Finance & Banking BEC Breach Report

Three BEC attacks your finance team is at risk of on Monday — and the wire-transfer controls mapped to FFIEC CAT 2024, GLBA §501(b), FinCEN 2024 advisory, and NYDFS Part 500.13 dual-control wires that stop them.

For community banks, credit unions, fintech treasury teams, wire-room operators, and correspondent-banking operations

$2.9B

BEC losses reported to FBI IC3 in 2024 — the highest of any cybercrime category

WHAT IS IN THIS REPORT?

TARGET PROFILE

Why Finance & Banking Teams Are the #1 BEC Target

Four structural realities make every wire-room, treasury desk, and correspondent-banking operation a preferred target. None of them require the attacker to break through a firewall. The attacker is asking — through email, phone, and increasingly voice-clone — to be paid.

Treasury desks move seven-figure wires on routine traffic

A community-bank wire operator settles $2M–$10M of correspondent wires on a normal morning. A fintech treasury desk sends ACH and wire payments to vendor accounts on a daily cadence. To an attacker scanning executive bios and treasury job postings, the median wire is indistinguishable from a legitimate one — and the only control that catches them is the callback verification.

Dual-control wires are the right policy, but the attacker exploits the gap above the threshold

NYDFS Part 500.13 and most prudent bank policies require dual control above a defined wire threshold. The attacker tests that by sending a wire request that sits just below the threshold, or by submitting three sub-threshold wires in sequence, or by targeting an institution whose threshold is set unusually low. The policy exists; the implementation is the variable.

Treasury / finance operators are trained to be helpful, not suspicious

A wire operator or treasury analyst is taught to be responsive to executive urgency. The FBI IC3 2024 dataset shows the #1 BEC variant is a spoofed CEO email asking the wire operator to send an "urgent, confidential outbound wire today" — often to a new beneficiary account the executive claims was just set up. The operator who waits to verify is the operator being measured on close-of-day.

Correspondent-banking ops trust vendor email — and that is the BEC leak point

Correspondent-banking ops coordinate with upstream / downstream bank counterparties over email and shared portals. A vendor email compromise at a third-party (auditing firm, wire-routing vendor, bene-verification service) lets the attacker insert cloned wire instructions into an in-flight reconciliation thread. The op side does not realize the vendor mailbox has been compromised for weeks.

VERIFIED BREACH DATA

Three Named Breach Anchors Targeting Finance & Banking

Every anchor below is grounded in the public FBI IC3 2024 dataset and verified case reporting. Date, dollar figure, and attacker pattern correspond to the underlying reporting — they are not invented.

ANCHOR 1 · $2.9B / 21,489 complaints

Spoofed CEO Email Requesting an Urgent Outbound Wire

PATTERN
Attacker registers a lookalike sender domain (e.g., ceo-jones.co vs ceo-jones.com) and emails the wire operator or AP lead with a confidential "closing on this today, please send by 4 PM" instruction to a new beneficiary. Tone mimics the real CEO: urgent, brief, references a known deal. Sent during the CEO's known travel window.

VICTIM ACTION
Treasury / wire operator reads the email at 11:40 AM, drafts the wire by 12:05 PM, awaits the dual-control approval above the institution's threshold. If the second approver catches nothing, the wire moves at 12:30 PM. Funds are in a mule account by EOD.

OUTCOME
FBI IC3 2024 reports $2.9B in BEC losses across 21,489 complaints — CEO-impersonation wires remain the single most reported pattern. Recovery rate ~13% industry-wide; FFIEC BEC joint statement puts recovery above 80% when the FBI Financial Fraud Kill Chain is activated inside the 72-hour window.

ANCHOR 2 · Targeted / correspondent-channel

Cloned Wire Instructions to Correspondent-Bank Ops via Vendor Compromise

PATTERN
Attacker compromises a third-party vendor mailbox that the bank's correspondent-banking ops trust — an auditing firm, a wire-routing service, a bene-verification platform. They live in the inbox for 3–6 weeks, monitor reconciliation threads, and inject cloned wire instructions into an active correspondent-banking thread at month-end.

VICTIM ACTION
Correspondent-banking ops receive wire instructions that arrive in-thread with prior correspondence and look like a routine settlement update. If the upstream correspondent's letterhead and the wire payload pass manual review, the wire moves below the threshold of any single review.

