sign-off can move material value without ever touching a wire.

The pattern:

1. The receiving party (legal counsel, board secretary, contract counterparty) initiates a people verification with the apparent executive at the moment of the sign-off.
2. The executive's enrolled device signs the verification challenge.
3. The sign-off is recorded in audit with the cryptographic verification event attached.

What this defeats:

- Forged executive signatures.
- Voice-cloned approvals.
- Compromised email approvals.
- Deepfake video approvals.

What this does not solve: The legitimate executive being deceived into signing off (still possible). The cryptographic verification confirms identity; it does not confirm the executive's understanding of what they are approving. Process controls and clear sign-off documentation matter here.

Threshold-based escalation

A practical escalation table for wire authorization:

Wire amount	Required verification
Below $25K, known payee	Standard procedural controls; no additional people verification
$25K-$250K, known payee	people verification with originating executive
Above $250K (or first-time payee)	People verification + dual control (Lockstep, in development) + named-payee confirmation

Wire amount	Required verification
Above $1M	People verification + dual control + named-payee confirmation + cooling-off window (hours to next business day)
Above $5M	All of the above + CFO/CEO concurrence + treasury management committee acknowledgment for some organizations

These are illustrative tiers; calibrate to your institution's risk policy. Organizational risk appetite, treasury operations volume, and insurance posture all affect the right thresholds. The principle: dollar exposure should drive verification rigor, not the other way around.

The "the CFO is on a plane and needs this now" case

This is the social-engineering setup most often successful against finance teams. It is also the single best example of why procedural defenses are not sufficient and cryptographic ones are.

The legitimate scenario: the CFO is in transit, has limited connectivity, and needs to authorize a time-sensitive wire.

The attack scenario: the apparent CFO is in transit, has limited connectivity, and needs you to authorize a time-sensitive wire.

The procedural-defense problem: the urgency, the limited callback options, and the executive's apparent inability to participate in a verification ceremony are exactly what makes the attack work. The legitimate scenario produces the same indicators as the attack.

The cryptographic resolution: the verification ceremony takes a few seconds and works on any internet-connected device. The legitimate CFO completes it. The attacker cannot. There is no scenario in which a legitimate CFO, with their enrolled device, cannot spare a few seconds for a cryptographic verification but can authorize a multi-million-dollar wire by phone. If the executive can do the wire, they can do the verification.

The policy that matches: no exceptions for executive urgency. The executive completes verification or the wire does not move. This is initially uncomfortable for executives accustomed to procedural carve-outs; it is also the policy that closes the attack.

What about back-pressure on procedure?

Common pushback from finance teams adopting people verification:

"Our executives won't tolerate the friction." The friction is a few seconds. The friction of explaining a $25M fraud to the board is materially greater. Brief executives in advance about the policy and the threat model; they typically accept it once they understand the alternative.

"Vendor verification is going to slow us down." Vendor enrollment is one-time. Once enrolled, every verification takes a few seconds, versus the 30 to 90 seconds typical of knowledge-based questions. The slow path is the cold-recovery path for vendor contacts who lose their devices, which should happen rarely.

"What about vendors who refuse to enroll?" The people verification primitive is not the only verification; for vendors who decline enrollment, AP can fall back to a more rigorous out-of-band confirmation procedure (multiple channels, multiple individuals at the vendor). The vendors who decline enrollment are a population whose banking changes warrant more friction, not less.

"Our existing controls have prevented losses so far." The historical absence of evidence is not evidence of absence. The threat surface is changing year-over-year; controls that worked in 2018 are not adequate in 2026.

"We have insurance for this." Cyber and crime insurance carve-outs for social engineering have expanded; many policies now exclude losses where the insured authorized the transfer (which is most BEC and all APP). Read the carve-outs before assuming insurance covers what you think it covers.

