Auto Attendant

AUTO ATTENDANT / RESEARCH & PRACTICAL GUIDANCE

Callback Verification Policy for Sensitive Requests (2026)

> Get a business phone number with a simple auto attendant menu from Auto Attendant. A caller picks who they need and the call rings that person's own mobile, so nobody on your team has to publish a personal number.

Published by Auto Attendant · 2026-11-08 · callback verification policy · sensitive phone requests · vishing prevention · caller id spoofing · out-of-band verification · vendor bank detail changes · business phone fraud prevention · front desk handoff

Original article: https://autoattendant.io/articles/verified-callback-policy-sensitive-business-call-requests



In this article

1. Executive Summary
2. Introduction and Background
3. Key Changes in Official Guidance and Call Handling
4. Implementation Considerations and Process Changes
5. Data Analysis and Evidence
6. Implications and Future Directions
7. Frequently Asked Questions (FAQs)
8. Conclusion

Executive Summary

A verified-callback policy answers one question for the person who picks up the main line: when a caller asks for something that moves money, opens access or discloses protected information, who is allowed to act, and on what evidence? Several U.S. official sources, each within its own scope and audience, give related advice. This report's position is that a matching number, a familiar name, a convincing voice or an urgent story is not proof, and that the check should run through contact details the business established independently, never through the incoming call. The FDIC Office of Inspector General (OIG) addresses banks and their business customers and tells them not to redial the number that called (FDIC OIG alert; redial advice). The FBI Internet Crime Complaint Center (IC3) advises secondary channels to verify requests for changes in account information (IC3 BEC guidance), and the FCC notes that a spoofed display can show a company a recipient already trusts (FCC spoofing guide).

The evidence base is real but bounded. IC3 recorded 1,008,597 complaints and $20.877 billion in reported losses for 2025 (IC3 2025 report), including 24,768 business email compromise (BEC) complaints (BEC table). The Federal Trade Commission (FTC) reported nearly $1 billion lost to business impersonators in 2025 (www.ftc.gov). The Association for Financial Professionals (AFP) reported that 30% of surveyed organizations were targeted by fraudulent phone calls (AFP survey highlights). None of these is a measure of small-firm phone scams, and none shows what a callback policy prevents. This report therefore claims no loss reduction. It describes what each cited source says, and the procedure it proposes is the author's own design, which none of the cited agencies has reviewed or endorsed.

The operational recommendation is a front-desk-to-owner handoff built from four parts. First, a request-type table (the handoff card) that says what the first answerer may do, what stops the call, who owns the decision, how a fresh contact is made and what evidence of approval is kept. Second, a neutral script that takes a nonsensitive reference and never asks for passwords, codes or account numbers. Third, a trusted-contact register with a named maintainer, an official source, a last-verified date, an authorized role and a backup. Fourth, synthetic drills scored on whether staff followed the steps, not on whether they guessed a voice was fake.

Identity and authority are separate checks. Reaching the right person proves who answered; the business's normal approval process, such as dual control, decides whether the payment, change or disclosure happens (Nacha 2026 risk management tips). Speed also matters after a suspected incident: IC3 says time is of the essence (IC3 2025 annual report), and FinCEN's Rapid Response Program has described a 72 hour reporting window in its 2022 fact sheet (FinCEN Rapid Response Program fact sheet). This scope is the United States only; Canadian reporting routes differ and are not covered here.

Introduction and Background

Small teams usually share one public phone number. A call to that number may ring a bookkeeper, an owner on a job site or a technician in a truck. That creates a specific decision problem: the person who answers is often not the person who may approve a payment, a password reset or the release of a file, and a caller's story

may be built to make them feel they are. This report is written for U.S. owners, office managers, bookkeepers and first-answer staff at businesses of roughly 2 to 20 people, including trades, agencies and small professional firms.

The scope is narrow. It covers inbound phone requests that touch money, access or confidential information, and asks what a first answerer should do in the first minute. It does not explain how to remove a spam label from an outbound number, does not teach call-authentication technology in depth and is not a general treatment of business email compromise. The sources are U.S. official documents, the reporting routes are U.S. routes, and nothing here is framed as a universal legal duty or extended to Canada.

Three terms recur. **Vishing** (voice phishing) is, in the Cybersecurity and Infrastructure Security Agency's (CISA) words, the social engineering approach that leverages voice communication (www.cisa.gov). **Caller ID spoofing** is the deliberate falsification of the information sent to a caller ID display (www.fcc.gov). **Out-of-band verification** means confirming a request over a different, independently established channel than the one that carried it. The Federal Communications Commission (FCC) adds that spoofing is not always illegal (www.fcc.gov), one more reason the display says nothing about legitimacy.

