Auto Attendant

AUTO ATTENDANT / RESEARCH & PRACTICAL GUIDANCE

Take Payment Over the Phone During a Business Call: 3 Methods

> 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 · 2026-10-31 · take payment over the phone · payment link vs virtual terminal · secure keypad phone payments · dtmf masking · pci compliant phone payments · virtual terminal for phone orders · mail order telephone order · small business payments

Original article: https://autoattendant.io/articles/payment-link-vs-virtual-terminal-vs-secure-keypad

In this article

1. Executive Summary
2. Introduction and Background
3. Path 1: Customer-Entered Payment Link
4. Path 2: Staff-Entered Virtual Terminal
5. Path 3: Specialist Keypad and Masking Services
6. Feature Comparison
7. Performance and Benchmarks
8. Implementation: Questions, Fallbacks and Acceptance Testing
9. Data Analysis and Evidence
10. Implications and Future Directions
11. Frequently Asked Questions (FAQs)
12. Conclusion

Executive Summary

A small firm that wants to take a card payment during a business call has three realistic collection paths: a payment link that the customer opens and completes on a provider-hosted page, a virtual terminal where an authorized employee types the card details, and a specialist telephone service that captures the keypad tones so the employee never hears the digits. This report compares them by one test: which people, devices, recordings and inboxes touch the card details. The Payment Card Industry Data Security Standard (PCI DSS) applies wherever payment card account data is stored, processed or transmitted, and PCI SSC FAQ 1153 (dated October 2012) says VoIP traffic that contains account data is in scope for applicable PCI DSS controls, which this report reads as leaving no separate telephone exemption, with scope starting where the traffic reaches the merchant's own infrastructure and not extending to the cardholder's own carrier path (www.pcisecuritystandards.org). The November 2018 telephone-payment supplement is guidance that expressly does not supersede PCI DSS, and its stated goal is that sensitive authentication data is never stored after authorization (listings.pcisecuritystandards.org).

A hosted link moves card entry onto the provider's page, for example Stripe's, which redirects the customer to a Stripe-hosted payment page (docs.stripe.com). That does not end the merchant's duties: the PCI Security Standards Council (PCI SSC) says merchants that redirect still carry the requirements in their Self-Assessment Questionnaire (SAQ) A (www.pcisecuritystandards.org). A virtual terminal keeps the employee's device in the data path, and PayPal states that the merchant secures the device and browser used to reach the terminal (securepayments.paypal.com). A keypad-masking service is described by vendors as removing tones before they reach the agent (sycurio.com), and the supplement says a well-designed deployment can take the agent environment and the customer-record system out of scope (listings.pcisecuritystandards.org). Those are vendor and supplement statements, not a certification of any particular firm.

Recording and voicemail are separate leak paths. PCI SSC FAQ 1210 (June 2025) says that if sensitive authentication data is collected on a call, every effort must be made to prevent it being recorded (www.pcisecuritystandards.org); it does not say that every payment call recording is unlawful. A Microsoft

Teams voicemail is delivered as an ordinary email with the audio attached (learn.microsoft.com), so a caller who reads a card number into a mailbox creates a stored copy.

Published US fees as of October 2026 differ by path: Square lists 3.5% + 15¢ for manually entered payments (squareup.com) and 3.3% + 30¢ for an online payment link (squareup.com). No independent benchmark of completion rates, fraud or savings exists in the sources reviewed, so the cost worksheet in this report uses owner inputs rather than assumed rates. A routing-only business number can send the call to the right person, but it cannot itself collect payment details. The decision ends with questions for the acquirer, and validation requirements are set by the payment brands and acquirers, not by business size (www.pcisecuritystandards.org).

Introduction and Background

The target question, how to take payment over the phone during a business call, is usually answered with a product list. That framing hides the more useful question: when the customer says "go ahead and charge the card," where do the digits go? Each hand-off, from the customer's keypad or voice to a phone platform, an employee's ear, a browser tab, a notes field or a voicemail inbox, either brings that system into the payment process or keeps it out.