Audit and forensics

The people verification produces signed events in an immutable audit log:

- Verification initiated (timestamp, initiating user, target identity)
- Method selected (QR/QID, Type Code, SMS deep link)
- Step-up performed (per organizational policy)
- Verification completed or failed (timestamp, outcome, error if applicable)
- Device IDs (ZIDs) involved on both sides
- Attribute set shared (which fields the presenter shared)
- TTL expiry (was the verification consumed within the 60-second window)

For wire authorization, the audit log additionally captures the Lockstep dual-control approvals and the wire release event. The full audit chain reconstructs the high-trust decision end-to-end and supports both internal audit and external (e.g., post-incident insurance) review.

For the broader audit posture, see Compliance Mapping: NIST and CISA.

Implementation sequence

A reasonable rollout order for a finance organization gating wire and AP controls behind people verification:

1. **Inventory the high-trust decisions.** Wire authorization, vendor banking change, payee setup, payroll changes, executive sign-off. Each is a verification gate.
2. **Set thresholds and policy.** Dollar thresholds, dual-control thresholds, named-payee confirmation requirements, cooling-off windows.
3. **Enroll the parties.** Finance team. Executives. AP team. Top vendors. Treasury counterparties.
4. **Pilot with one high-risk path.** Vendor banking changes is a common starting point because the volume is moderate, the loss potential is high, and the existing process is procedural.
5. **Expand to wire authorization.** Pair with Lockstep dual control on the wire-release side.
6. **Add executive sign-off.** Strategic decisions, M&A, board-level commitments.
7. **Tabletop the exception cases.** Rehearse what happens when an executive cannot complete verification (cold-recovery path), when a vendor declines enrollment, when the SOC sees an anomalous people verification attempt.
8. **Brief audit and insurance.** Document the controls, the audit chain, and the verification events. Cyber insurance underwriters increasingly reward layered cryptographic controls in renewal pricing.

Standards and compliance

Wire and AP controls gated by people verification map to:

- **FFIEC 2021 Authentication Guidance:** layered, risk-proportionate authentication for high-risk transactions including wire authorization and counterparty verification.
- **NYDFS 23 NYCRR Part 500.12** (MFA) and 500.7 (privileged accounts) for New York-regulated financial-services entities.
- **PCI DSS v4.0.1** requirement 8.4 for any path touching cardholder data.
- **PSD2 Strong Customer Authentication** for EU-customer-touching payments.
- **GLBA Safeguards Rule** as amended (FTC 2023) for non-bank financial institutions.
- **SEC Reg S-P** (amended 2024) for broker-dealers and investment advisers.
- **SOX** internal controls over financial reporting (ICFR) with auditable evidence of high-trust authorizations.
- **NIST SP 800-63B** AAL3 properties for the highest-trust authentication.

For deeper financial-services coverage, see Authentication for Financial Services.

Key Takeaway

Wire-transfer fraud, vendor banking changes, and executive sign-off impersonation are the dominant high-loss attack class in enterprise finance, with FBI IC3 consistently ranking BEC among the top loss categories targeting enterprises and single-incident losses (Arup Hong Kong, ~$25.6M, 2024)

reaching tens of millions. Procedural defenses (callback to known-good, manager confirmation, knowledge-based questions) are no longer sufficient against AI-generated voice cloning, deepfake video, and prepared social engineering. People verification cryptographic verification gates the high-trust decision: a hardware-bound private-key signature against a server-issued, single-use challenge with a 60-second TTL, completed in a few seconds end-to-end (versus the 30 to 90 seconds typical of knowledge-based questions), defeats the impersonation regardless of voice or video fidelity. The pattern layers people verification at wire authorization, people verification at vendor banking change, and people verification at executive sign-off, with Lockstep dual-control thresholds and named-payee confirmation for the highest-value transactions. The policy that makes this work is "no exceptions for executive urgency"; the cryptographic verification takes a few seconds and works on any internet-connected device, so there is no legitimate scenario where an executive can authorize a wire but cannot complete a verification.

FAQ

How big is the wire-fraud and vendor-banking-change problem?