The evidence has limits. IC3 describes its statistics as an assessment taken at a point in time (www.ic3.gov). The Cleveland Fed's payments research brief of 2026-09-25 is context, not a phone-scam dataset: its footnote 8 says BEC has been one of the most common tactics against businesses over the last several years (www.clevelandfed.org). No source reviewed measures how often a callback procedure prevents a loss at a 2 to 20 person firm. The FDIC OIG alert was retrieved without a visible issue date, so it is cited here as retrieved in November 2026.

A disclosure: this report appears on autoattendant.io, which offers a flat-rate business phone number with a menu that rings team members' existing mobile phones. Routing of that kind finds the right colleague. It is inbound only, it is not an answering service, and it does not verify the requester or authorize any payment, disclosure or account change. Nothing below depends on a particular phone product.

Key Changes in Official Guidance and Call Handling

Change 1: Caller ID and a familiar voice are no longer treated as evidence

The FDIC OIG describes a scam in which the caller ID display is falsified so the call appears to come from the business's own bank (FDIC OIG alert), and the caller may know and use the real names of the business's employees (FDIC OIG alert). Its advice is blunt: assume any caller, even from what appears to be a known number, could be a scammer (FDIC OIG alert). The FCC adds that recipients may not be able to tell right away whether a call is spoofed (FCC spoofing guide), and a "local" display does not mean a local caller (FCC deepfake and robocall guide).

Call authentication does not close this gap for a front-desk decision. The FCC explains that STIR/SHAKEN (the call-authentication framework) lets the receiving phone company verify that a call is from the number displayed (www.fcc.gov). In an October 2025 proposal, the FCC observed that such information often does not let consumers know who is calling (docs.fcc.gov). Number-level assurance is not identity-level assurance.

Voice adds a second layer. The FTC warns that a call can sound like your boss asking for bank account numbers (consumer.ftc.gov), and the FBI states that AI-generated content is often difficult to identify (www.ic3.gov). Staff therefore cannot be asked to detect a fake. They can only be asked to follow a process that does not depend on detection.

Change 2: Verification runs through contact details the business established independently

The sources below give verification advice in their own words and for their own audiences. The FDIC OIG says not to redial the number that called (FDIC OIG alert) and to give an unsolicited caller no information (FDIC OIG alert). The FCC says to hang up and call the number on an account statement or in the phone book (FCC spoofing guide). IC3's November 2025 public service announcement (PSA) says to hang up, verify the correct number and call it yourself (IC3 November 2025 PSA), and its September 2026 PSA, which concerns impersonation of law-enforcement and government officials rather than business or vendor callers, says to use contact information other than that provided by the person contacting you (IC3 September 2026 PSA). The FTC says to use a phone number, website or email address you know is real (consumer.ftc.gov).

Two refinements matter for a small team. A "new" number for a known contact is itself a request to verify: the FBI says to confirm new contact information through a previously confirmed platform or trusted source (www.ic3.gov). And the source of the number matters more than the act of calling. Banks publishing their own guidance say the same: JPMorgan advises a trusted number from a system of record (www.jpmorgan.com), Frost Bank says never to use a number from an email thread, invoice or attached document (www.frostbank.com), and PNC says to use a number on your records instead of the one in the request (www.pnc.com). These are individual banks' recommendations, not regulatory requirements.

JPMorgan also lists relying on an inbound call to update contact information among practices to avoid (www.jpmorgan.com). A caller who "just wants to confirm the new details" is therefore not a verification path, even when friendly.

Change 3: Identity and authority are treated as separate checks

Reaching the right person answers "who is this?" It does not answer "may this person approve this?" The Nacha guidance for payment originators illustrates the split. It tells businesses to authenticate payment requests or changes to payment instructions by independently verifying the request or change (Nacha originator tips), and separately explains dual control: a fraudster may be able to get past one individual but will have difficulty tricking two (www.nacha.org). Wells Fargo describes the same idea as approval by a second user on a different device (www.wellsfargo.com), and U.S. Bank recommends dual authorization (www.usbank.com). PNC adds that businesses should limit who can initiate and approve payments (www.pnc.com). The older NIST small-business guide, now withdrawn, said no single individual should both initiate and approve a transaction (NIST IR 7621r1, withdrawn).

JPMorgan's callback guidance makes the same point from the contact side: speak to the person responsible for the change in payment instructions (www.jpmorgan.com). A callback that reaches a colleague who has no authority over the change completes a phone call, not a control. This is why the handoff card in the next section names an authorized owner for each request type.