This report is written for owners and office managers at two-to-twenty-person trades and professional-service firms in the United States who ask for deposits, settle invoices or accept telephone orders. The Small Business Administration (SBA) Office of Advocacy counts 36,207,130 small businesses in the United States as of its February 2026 release (advocacy.sba.gov), so the audience is large and mostly outside enterprise compliance teams. PCI DSS is an industry standard with international application, not a universal US statute, and the payment brands and acquirers decide what each merchant must validate. PCI SSC says the standard is intended for all entities involved in payment processing, whatever their size (www.pcisecuritystandards.org), and that whether a small merchant must validate is determined by the individual payment brands (www.pcisecuritystandards.org).

Choose the payment job first

Three jobs recur in small-firm calls:

- **Deposit or invoice during the call.** The customer is on the line and ready to pay now.
- **Remote payment later.** The call ends with an agreed amount and the customer pays afterwards.
- **Caller without usable web access.** No smartphone, limited data or a preference for the telephone.

A link suits the second job well, a terminal or keypad flow suits the first and third, and the third also needs an assisted alternative, covered later.

What this report does not do

It does not assign an SAQ category, certify any workflow, or script how to read card numbers aloud. Its aim is a decision and a question list for the acquirer. Call-recording consent and the recording notice are covered in the publisher's separate small business call recording checklist, so this report starts at the choice of collection method.

Where a routing-only phone number fits

The publisher of this article sells a flat-rate business phone number with a multi-option auto attendant that rings team members' existing mobiles. It is a routing product: it is not an answering service, an AI receptionist or a payment processor, and nothing in this report implies it supplies keypad payments or any compliance certification. Such a number can send "billing question" callers to the right person or to a recorded instruction. Whatever payment capability follows has to come from a separate payment provider or telephony service. Some routing products, including this one, email voicemail with the recording and a transcript, which matters for the data-hygiene section below.

Evidence base and its limits

The primary sources are PCI SSC FAQs, the 2018 supplement and the SAQ documents. The supplement is dated and supplemental. Vendor pages describe only their own services. Institutional policies, such as those of universities and a state treasury, are included as examples of how organizations operationalize the same documents, not as rules for small firms. No source reviewed supplies a controlled comparison of completion rates, fraud rates or savings, and none is claimed here.

Path 1: Customer-Entered Payment Link

Capabilities

In this path the employee creates a link for a defined amount, delivers it, and the customer enters card details on the provider's page. Stripe documents that its Payment Links redirect customers to a Stripe-hosted payment page (docs.stripe.com), and Square describes the same shape: the customer opens a secure online checkout page and submits payment there (squareup.com). Delivery channels are broad, and the Federal Trade Commission (FTC) advises using Transport Layer Security (TLS) or another secure connection to protect card information in transit (www.ftc.gov). Stripe lists email, SMS or social media (docs.stripe.com); PayPal lists email, text messages, social media and messaging apps (www.paypal.com); Square lists email, WhatsApp or SMS (squareup.com). SumUp's US help center states that customers enter payment details through its online portal (help.sumup.com).

The payment journey is short. The caller hears the amount on the call, receives the link by text or email, enters the card on the provider's page, and the merchant sees a confirmation. The employee's device, the phone platform and any recording never carry the digits, provided the caller does not read them aloud as a shortcut.

Adoption and provider support

Hosted links are offered by the major small-business processors reviewed. Pricing is typically bundled: Stripe lists Payment Links as included at no additional charge for businesses on standard payments pricing (stripe.com), and PayPal lists no setup cost or monthly fees (www.paypal.com). Not every merchant qualifies; SumUp's US help center notes additional security restrictions for payment links (help.sumup.com). No source reviewed publishes the share of small firms that use links on phone calls, so adoption is described only as provider support, not as market share.

Strengths and limitations

The main strength is data flow. The card number is typed by the person who owns the card, into a page operated by a payment provider, rather than spoken to an employee. The PCI SSC telephone supplement notes that sending a link through a messaging service may be treated like an e-commerce merchant redirecting to third-party payment pages, while still requiring the link's integrity and validity to be evaluated (listings.pcisecuritystandards.org).