OUTCOME
Same pattern visible in the Treasury / Treasury OFAC enforcement record and the FinCEN 2024 advisory on increased BEC targeting of correspondent-banking ops. Recovery is highly variable because the reconciled correspondent relationship adds an extra step — but losses are commonly 7-figure.

ANCHOR 3 · Threshold-bypass (multi-million)

Deepfake CFO Voice Authorizing a Wire Above Dual-Control Threshold

PATTERN
Attacker scrapes a 30-second public audio sample of the CFO (earnings call, investor video, conference keynote, internal town hall). Clones the voice using commodity voice-cloning. Calls the wire approval queue with urgent language matching the CFO's known tone — references a real deal name and the beneficiary by first name.

VICTIM ACTION
Wire approver answers the call with the cloned voice confirming the wire. Assuming the voice authentication passes, the approver pushes through dual-control with a confirmation that the paper trail shows was a "live confirmation" — but was voice-synthesized. The wire moves the next business day.

OUTCOME
Reported as an emerging pattern in the Q1 2024 IC3 BEC data. NYDFS Part 500.13 dual-control policy is the right structural control, but the second approver relying on a voice match is the leak. Banks that require a non-voice channel (signed callback, second live voice from a known number, in-person confirmation) for wires above the threshold close the gap.

ANATOMY OF A FINANCE-TARGETED BEC ATTACK

The Finance-Targeted BEC Kill Chain

TEACHING CASE · ANONYMIZED · 2026

A treasury analyst at a mid-size community bank received an email 90 minutes before end-of-day from what appeared to be the CEO's address, requesting a $2.3M wire to a new beneficiary for "the acquisition we've been working on — need it out today." The analyst validated the wire against the dual-control threshold and forwarded to the second approver, who approved based on a callback to the CFO at a number the email provided — answered by a cloned CFO voice. The wire was released at 4:14 PM. Recovery inside the FFKC window: contact the FBI field office within 90 minutes; the bank's cyber-insurance carrier was notified within 30 minutes; the Bank Secrecy Act officer filed a FinCEN SAR within 4 hours.

1
Public Reconnaissance
Weeks before attack

Attacker scrapes the bank's org chart, identifies the CEO, CFO, wire-room manager, and corresponding correspondent-banking ops. Pulls public audio (earnings calls, conferences, investor videos) for voice cloning. Identifies the dual-control threshold by inferring from wire-volume postings.

2
Lookalike Domain Registered
1–4 weeks before

Attacker registers a near-identical sender domain (e.g., ceo-jones.co vs ceo-jones.com) with valid SPF / DKIM / DMARC records and warmed-up mailbox history, so the message does not look brand-new. If impersonating a vendor, attacker compromises a real mailbox instead.

3
Executive Impersonation Setup
7–14 days before

If there is a hot deal in progress, the attacker references it from public records. If not, the attacker drafts an "acquisition" narrative. Either way, the email is short, urgent, and matches the CEO's known cadence (heavy, abbreviated, brief requests).

4
Urgent Wire Request
Hours to days before

Email arrives — urgent tone, "needs to go out today," references a known deal, names a new beneficiary account. The wire is structured to sit just below the dual-control threshold or to request a routine-looking entry that will pass standard review. Urgency is always present.

5
Verification Bypass
During the wire decision

If the operator or approver calls the number in the email to "double-check," a deepfake voice answers. If the operator uses their own file's number, the real CEO replies "those are correct" without knowing the attacker's email is sitting in a separate thread. The paper trail says they verified.

6
Wire Authorized
Minutes after sent

Wire moves above the dual-control threshold (or below it, depending on the bank's policy and the attacker's structure). Funds are laundered through transit accounts. FBI Financial Fraud Kill Chain has a 72-hour window for clawback — measured from the moment the wire settles, not from discovery.

7
Funds Laundered / Recovery Window Closes
24–72 hours

Funds reach a mule network and disperse to crypto off-ramps or international transit accounts. After 72 hours, recovery probability collapses. If the bank filed IC3 within 4 hours and engaged the FFKC, recovery odds exceed 80% — but only with the field-office escalation path, not a web-form-only report.

CONTROL CROSSWALK TO DFW

Wire-Transfer Controls Mapped to FFIEC CAT / GLBA / NYDFS / FinCEN

Every control below is mapped to a specific FFIEC, GLBA, NYDFS, or FinCEN citation so the controls hold up to an examiner inquiry, a SAR follow-up, and a cyber-insurance recovery claim. Hand the same crosswalk to your BSA officer and to your cyber-insurance broker.