Change 4: Speed after a suspected incident is emphasized, and the reporting routes are specific

IC3 tells victims of a fraudulent transfer that time is of the essence and to contact the financial institution immediately (IC3 2025 annual report). Its BEC page adds that requesting a reversal and indemnification documents as quickly as possible may reduce or eliminate losses (IC3 BEC page), a statement of possibility, not a guarantee. FinCEN's Rapid Response Program fact sheet, dated February 2022, reported greater success when transfers are reported to law enforcement within 72 hours of the transaction (FinCEN Rapid Response Program fact sheet), and tells victims not to contact FinCEN directly (FinCEN Rapid Response Program fact sheet).

Implementation Considerations and Process Changes

Step 1: Separate ordinary requests from sensitive ones

Most inbound calls are ordinary and should still get prompt, friendly service. A request becomes sensitive when it would change money, access or protected information. The following fictional examples are invented for illustration.

- **(Hypothetical Example) Ordinary:** A homeowner calls to move an appointment. The first answerer handles it and notes the change.
- **(Hypothetical Example) New payment details:** A caller says they are from a supplier, that the bank account on file has closed, and that the next invoice should go to a new account.
- **(Hypothetical Example) Bank impersonation:** A caller says the business account shows suspicious activity and asks the person who answered to read a code that was just texted.
- **(Hypothetical Example) Familiar voice:** A caller who sounds like the owner asks the office manager to buy gift cards for a client today and not to mention it to anyone.
- **(Hypothetical Example) Register change:** A caller asks to "update the callback number" for a vendor because the usual contact is on leave.

The FTC's small-business guide lists a call that seems to come from a trusted source among the ways cyber scams begin (www.ftc.gov), and notes that scammers want you to act before you have a chance to check out their claims (www.ftc.gov). The FDIC OIG likewise lists a false sense of urgency among warning signs (www.fdicoig.gov). In these examples the signals are urgency, secrecy and a request to bypass the usual approver, not voice quality.

Step 2: Define triggers with the owner

Triggers should be written by the owner or approver and adapted to the business's existing procedures. A starting list drawn from the sources:

- **New or changed payment details.** Central Pacific Bank lists requests to change payment processes, account information or wire transfers as a red flag (www.cpb.bank).
- **Urgent or unusual purchases or payments.** AFP's survey conclusion says immediate or emergency payments should be closely examined (www.truist.com).

- **Access, reset or code requests.** IC3 notes that companies generally do not contact you to ask for your username, password or one-time passcode (www.ic3.gov).
- **Confidential file or data requests.** CISA advises not giving out information about the organization unless you are certain of a person's authority to have it (www.cisa.gov).
- **Instructions that bypass the usual approver or require secrecy.** IC3 describes callers urging victims not to tell family, friends, financial institutions or law enforcement about the call (www.ic3.gov).
- **Any request to change the register itself.** Covered in Step 6.

Step 3: The one-page handoff card

Table 1 below is the proposed handoff card. It combines the dimensions a first answerer needs: the request type, what the first answerer may do, what stops the call, who owns the decision, how the independent contact is made and what evidence of approval is kept. It contains no account numbers or secrets, and should be adapted by the owner and the business's bank before use.

Request type	First answerer may	Stop and escalate if	Authorized owner	Independent contact route	Evidence of approval
Ordinary service enquiry (hours, quote, scheduling)	Handle normally; take name, nonsensitive reference and callback preference	The caller asks for money movement, access or protected details	First answerer	None needed	Job or ticket note
New or changed payment details (vendor, payee, payroll, beneficiary)	Take a neutral message; say changes follow the standard process; do not confirm or discuss existing details	Any change request, urgency, or "use this new number"	Bookkeeper or owner (named)	Number from the contact register or contract, not the caller, invoice or email (www.fhb.com)	Second approver's sign-off recorded; callback date and who was reached
Caller claims to be the business's bank	Say the team will return the call through the bank's published channel; end the call politely	Any request for credentials, codes or account details	Owner or designated account administrator	The bank's published number or relationship contact (www.jpmorgan.com)	Note of the bank contact reached and the matter confirmed
Access, password reset or code request	Take a neutral message; never read out, repeat or accept codes	Any request for a username, password or one-time code	Account administrator	Existing admin route in the register	Reset ticket from the provider's own portal
Confidential file or customer data request	Take a neutral message and a nonsensitive reference	Requester not already on an approved list, or asks for secrecy	Owner or data steward	Contact held in the register for that customer or agency	Written approval to release, and what was released
Familiar voice, unusual urgent request	Pause; offer to pass a message; do not act	Request involves money, gift cards, secrecy or bypassing the approver	The named approver (not the caller)	A known number or in-person check with the person (consumer.ftc.gov)	Approver's confirmation through the known route