The limits are practical and regulatory. First, a hosted page does not remove all merchant duties. PCI SSC states that merchants whose pages redirect to a third-party processor or embed its inline frame still have responsibility for the requirements in SAQ A (www.pcisecuritystandards.org). Stripe likewise says that businesses must handle card data in a PCI-compliant manner and attest annually (docs.stripe.com). Second, links can be reusable. Stripe documents that a link can be reused with multiple customers or limited by number of purchases (docs.stripe.com), PayPal says a single link can be shared with multiple customers (www.paypal.com), and Stripe's documented control is deactivation, after which customers can no longer use the link (docs.stripe.com). For a one-customer deposit, owners should ask how to issue a single-use or customer-specific request. Third, a link requires a device and connectivity on the caller's side, which is the accessibility problem addressed later.

A distinction matters throughout: sending a payment link is not the same as sending card information by text. PCI DSS Requirement 4.2.2, as described in a PCI SSC FAQ, prohibits sending unprotected primary account numbers (PANs) through end-user messaging technologies (www.pcisecuritystandards.org), and the same FAQ lists email, instant messaging, SMS and chat as such technologies. A link contains no card number, but the message thread should still be treated as a channel where a customer might reply with digits, and the handoff checklist below says what the employee does if that happens.

Path 2: Staff-Entered Virtual Terminal

Capabilities

A virtual terminal is a browser page where an authorized employee keys the card details the customer reads out. PayPal describes it as a browser-based interface where a merchant manually enters card details (securepayments.paypal.com) and lists phone orders among the uses. SumUp offers terminal entry on any desktop or mobile device (www.sumup.com), and Authorize.net describes its terminal as especially useful for mail order or telephone order (MOTO) payments (support.authorize.net). Square lists no monthly fee or commitments for its terminal (squareup.com), and its help article lists the fields keyed in: card number, expiration date, security code and billing postal code (squareup.com).

Some terminals also send a payment link by text, which blends Path 1 into Path 2. SumUp's terminal page describes a customer entering card details on a secure payments page (www.sumup.com), and Square lists a separate fee line for payment links sent by text from the terminal (squareup.com). Stripe names Payment Links and Hosted Invoices as alternatives to manually entering card information (support.stripe.com).

Adoption and provider support

Provider gating varies. Stripe says that before MOTO transactions can be enabled, Stripe must verify the account (docs.stripe.com). Authorize.net notes that address fields must be enabled and required in order to run Address Verification Service (AVS) checks (support.authorize.net). Visa's 2016 fraud-prevention webinar tells merchants to use AVS to verify the cardholder billing address (usa.visa.com); because that document is dated, owners should confirm current card-brand rules with the acquirer.

Strengths and limitations

The strength is control: the employee can ask for AVS and card-security data and handle declines on the call. The West Virginia State Treasurer's handbook, for its agencies, says phone payment details should be entered directly into the terminal or encrypted keypad (wvtreasury.gov), which shows how institutions narrow the data path. The limitation is that the employee's ear, device, browser and network sit in the data path. PayPal states that the merchant is responsible for securing the device and browser used to access the terminal (securepayments.paypal.com), and Stripe says that for manually entered cards the merchant is responsible for protecting the card data under PCI requirements (support.stripe.com).

The PCI SSC SAQ for virtual terminals sets out when the narrowest questionnaire applies. SAQ C-VT covers merchants who key one transaction at a time into an internet-based virtual payment terminal, and it requires that the terminal is reached only from a device isolated in a single location (listings.pcisecuritystandards.org). A shared office laptop that also reads email, or a staff mobile that also runs the voicemail app, may not fit that description. Eligibility wording can change between SAQ versions, so the questionnaire the acquirer requests, not a marketing label, is the reference.

Institutions show the practical consequences. The University of California, Santa Barbara states that VoIP phones connected to campus networks are not PCI compliant (bfs.ucsb.edu), and the University of Louisville policy states that VoIP is not considered PCI compliant (louisville.edu). Those are organizational policies. PCI SSC FAQ 1153 (October 2012) says that PCI DSS requirements apply wherever payment card account data is stored, processed, or transmitted, and that VoIP traffic containing such data is in scope for applicable PCI DSS controls, although scope starts where the traffic reaches the entity's own infrastructure and does not extend to the cardholder's own carrier path. The difference matters for a small firm: the policies are conservative local rules, but the underlying scope question, which systems touch the digits, is the same one an owner has to answer.