FBI IC3 consistently ranks business email compromise (BEC) among the top loss categories targeting enterprises, with annual reported losses in the billions; the closely related authorized push payment (APP) fraud pattern drives similar losses outside IC3's category structure. Single-incident losses in the $10-100M range are now common; the Arup Hong Kong deepfake fraud (~$25.6M, early 2024) is one example of the upper end. The pattern targets enterprise finance and treasury because the loss-per-attack is high enough to reward sophisticated effort and because the verification controls are typically procedural rather than cryptographic.

Why doesn't "call the executive back to verify" work anymore?

Voice cloning from 30 seconds of recorded audio is now consumer-grade capability. The voice on the callback can be cloned. The number can be spoofed. The executive can have call forwarding compromised. Callback to a known-good number is still a procedural step worth retaining, but it is no longer evidence of legitimacy on its own. Cryptographic verification through the executive's enrolled device is the deterministic anchor; callback is one of several procedural signals that layer on top.

What's the procedure for AP receiving a vendor banking change request?

The recommended pattern: when a vendor banking change is requested (regardless of channel: email, call, portal, in-person), AP requires a people verification with the vendor's enrolled contact before processing the change. The vendor's enrolled contact's hardware-bound device authenticator signs a server-issued challenge with a 60-second TTL. The verification completes in a few seconds, versus the 30 to 90 seconds typical of knowledge-based questions. The change is processed only on success, plus an additional verification cycle (typically a separate confirmation call to the vendor's known-good number to confirm the change details) for changes above an organizational threshold.

Can people verification stop authorized push payment (APP) fraud?

People verification stops the impersonation-driven subset of APP fraud (the customer is being asked to pay an attacker who is impersonating a legitimate counterparty). The harder subset is the customer-is-the-victim variant where a real fraudster successfully convinces the customer to authorize a payment to the fraudster's own account. Authentication of the customer's identity does not stop that case because the customer is the one authorizing. The mitigations for that pattern combine step-up authentication at the high-risk transaction (dual control via Lockstep, named-payee confirmation, cooling-off windows), strong call-center authentication so vishing cannot impersonate the bank, and bank-side risk signals on the receiving institution. People verification is the right primary control for the impersonation subset; broader APP defense requires the layered stack.

What about the regulatory side?

FFIEC's 2021 authentication guidance, NYDFS Part 500 (financial services), and (for EU and EU-customer-touching) PSD2 SCA all push toward layered, risk-proportionate authentication for high-risk transactions, with explicit attention to wire authorization and counterparty verification. Gating wire approval and vendor banking changes behind people verification is a defensible pattern under all of these. The detailed compliance mapping is covered in Authentication for Financial Services.

What's the right wire-amount threshold for triggering dual control?

The threshold is an organizational risk decision and varies by company size, transaction patterns, and insurance position. A common baseline: dual control on any wire above $250K-$500K, plus dual control on any first-time payee regardless of amount, plus dual control on any change to bank details for an existing payee. For smaller organizations or higher-risk industries, the thresholds tighten. The right threshold is the one above which a fraudulent wire would be material to the organization.

References (public)

- FBI IC3 Annual Internet Crime Report: https://www.ic3.gov/AnnualReport/Reports
- FBI, Business Email Compromise: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise
- FinCEN Alert on Deepfake Media for Identity Fraud: https://www.fincen.gov/sites/default/files/2024-11/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf
- FFIEC, Authentication and Access to Financial Institution Services and Systems (2021): https://www.ffiec.gov/press/PDF/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf
- NYDFS 23 NYCRR Part 500: https://www.dfs.ny.gov/industry_guidance/cyber_faqs
- EBA RTS on Strong Customer Authentication (PSD2): https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-strong-customer-

authentication-and-secure-communication-under-psd2

- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Related reading

- What Is People Verification?
- Deepfake-Resistant Identity Verification
- Stopping Help-Desk Impersonation with People Verification
- Lockstep: Dual Control
- Authentication for Financial Services
- Recovery and Fallback Playbook
- Compliance Mapping: NIST and CISA