Request type	First answerer may	Stop and escalate if	Authorized owner	Independent contact route	Evidence of approval
Request to change the register	Decline to act; take a message	Any request, from anyone, by phone	Register maintainer plus independent reviewer	A previously confirmed route (www.ic3.gov)	Two-person change log entry

Table 1 is a template. Its columns follow the guidance above: independent contact details (consumer.ftc.gov), a named person responsible for the change (www.jpmorgan.com) and a second approver where money moves (www.wellsfargo.com). The key design choice is the second column: the first answerer is never asked to decide whether a caller is genuine, only to pause, take a neutral message and hand off. The business must name actual people and backups for every "Authorized owner"; a role nobody holds is decoration, not a control.

Step 4: Give the first answerer a neutral script

A short script lets staff stop the request without confrontation or accusation:

- **Acknowledge.** "Thanks for calling. I can take a message for the right person."
- **Take a nonsensitive reference.** Name, company and a general topic. The FDIC OIG advises giving an unsolicited caller no information, including confirming name, business name or account information (www.fdicoig.gov).
- **State the standard process.** "Changes like that follow our standard verification process, and someone will contact you through our records."
- **Do not promise an emergency response.** The business line is for messages. If the caller insists on urgency, the answer stays the same.
- **End and hand off.** Pass the message privately to the named owner, as described in Step 7.

Two cautions apply. The first answerer should not ask callers for reusable secrets such as passwords, PINs or account numbers as a way of "proving" themselves, and should never collect payment card or bank credentials. Nacha's guidance points the same way: never provide password, username, authentication credentials or account details when contacted (www.nacha.org). And a friendly call is handled the same way as any other; the FTC's small-business guide states that an informed staff is the best defense (www.ftc.gov).

Step 5: Start a fresh verified contact

The authorized owner, not the first answerer, starts the callback. The sequence is:

- **Pause the requested action.** No payment, change, disclosure or reset happens during the call.
- **Find the contact in the register or another independent source.** A bank's number from its website or an account statement (www.fcc.gov), or a vendor's number from the contract or onboarding record (withdrawn NIST IR 7621r1), not from the caller, the invoice or a link in the message (First Hawaiian Bank guidance).

- **Reach the authorized contact.** For a vendor, that means the person with authority over payment instructions, not whoever answers.
- **Run the approval process separately.** Identity confirmation does not authorize the transaction. Apply the business's normal approval, including dual control where money moves (www.nacha.org).
- **Record what happened.** Date, who was reached, by which route and who approved.

NIST's older small-business guide described this for unsolicited callers: ask for the caller's name and office, say you will call right back (nvlpubs.nist.gov), and use the company's website or contract (IR 7621r1). It was withdrawn on 2026-11-02 and superseded by NIST Cybersecurity White Paper (CSWP) 50 (NIST withdrawal notice), which says to verify requests to change sensitive information, such as new routing numbers, with a trusted source (NIST CSWP 50). CSWP 50 is titled "Small Business Cybersecurity: Non-Employer Firms" and was written for firms with no employees other than the owner, though NIST says it may also be useful to businesses with very few employees, so it fits a 2 to 20 person team only partly. FinCEN's BEC analysis likewise recommends verifying suspicious payment instructions using multiple means of communication (www.fincen.gov).

One limit needs stating plainly: an independent callback can confirm that a vendor or bank asked for something, not that every request is legitimate, so the approver should still ask whether the change makes business sense. The business also needs a supported outbound way to call. A purely inbound phone service cannot supply one, so the owner should confirm which outbound line staff will use.

Step 6: Build and maintain the trusted-contact register

The register is the business's independently maintained list of who may ask for what, and how to reach them. It must not be built from incoming calls. *Table 2* below proposes its fields.

Field	What to record	Why it is there
Counterparty	Bank, key vendors, payroll and tax providers, insurers, major customers	Limits the register to relationships where a request could move money or data
Authorized role at the counterparty	The role with authority over payment instructions or account changes, not a named individual only	A callback should reach the person responsible for the change (www.jpmorgan.com)
Source of contact details	Contract, onboarding record, bank statement or the organization's official site; never a call, invoice or email (www.frostbank.com)	Establishes that the number was independently obtained (www.cisa.gov)
Register maintainer	A named person, with a named deputy	Someone must own updates, as with any contact list in an incident plan (nvlpubs.nist.gov)
Last verified date	Date and method of last check	Shows the entry is current; stale entries are reviewed first
Independent reviewer	A second person who reviews changes	Prevents a single request or a single mistake from changing the list

Field	What to record	Why it is there
Authorized internal approver and backup	Who approves, and who steps in when they are absent	Avoids urgent pressure to "just do it" when the approver is away
Access control	Who can view and who can edit; where stored	FTC guidance says each employee should have access only to resources needed for their job (www.ftc.gov)
Offline copy	A printed or offline copy for outages	CISA and NIST both advise printed or offline contact lists (www.cisa.gov) (nvlpubs.nist.gov)

The register is the only place a callback number may come from, so a request to change it is itself sensitive and gets its own row on the handoff card. Protect its access, and avoid copying sensitive customer data into generic task systems where many people can see it.