Path 3: Specialist Keypad and Masking Services

Capabilities

In a keypad flow the customer types card digits on the phone keypad. The system captures the dual-tone multi-frequency (DTMF) tones and sends the digits to the payment gateway while the employee stays on the line. The PCI SSC supplement defines masking as replacing the tones with a random or flat tone (listings.pcisecuritystandards.org). Vendors describe the result consistently. PCI Pal says tones are intercepted and masked with a monotone comfort beep for the agent (www.pcipal.com); Sycurio says the system detects the tones and removes them before they reach the agent (sycurio.com) and that customers stay on the call

with an agent (sycurio.com); Twilio's payment API says agents are not able to hear any DTMF tones (static1.twilio.com). Twilio adds that its Pay verb redacts captured digits from logs (www.twilio.com). These are vendor claims about their own services.

Adoption and provider support

Developer platforms expose the flow as an API: Telnyx documents a caller guided through interactive voice response (IVR) prompts to enter payment details via DTMF (developers.telnyx.com), and Twilio documents a PCI Mode that includes built-in DTMF redaction (www.twilio.com). Integration details constrain the choice. Twilio's tutorial says Pay Connectors require PCI Mode to be enabled in the console (www.twilio.com), and its Studio widget supports only the Stripe connector (www.twilio.com). Telnyx notes that its API does not enforce HTTPS on the connector endpoint, so the merchant must configure a secure one (developers.telnyx.com). Business phone vendors may not provide the flow at all: Dialpad says it is not a PCI processor for payment workflows (www.dialpad.com). These are build-it-yourself or integrator-assisted options, and a 2 to 20 person firm will usually need a reseller or a payment-aware telephony provider rather than writing code.

Strengths and limitations

The supplement says a properly designed and deployed DTMF-masking solution can take the telephony environment, the agent environment and the customer-record system out of scope. It also explains the weaker alternative. Pause-and-resume stops the recording during card entry, which can take recording and storage systems out of scope, but it does not reduce PCI DSS applicability to the agent, the agent desktop or other telephone systems, because the agent still hears the card data (listings.pcisecuritystandards.org). The supplement lists a common failure: the agent forgetting to pause at the right time, leaving card data in the recording (listings.pcisecuritystandards.org). Genesys documents that agents must manually activate Secure Pause (help.genesys.cloud), and Dialpad documents that agents can pause their recordings to take payment data (www.dialpad.com).

Vendors differ on how they describe the trade-off. PCI Pal says pause-and-resume still leaves infrastructure and agents in scope (www.pcipal.com), while Eckoh says masking lets recording continue safely because tones are suppressed (www.eckoh.com). Where the platform is a build-your-own one, Telnyx says ongoing recordings are masked during the Pay session (developers.telnyx.com), and Twilio says voice recordings in a PCI workflow require PCI Mode (www.twilio.com). The common limit is that scope reduction depends on the actual configuration, including exports, logs, transcripts and notifications. The supplement itself is supplemental and does not add, extend, replace or supersede PCI DSS requirements (listings.pcisecuritystandards.org).

Feature Comparison

Table 1 below sets the three paths, plus the pause-and-resume variant, against the questions this report started with. It is an original synthesis of the sources cited in the sections above, not a vendor claim, and every cell should be confirmed with the acquirer.

Method	Who enters the data	Who can hear or see it	Systems touched	Evidence to request	Failure fallback
Customer-entered link	Customer, on the provider's hosted page (docs.stripe.com) (help.sumup.com)	Provider page only, if the caller does not read digits aloud	Message channel carries the link; hosted page; confirmation email or dashboard	Written confirmation of the questionnaire type the acquirer expects; link delivery and single-use controls (docs.stripe.com)	Resend link, switch to assisted keypad or terminal (support.stripe.com); never ask for digits by text
Staff-entered virtual terminal	Authorized employee, keyed from what the customer says (securepayments.paypal.com) (support.authorize.net)	Employee hears and sees it; anyone nearby; any active recording	Employee device and browser; phone platform audio; recording and transcripts if on	Isolated-device eligibility if SAQ C-VT is sought; recording suppression settings (www.pcisecuritystandards.org)	Retry keyed entry, or send a link from the terminal (squareup.com) (www.sumup.com)
Keypad with DTMF masking	Customer, on the phone keypad (developers.telnyx.com)	Customer only; vendors state the agent hears a flat or monotone tone (www.pcipal.com) (static1.twilio.com)	Masking service, payment gateway; agent desktop receives status only	Vendor attestation for the actual configuration (sycurio.com); scope statement from the acquirer	Agent-assisted alternative route; confirm outcome through the gateway
Pause and resume recording	Customer speaks; employee keys it	Employee still hears the data (www.pcipal.com)	Employee device, browser, phone platform; recording excluded only if pause works	Evidence the pause is automatic or audited (help.genesys.cloud)	Delete or restrict recordings that captured data (www.pcisecuritystandards.org)