FFIEC CAT 2024 &MIDDOT; CYBERSECURITY CONTROLS

Out-of-Band Wire Verification & Beneficiary Master File Change Controls

Annual documented training on Verify-Out-Of-Band protocol: any wire above the institution's dual-control threshold requires callback verification using a known phone number from a maintained contact file (not from the email or voice-tree prompt). Beneficiary master file changes require dual-control approval with a closed-loop acknowledged receipt. Funds movement to a new beneficiary requires elevated review even when the email signer is recognized.

GLBA §501(B) &MIDDOT; SAFEGUARDS RULE

Annual Training on BEC / Wire-Fraud Recognition

Every wire operator, treasury analyst, AP lead, dual-control approver, and BSA officer receives documented annual training on (a) lookalike-domain detection, (b) voice-clone awareness for callback verification, (c) urgency-language cadence recognition, and (d) the institution's escalation path for suspicious wire requests. Training records are tabbed in date order for examiner review.

NYDFS PART 500.13 &MIDDOT; DUAL-CONTROL WIRES

Dual-Control Wires Above the Defined Threshold & Non-Voice Confirmation Channel

NYDFS Part 500.13 requires dual control for wires above a defined threshold. The institution's threshold and the second approver's evidence — non-voice channel confirmation (signed callback, second live voice from a known number, in-person confirmation) — are documented. The dual-control policy is tested quarterly against simulated BEC and the second-approver evidence retains paper form.

FINCEN 2024 ADVISORY &MIDDOT; BEC / WIRE / SAR FILING

BSA Officer Notification & SAR Filing Within 4 Hours

Bank Secrecy Act officer is on the wire-fraud escalation path: notified within 30 minutes of a suspected wire fraud, opens a FinCEN SAR within 4 hours, and coordinates the FBI field-office contact. The FinCEN 2024 advisory on increasing BEC targeting of financial institutions is referenced in the institution's customer-awareness program and in the written escalation flow.

STAT

Only 13% of BEC victims recover any of the lost funds industry-wide. For institutions that engaged the FBI Financial Fraud Kill Chain (FFKC) inside 72 hours and filed IC3 with field-office escalation, recovery rose above 80% — but only when the bank, correspondent bank, and FBI field office coordinated real-time. Time is the single most expensive variable in BEC.

INCIDENT RESPONSE

First 60 Minutes After a Suspected Wire Fraud at a Bank

If a wire was sent and you suspect it was fraudulent, act immediately. The FBI Financial Fraud Kill Chain is a 72-hour window — measured from when the wire settles, not from when the bank confirms the fraud. Every hour reduces your chance of recovery, and the FinCEN SAR filing clock has its own expectations.

MINUTES 0–15 · STOP AND CALL THE BANK

- [ ] Do NOT reply to the suspicious email. Do NOT send any more wires from the affected operator station.
- [ ] Call your wire-room / correspondent-relationship bank's fraud department immediately. Request a wire recall and ask to engage the Financial Fraud Kill Chain (FFKC).
- [ ] If the wire was sent in the last 24 hours, request your bank contact the Federal Reserve directly. The FFKC only works inside 72 hours.
- [ ] If the wire went inter-bank (correspondent channel), notify the upstream / downstream correspondent bank immediately — they may be able to freeze on their side.
- [ ] Document every action: time, person called, what they said, next steps agreed.

MINUTES 15–30 · NOTIFY AND REPORT

- [ ] Call your local FBI field office (NOT ic3.gov alone — field-office escalation is what enables the FFKC). The FinCEN 2024 advisory notes that IC3-only reports have materially worse recovery rates than field-office-coordinated cases.
- [ ] File an IC3 complaint at ic3.gov — include all emails, wire confirmation, callback recordings if available, and any related correspondence. Time-stamp everything.
- [ ] Notify your cyber-insurance carrier — most policies have a 72-hour reporting window. File the claim immediately.
- [ ] Notify the Bank Secrecy Act officer. The BSA officer files the FinCEN SAR within 4 hours.
- [ ] Preserve the operator station and any phone / voice logs that captured the deepfake callback. Do NOT power off equipment.