Step 7: Route sensitive messages privately

The general team may receive the initial call; only the authorized people need the details. Absence escalates to the named backup, not to everybody. The FTC advises keeping sensitive data only as long as there is a business reason (www.ftc.gov). If the business keeps written message notes, a written retention policy helps identify what must be kept (www.ftc.gov), and paper records should be shredded, burned or pulverized before disposal (www.ftc.gov). The FTC also advises training employees not to send passwords or sensitive information by email (www.ftc.gov). Retention rules vary by business and contract, so confirm them with the owner's advisers.

A note for teams using forwarded calls: some setups present the business number, not the original caller's number, on the mobile that rings, so the screen can neither confirm nor contradict the caller. Check with the provider whether the original number is exposed after forwarding before relying on it for anything.

Step 8: Rehearse with synthetic calls and measure compliance

CISA says tabletop exercises do not have to be large productions (www.cisa.gov), and one of its example scenarios has a bank phoning an accountant about transfers the accountant did not initiate (www.cisa.gov). NIST CSWP 50, which is written for the smallest firms, advises practicing the incident response plan with tabletop exercises (NIST CSWP 50). CISA's incident-response guidance adds that people who report false alarms should be treated graciously (www.cisa.gov) and that retrospectives must be blameless (www.cisa.gov). *Table 3* proposes a drill sheet. All of the scenarios are synthetic and are proposed tests, not experiments that have been performed.

Drill (Hypothetical Example)	Setup	Required steps	Pass means
Spoofed-looking bank callback	A tester calls, says the account shows suspicious activity and asks for a code	Pause; neutral message; no code shared; owner calls the bank's published number	Every required step done; no information disclosed (www.fdicoig.gov)

Drill (Hypothetical Example)	Setup	Required steps	Pass means
Genuine supplier, changed payment details	A tester plays a real supplier asking to update bank details	Neutral message; hand-off; callback to the register number; second approver signs off	Change made only after both steps; evidence recorded
Familiar voice, unusual urgent request	A tester imitates the owner asking for an urgent purchase and secrecy	Pause; do not act; reach the real owner by a known route (consumer.ftc.gov)	Request held until confirmed through the known route
Employee absence	The named approver is unreachable	Message goes to the named backup, not to everyone	Time to reach an authorized backup is recorded
Request to update the register	A tester asks to change a vendor's callback number	Decline; route to maintainer and independent reviewer	Register unchanged until two-person review
Normal customer enquiry	A tester asks for an appointment and an estimate	Handle promptly and politely	Service not slowed; nothing escalated unnecessarily

Table 3 scores compliance, not fake detection. The local measure is drills meeting all required steps divided by drills run, plus the time to reach an authorized backup. Neither number should be extrapolated to fraud reduction, revenue or an industry benchmark. The last row matters as much as the others: a policy that blocks ordinary customers fails in a different way.

An optional staffing worksheet can estimate the cost of the process itself, kept separate from any loss-prevention forecast, which lacks evidence. The formula is extra verification minutes per sensitive call, times the number of such calls, divided by 60, times the internal hourly cost. **(Hypothetical Example)** If a firm handles 6 sensitive callbacks a month at 12 extra minutes each and an internal cost of $40 per hour, the cost is 6 × 12 ÷ 60 × $40 = $48 per month. The inputs are invented, and a business should replace them with its own measured values.

Step 9: If an instruction was already acted on

Stop acting on the instruction, then use the bank's established reporting channel and current U.S. official routes. IC3 sets out three steps:

- **Bank first.** Contact the originating financial institution as soon as fraud is recognized (www.ic3.gov).
- **Ask for a reversal.** Request a reversal of the transfer and a Hold Harmless Letter or Letter of Indemnity (www.ic3.gov).
- **File with IC3.** File a detailed complaint with IC3 (www.ic3.gov).