The table shows that "the provider's page is secure" and "the merchant's telephone process is compliant" are different statements. The link path removes the employee and the recording from the data path; the terminal path keeps both in it. Pause-and-resume sits between them and is the only row whose protection depends on an employee remembering a step.

Where card data can leak outside the chosen method

Regardless of method, five places commonly hold digits that were never meant to be stored.

- **Voicemail.** A Microsoft Teams voicemail is an email message with an audio file attachment (learn.microsoft.com), delivered to the mailbox as standard email (learn.microsoft.com). Microsoft documents an optional control to encrypt voicemail left by internal and external callers (learn.microsoft.com).
- **Transcripts.** RingCentral transcribes voicemail into text available by email and in its app (support.ringcentral.com), and Google Voice forwards voicemail transcripts to the user's email (support.google.com).
- **Messaging.** The supplement says never to send cardholder data over an unencrypted end-user messaging medium such as chat, social media, SMS or email (listings.pcisecuritystandards.org).

- **Notes and paper.** The West Virginia State Treasurer's handbook tells agencies not to write down cardholder information or payment details provided by phone (wvtreasury.gov), and St. Olaf College directs payers to a secure gateway rather than writing details down over the phone (wp.stolaf.edu).
- **Recordings.** FAQ 1210 expects suppression or redaction of audio during data entry where the technology exists.

Not all card data is equal. A card verification code (CVV) is the 3- or 4-digit number printed on the card, and PCI SSC says it is not permitted to retain card verification codes after authorization (www.pcisecuritystandards.org). The same FAQ says PCI DSS does not prohibit collecting them before authorization. Requirement 3.3.1 states that sensitive authentication data (SAD) is not retained after authorization, even if encrypted (listings.pcisecuritystandards.org). FAQ 1210 adds that PCI DSS does not override local or regional audio retention laws (www.pcisecuritystandards.org). The accurate summary is therefore not "payment recordings are illegal." It is that SAD must not remain after authorization, recording of it must be prevented where possible, and data that cannot be kept out should be securely deleted immediately on authorization.

What an auto attendant can and cannot do

An auto attendant is a menu that answers the call and routes it. For payments it can offer an option such as "billing question", send that option to the person who handles billing, play a recorded instruction that says which payment method to expect, or tell callers never to leave card details in a message. It cannot itself collect or protect payment details. A voice menu that routes to mobiles has no hosted payment page, no tone masking and no gateway connection unless a separate payment capability is added. Callers should be told, in the greeting and again in the voicemail prompt, that no card numbers should be left in a message. Keep the payment capability separate from the menu, and ask the phone provider whether voicemail is emailed with an attachment or a transcript, because that is the inbox path shown above.

Performance and Benchmarks

No independent benchmark of completion rate, fraud, chargeback or time-to-pay across the three paths was found in the sources reviewed, and none is asserted. What can be compared from first-party pages is published US pricing as of October 2026. *Table 2* below lists the fee lines found, as shown on each vendor's page and subject to plan terms (some rates may apply only to new customers or legacy plans, and rates can differ by payment type), all of which are vendor statements for the vendor's own price and all subject to change.