MINUTES 30–45 · SECURE AND PRESERVE

- [ ] Lock the affected email account (lookalike-domain sender) and any other mailbox that touched the wire request. Enforce phishing-resistant MFA (FIDO2 / WebAuthn) if not already in place.
- [ ] Review email forwarding rules — attacker auto-forwarding is common in BEC.
- [ ] Check which other accounts may be affected — wire-room manager, dual-control approver, vendor portals.

- Pull correspondent-banking operational language for the upstream / downstream relationship. Most correspondent agreements require immediate notification.
- Brief the BSA officer on whether to file an end-of-day or end-of-week FinCEN SAR — coordinate so multiple SARs do not duplicate the same underlying event.

MINUTES 45–60 · LOCK DOWN AND BRIEF

- Stop all outgoing wires from the affected operator / approver pair until the incident is contained.
- Review all pending transactions — check for any other suspicious instructions in any operator queue.
- Brief the wire-room manager, BSA officer, and dual-control approval pool. Do not keep this quiet — every approver handling a wire should know.
- Update the wire-fraud-policy document. If this incident reveals a control gap (e.g., dual-control approver relying on a single voice channel), fix it before the next wire.
- Schedule a post-incident review with the FFIEC-aligned governance committee within 14 days. Document the attacker's entry point, the control that failed, and the new control being adopted.

LIVE TRAINING

Put This Into Practice — Live BEC Training for Finance & Banking Teams

The breach report is the starting point. Your wire operator, treasury analyst, dual-control approver, and BSA officer need to practice these controls under simulated pressure — not just read about them. That is what SecurEveryone's live training delivers.

PERSONAL

$150

1 session · 1 hour

Individual briefing on BEC anatomy, lookalike-domain detection, deepfake voice recognition, and the Verify-Out-Of-Band protocol. Good for a single wire operator or AP analyst.

Best for: Wire operators, treasury analysts, new hi

- 1-hour live BEC briefing
- Lookalike-domain walkthrough
- Verify-Out-Of-Band protocol training
- Callback script you can use today
- Certificate of completion

EXECUTIVE

$390

1 session · 90 minutes

For CEOs, CFOs, wire-approving officers, and dual-control approvers. Covers the complete finance-targeted BEC kill chain, the FFIEC CAT 2024 / GLBA / NYDFS crosswalk, and the 60-minute first-response runbook on a simulated wire.

Best for: CEOs, CFOs, controllers, BSA officers

- Finance-targeted BEC kill chain deep dive
- FFIEC CAT / GLBA / NYDFS / FinCEN crosswalk
- 60-min first-response runbook
- Live callback verification drill
- FFKC + FinCEN SAR escalation flow

BUSINESS

$900 flat

Unlimited users · 12 months

Full-team BEC defense training with every wire-room operator, dual-control approver, treasury analyst, and BSA officer included. Quarterly simulated BEC scenarios, FFIEC-aligned documentation, and the FinCEN-ready wire-fraud escalation language.

Best for: Banks, credit unions, fintechs, correspondent-banking ops

- Unlimited live sessions for 12 months
- Quarterly BEC tabletop exercises
- Wire-room-specific scenarios
- FFIEC CAT documentation
- FFKC + FinCEN SAR escalation archive
- Examiner-ready training records
- Cyber-insurance-ready incident file

CALL TO ACTION

Book a SecurEveryone Executive Session now. All sessions include the Finance & Banking BEC Breach Report, FFIEC CAT 2024 / GLBA / NYDFS / FinCEN crosswalk, and the 60-minute first-response runbook your team can reference.

ABOUT SECUREVERYONE

Cybersecurity Training for the Organizations That Cannot Afford to Get It Wrong

- Live, instructor-led sessions — not pre-recorded videos.
- Finance-specific scenarios: BEC wire fraud, spoofed-CEO request, deepfake CFO callback, vendor mailbox compromise, correspondent-banking ops.
- Verify-Out-Of-Band protocol training included with every session.
- Quarterly BEC tabletop exercises for Business tier clients.
- Compliance-ready documentation for FFIEC, GLBA, NYDFS Part 500, and FinCEN.
- Sessions delivered over Zoom, Meet, or Teams — whatever your team uses.

Ready to book?

Visit secureveryone.com/book or book directly from our Calendly:

secureveryone.com/book !’

SecurEveryone LLC · 1201 North Orange Street, Wilmington, DE 19801 · +1 (302) 212-0500 · info@secureveryone.com