Other U.S. routes exist. The FTC directs businesses to report phishing attempts, fake invoices and other scams at ReportFraud.ftc.gov (consumer.ftc.gov). The FDIC OIG hotline handles reports of criminal activity involving an FDIC-regulated or FDIC-insured bank (www.fdicoig.gov). For unwanted or spoofed calls, the FCC guide asks complainants to note if a number is being spoofed, blocked or mislabeled (www.fcc.gov). The right route depends on the facts, and none of them guarantees recovery. A business that has lost money should speak with its bank and with its own attorney or accountant; this report is not legal advice and reaches no legal conclusions.

Data Analysis and Evidence

None of the figures below measures phone scams at 2 to 20 person firms, and none measures how well a callback procedure works. They describe the environment the policy operates in.

- **IC3 complaint data, 2025.** IC3 reported 1,008,597 complaints and $20.877 billion in losses for 2025, a 26% increase in losses from 2024 (IC3 2025 annual report). BEC accounted for 24,768 complaints (IC3 2025 annual report) and $3,046,598,558 in adjusted losses (IC3 2025 annual report). These are complaints submitted to IC3, not measures of prevalence, and IC3 notes possible duplicates (IC3 2025 annual report).
- **FTC reports.** The FTC reported that people lost a staggering $3.5 billion to imposter scams in 2025 (www.ftc.gov), and nearly $1 billion to business impersonators (www.ftc.gov). It noted that some of the costliest impersonation scams start with a fake security alert, often from a bank (www.ftc.gov). FTC and IC3 data are separate, self-reported datasets and must not be added together.
- **AFP survey.** The Association for Financial Professionals' (AFP) 2026 survey, conducted in January 2026 among 465 treasury practitioners (www.financialprofessionals.org), found that 76% of U.S. organizations experienced attempted or actual payments fraud in 2025 (www.financialprofessionals.org). The report states that nearly 75% experienced email or BEC fraud and 30% were targeted by fraudulent phone calls (www.truist.com), and lists attempts to change bank account details among phone fraud types (www.truist.com). Nacha relays AFP's finding that 74% of organizations experienced BEC, up from 63% in 2024 (www.nacha.org). Respondents are treasury practitioners at U.S. organizations of varying sizes, and the highlights document gives no 2 to 20 person split. AFP says smaller firms face fraud less frequently but lack the recovery infrastructure of larger firms (www.financialprofessionals.org).
- **Reported control use.** Respondents reported on callback-style controls: verifying fund transfer requests by calling an authorized contact at the payee (www.truist.com) and policies to verify changes to invoices, bank deposits and contact details (www.truist.com). In the highlights table, 94% and 96% of respondents respectively reported having implemented them, while 42% reported using passcodes known only to both parties (www.truist.com). Respondent-rated effectiveness is opinion, not measured prevention, and the highlights do not state denominators. The figures show that callback controls are common among surveyed treasury teams, not that they work.
- **FinCEN Rapid Response Program.** FinCEN's 2025 Year in Review lists Phone Scam as a typology with $18,577,595.74 frozen in fiscal year 2025 (www.fincen.gov), against $90,954,662.26 for BEC (www.fincen.gov). These are amounts frozen through one referral program, not national totals.
- **Reading the numbers together.** The official sources point to a similar control (independent verification) although they measure different things. No source quantifies the benefit for a small firm, so a claimed percentage reduction would be unsupported. The process cost is small and measurable by the firm itself, as the Step 8 worksheet shows. The Cleveland Fed brief adds that PDF invoices sent via email are particularly vulnerable (www.clevelandfed.org); it lists the 2026 AFP survey among its references (www.clevelandfed.org), so it partly restates that survey and is not independent confirmation.

Implications and Future Directions

- **The policy is a handoff, not a detection skill.** The guidance reviewed assumes people cannot reliably judge authenticity by ear or by screen. A procedure that asks staff to pause, record and hand off sidesteps that problem. IC3 also says BEC continues to target small local businesses (www.ic3.gov), so a small headcount does not exempt a team.
- **Phone systems are a routing layer, not an authority layer.** A shared number with a menu finds the right colleague. It does not know who is calling, whether a request is legitimate or who may approve it. Owners should verify several open facts before relying on any phone service here: the bank-approved verification channel, whether the backup is reachable and accessible, whether the service shows the original caller number after forwarding, and what note retention the business requires. An inbound-only routing menu, which is what autoattendant.io provides, supplies no outbound verification line, so the owner must choose a supported outbound route. Needs that call for an answering service, which would answer on a business's behalf, or an outbound contact-centre suite are outside what a routing menu does, and readers who need them should look to providers of that kind.
- **Likely developments.** Nacha's October 2026 practical-steps article lists clear procedures for validating payment instruction changes (www.nacha.org), verifying account information using trusted channels (www.nacha.org) and additional approvals for higher-risk or unusual transactions (www.nacha.org). IC3's September 2026 PSA reports scammers spoofing numbers, names and credentials (www.ic3.gov). A reasonable expectation is that banks and associations keep publishing procedural controls, though no source reviewed forecasts a specific change. NIST's withdrawal of its older small-business publication (nvlpubs.nist.gov) shows the reference points themselves move, so the policy needs a review date.
- **What would improve the evidence.** A small-business-specific study of inbound phone requests, and drill results from real teams measured as compliance rates, would be more useful than any figure here. Until then the procedure is this report's own design, informed by official guidance, cheap to run and of unmeasured effectiveness.