Provider (US page)	Customer-entered link	Staff-keyed terminal entry	Monthly fee noted
Square	3.3% + 30¢ per online transaction (squareup.com); 3.3% + 30¢ for a link sent by text from the terminal, which Square lists under legacy plans; its current Free, Plus and Premium lists show no separate text-link line (squareup.com)	3.5% + 15¢ (squareup.com)	None for the terminal (squareup.com)

Provider (US page)	Customer-entered link	Staff-keyed terminal entry	Monthly fee noted
Stripe	2.9% + 30¢ per successful domestic card transaction (stripe.com)	3.4% + 0.30 USD for cards entered manually or via Terminal MOTO (support.stripe.com)	Payment Links included at no additional charge (stripe.com)
PayPal	2.99% + $0.10 per transaction for cards and Apple Pay on its payment-links page (www.paypal.com)	3.39% + $0.29 per transaction (securepayments.paypal.com); the page notes fees can change	No setup cost or monthly fees on Payment Links
SumUp	3.25% + $0.15 per payment-link transaction (help.sumup.com)	Not captured from the page	Not captured

The pattern is that keyed entry carries a different fee shape from a hosted link at each provider that publishes both: a higher percentage with a lower fixed fee at Square, a higher percentage at Stripe. Which is cheaper depends on ticket size, so the worksheet in the data section uses owner inputs. Two caveats apply. Owners should use the current fee schedule for their own account, since rates vary by plan, customer type and payment type. SumUp's separate invoice page lists a different online-invoice rate, and the two should not be treated as one product.

The right comparison for a small firm is therefore total cost per completed payment, including staff minutes for assisted payments, and not the headline percentage. Twilio's current voice pricing page lists Pay Connectors as a separate per-transaction line in addition to per-minute voice charges (www.twilio.com), which shows that a keypad flow built on a telephony platform adds its own cost layer.

Implementation: Questions, Fallbacks and Acceptance Testing

Questions for the acquirer and phone provider

The goal is a decision supported by written answers. PCI SSC says it does not enforce compliance or define validation reporting requirements; the payment brands maintain the validation programs and decide who must validate and how (www.pcisecuritystandards.org), so the acquirer is the party to ask. *Table 3* below is a responsibility register to fill in for each party.

Party	Question to ask	Evidence to request in writing	Owner
Acquirer or processor	Which collection workflows are approved for our merchant account, and which questionnaire applies?	Written statement of the questionnaire type and any additional requirements; an SAQ is not chosen from a marketing label	Owner or finance lead
Payment provider	Does the hosted page or terminal fit the approved workflow, and what remains our duty?	Provider documentation of shared responsibility (docs.stripe.com); redirect obligations	Owner

Party	Question to ask	Evidence to request in writing	Owner
Phone provider	Do tones, audio, transcripts, AI summaries, exports and notifications ever contain card data on our configuration?	Settings screenshots; voicemail email behavior (learn.microsoft.com); recording and transcription behavior (support.ringcentral.com)	Office manager
Outsourced answerer, if any	Will they ever take payments, or only route the call?	Written scope statement and incident route	Owner
Merchant (us)	Who is authorized, which devices, and what is the incident route?	Third-party provider list; handoff checklist	Owner

The register assigns one person per row. A provider that handles card data is a third-party service provider, so the merchant row should list every such provider by name. The register is not a certification: it records who said what, when.

Accessibility and failed-payment fallback

A payment process that only works for callers with a smartphone and a free hand excludes some customers. The fallback should be approved, not improvised.

- **Caller cannot open the link.** Offer the keypad flow or an assisted flow through the terminal, and do not ask for digits by text.
- **Caller lacks a smartphone.** Offer a call-back during which a staff member sends the link to another device, or schedule payment by invoice.
- **Caller cannot use a keypad.** Offer assisted entry through the approved route.
- **Relay callers.** The Federal Communications Commission (FCC) states that dialing 711 connects the caller to a relay communications assistant (www.fcc.gov), and notes that 711 does not work for video relay service calls (www.fcc.gov). The Americans with Disabilities Act (ADA) guidance says staff who answer must treat relay calls just like other calls (www.ada.gov), and that businesses must communicate effectively with people who have communication disabilities (www.ada.gov). Which assisted method suits a relay conversation should be settled with the acquirer in advance, since a relay assistant may read digits aloud.
- **Confirmation delayed.** Tell the caller not to retry repeatedly; the employee checks the dashboard or gateway before asking again.

Pressure is the wrong fallback. If the approved routes fail, give the customer an alternative such as an invoice, a later call or in-person payment, rather than a way to speak or text digits. This is general operational guidance; whether an accommodation is legally required in a given case is a question for a lawyer, and the ADA material above is context, not advice.