Frequently Asked Questions (FAQs)

How do I verify a phone call request before acting on it?

Do not act during the call. Pause the request, then reach the organization through contact details obtained independently, such as the number on an account statement (www.fcc.gov) or in the contact register, and reach a person with authority over the matter (www.jpmorgan.com).

What is the call back verification procedure for wire transfer requests?

Treat any request to change beneficiary details or send an urgent wire as a trigger. Use secondary channels to verify requests for changes in account information (www.ic3.gov), call a number from your own records rather than the request (www.pnc.com), then apply a second approver (www.wellsfargo.com). Ask the bank which channel it treats as approved.

What belongs in a vishing prevention policy for a small business?

A short list of triggers, a neutral script, a register of independently sourced contacts, a named approver with a backup, private routing, drills and an incident route. The FTC advises an office policy of double-checking by contacting the company on a number you know is genuine (www.ftc.gov), and CISA says staff must be formally trained (www.cisa.gov).

Is there a callback verification policy template?

Table 1 (the handoff card) and Table 2 (the register) are starting templates, not legal or banking advice. Adapt them with the business's bank and advisers, and keep account numbers and secrets out of any shared copy.

How do I verify a caller's identity for a sensitive request?

Not during the call, and not by asking for passwords, codes or account numbers. Verification happens afterward through an independent route, and authority is checked separately through the approval process (www.nacha.org).

What is out-of-band verification for phone requests?

Confirmation over a different channel than the one that carried the request. Wells Fargo describes verification using a different communication channel than the one used to make the request (www.wellsfargo.com), and IC3 recommends secondary channels for account changes (www.ic3.gov).

What are the best practices for preventing business phone fraud?

Independent contact details, a second approver for money movement, training and known reporting routes. NIST says to teach employees how to spot and report a phish (www.nist.gov). Effectiveness for small firms is unmeasured.

How does caller ID spoofing affect business protection?

It removes the display as a basis for trust. Spoofed displays can show a company or agency you already know and trust (www.fcc.gov), so a displayed number does not authorize a request.

Conclusion

Several U.S. official sources cited in this report, including the FDIC OIG, IC3, the FCC and the FTC, advise verifying a phone request through a contact the business knows to be genuine rather than through the incoming call. Separating the approval of money movement or an account change from caller identity, and requiring a second person to approve, is this report's own design; the sources cited for it are Nacha, bank guidance and a withdrawn NIST guide, and no government agency is claimed to have endorsed it.

For a team of 2 to 20 people, the handoff card, trusted-contact register, neutral script and drill sheet turn that guidance into a decision a first answerer can follow in seconds. The first answerer pauses, takes a nonsensitive reference, states the standard process and passes the message privately. The authorized owner starts a fresh contact from the register and runs the normal approval. A suspected incident goes to the bank and the U.S. reporting routes without delay.

The limits bear repeating. The data cited measure complaints and survey responses, not this procedure. A callback cannot establish every request's legitimacy, and no route guarantees recovery. Owners should adapt the templates with their bank, accountant and attorney, set a review date, and measure only what a small team can: drills that met every step, and the time to reach an authorized backup.

A shared number routed to each person's existing mobile can help reach the right colleague, but it is a routing layer only and does not verify or authorize anything.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.fdicoig.gov/call-spoofing-scams
2. https://www.ic3.gov/CrimeInfo/BEC
3. https://www.fcc.gov/consumers/guides/spoofing
4. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
5. https://www.ftc.gov/news-events/news/press-releases/2026/06/ftc-data-show-people-reported-losing-3-point-5-billion-imposter-scams-2025
6. https://www.truist.com/content/dam/truist-bank/us/en/documents/info/cci/2026-afp-payments-fraud-control-survey-report-key-highlights.pdf
7. https://www.nacha.org/news/tips-originators-comply-2026-risk-management-rules
8. https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf
9. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
10. https://www.clevelandfed.org/publications/payments-research-brief/2026/prb-20260925-b2b-payments-part-two
11. https://www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot
12. https://www.fcc.gov/call-authentication
13. https://docs.fcc.gov/public/attachments/FCC-25-76A1.pdf
14. https://consumer.ftc.gov/consumer-alerts/2024/04/fighting-back-against-harmful-voice-cloning
15. https://www.ic3.gov/PSA/2025/PSA250515
16. https://www.ic3.gov/PSA/2025/PSA251125
17. https://www.ic3.gov/PSA/2026/PSA260917
18. https://consumer.ftc.gov/features/how-avoid-imposter-scams
19. https://www.jpmorgan.com/insights/cybersecurity/business-email-compromise/when-callbacks-go-wrong
20. https://www.frostbank.com/dam/Docs/BusinessPDFs/BusinessInsights-EmailCompromise.pdf
21. https://www.pnc.com/insights/small-business/running-your-business/payment-fraud-checklist-for-business-owners.html
22. https://www.wellsfargo.com/com/fraud/fraud-schemes
23. https://www.usbank.com/dam/en/documents/pdfs/customer-services/usbank-gtm-payment-fraud-solutions-update-final.pdf
24. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
25. https://www.ftc.gov/business-guidance/resources/scams-your-small-business-guide-business
26. https://www.cpb.bank/insight-topics/2024/fraud/essential-tips-for-safeguarding-your-business-from-wire-transfer-fraud

27. https://www.fhb.com/en/resource-center/small-business/protect-your-business-from-vendor-impersonation-and-invoice-fraud
28. https://www.nacha.org/sites/default/files/2019-04/NACHABECVIF.pdf
29. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.50.pdf
30. https://www.fincen.gov/sites/default/files/shared/Financial_Trend_Analysis_BEC_FINAL.pdf
31. https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/teach-employees-avoid-phishing
32. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
33. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
34. https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf
35. https://consumer.ftc.gov/consumer-alerts/2026/05/run-small-business-pay-your-bills-not-scammers
36. https://www.fdicoig.gov/oig-hotline
37. https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts
38. https://www.financialprofessionals.org/about/learn-more/press-releases/Details/over-75-percent-of-us-firms-experienced-payments-fraud-in-2025-while-ai-adoption-for-fraud-mitigation-lags
39. https://www.nacha.org/news/business-email-compromise-attempts-rose-sharply-2025-report-finds
40. https://www.fincen.gov/system/files/2026-05/FinCEN-Year-in-Review-2025.pdf
41. https://www.ic3.gov/PSA/2024/PSA240911
42. https://www.nacha.org/news/practical-steps-corporate-payment-practitioners-reduce-credit-push-payments-fraud
43. https://www.cisa.gov/cyber-guidance-small-businesses
44. https://www.nist.gov/itl/smallbusinesscyber/phishing

THE PUBLISHER

About Auto Attendant

Auto Attendant gives a small business one phone number and a recorded menu that sends each caller to the right person. The call rings the mobile that person already carries, using their normal dialler and their normal mobile plan. Pricing is a single flat monthly fee for the whole company rather than a charge for each user, and there is no app, desk phone or hardware to install.

One number, one menu, the phones you already own

A caller dials the business number, hears a short greeting and chooses an option. Each option can ring one mobile, ring several at once so whoever is free answers first, or try people one after another in a set order. There is no limit on how many people sit on the receiving end, because nobody is billed per seat. Setup is done by the owner in a few minutes: pick a number, write the greeting, and point each option at a mobile.

What it deliberately is not

An auto attendant routes a call; it does not answer one. Nobody at Auto Attendant speaks to callers, and no AI stands in for a receptionist. A business that wants its calls handled, messages taken and appointments booked wants an answering service, which is a different product at a different price. A business that needs call recording, queues, agent dashboards or CRM integration wants a contact centre platform. Auto Attendant is for the case where the call should simply reach the right pocket.

Keeping personal numbers off the internet

The business number is the only number a caller ever sees. Personal mobile numbers are never displayed and never given out, which is what lets an owner put a number on a website, an invoice, a van or a Google Business Profile without handing a personal line to everyone who finds it. An existing advertised number can be ported across and kept, and the old line keeps working while the port is in progress.

Work with Auto Attendant

Visit Auto Attendant to see how it works, how it compares to a personal mobile, Google Voice and a full phone platform, and the current pricing.

Telephone number portability, emergency calling and caller-ID rules differ by country and change over time. Articles published here describe general practice and cite primary regulator and carrier sources; they are not a guarantee of any timeline, and they are not legal or regulatory advice for a specific business.

Website: https://autoattendant.io

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.