Acceptance walkthrough

Before any live customer pays by the new method, test it with a provider sandbox or test method and synthetic data, with written approval from the acquirer. Do not test with real card verification codes in a recording or voicemail.

1. **Draw the journey.** For one test call, list caller, employee device, phone platform, payment provider, storage and receipt.
2. **Run a synthetic payment.** Use the provider's documented test cards only.
3. **Search afterwards.** Check call recordings, transcripts, voicemail email, call notes and message threads for any digits.
4. **Check the failure paths.** Test a declined result, a link that is not opened and a caller who cannot use a keypad.
5. **Record approval.** File the acquirer's written confirmation and the test date.

Short documented payment handoff

The checklist below does not certify compliance; it makes the process repeatable.

- **Receipt confirmation:** who confirms the payment succeeded, and where.
- **Failed link:** resend, then switch to the approved alternative.
- **Customer assistance:** the approved assisted route and who may use it.
- **No card details in voicemail:** the greeting and voicemail prompt tell callers not to leave card details, and staff delete any such message and report it per the incident route.
- **Incident reporting:** a named contact at the acquirer or provider for suspected exposure.
- **Retention:** keep only what there is a business need for; the Federal Trade Commission (FTC) advises holding information only as long as there is a legitimate business need (www.ftc.gov).

Data Analysis and Evidence

The quantitative evidence is thin and mostly indirect, which is itself a finding.

Audience size. The SBA Office of Advocacy counts 36,207,130 small businesses (advocacy.sba.gov). That says nothing about how many take telephone payments. Federal Reserve Payments Study data show that in-person payments were 63.8 percent of general-purpose card payments by number in 2022 (www.federalreserve.gov), which implies the remainder were remote, but the study does not isolate telephone orders, so the share taken over the phone is unknown.

Standards dates. PCI SSC published PCI DSS v4.0.1 as a limited revision and stated that v4.0 would be retired on 31 December 2024 (blog.pcisecuritystandards.org). PCI SSC also stated that the v4.0.1 limited revision does not change the 31 March 2025 effective date of the new requirements. The telephone supplement dates from November 2018, so it predates both versions and should be read as background. The SAQ eligibility quotations in this report come from the v4.0 documents, and the v4.0.1 versions clarified some criteria; the current text should be reopened with the acquirer before any compliance statement is made.

Questionnaire eligibility signals. SAQ A applies to merchants who accept only card-not-present transactions (listings.pcisecuritystandards.org) and have all processing of account data entirely outsourced to compliant third-party service providers. SAQ P2PE applies to merchants who receive account data on paper or over a telephone and key it directly and only into a payment terminal from a validated point-to-point encryption solution (listings.pcisecuritystandards.org). SAQ D is the fallback for merchants who do not meet the criteria for any other SAQ type. These statements describe eligibility criteria, not a classification of any workflow

described here. Institutions illustrate how the criteria turn into policy: the University of Missouri System distinguishes merchants that process only through a web-based virtual terminal and store no cardholder data electronically (www.umsystem.edu), and UCSB prohibits typing card information into a browser for its own telephone payments while citing the PCI telephone supplement (bfs.ucsb.edu). Those are campus rules and should not be generalized to small firms.

Cost worksheet (owner inputs)

No example rates are assumed. Use one currency and one billing period for every input:

Monthly cost = monthly service fee + (transactions × fixed fee per transaction) + (transaction value × percentage rate) + (assisted-payment minutes × loaded staff cost per minute) + validated add-ons

- **Monthly service fee:** from the provider's current US page.
- **Transactions and value:** from the last 3 months of invoices and deposits, divided by 3.
- **Percentage and fixed fee:** from the acquirer's current schedule, not a review site; Table 2 shows that keyed and hosted rates differ.
- **Assisted minutes:** minutes an employee spends on calls where the link or keypad route fails.
- **Add-ons:** only items the acquirer has confirmed in writing, such as a per-transaction connector line (www.twilio.com).

Because rates and fixed fees differ by method and ticket size, run the formula once per method with the same transaction data and compare the totals.

Implications and Future Directions

For a small firm the practical implication is that the payment choice should precede the phone choice. Six decision rules follow from the evidence above:

- **Default to the link** when the payment can wait until after the call, because it keeps the employee, the phone platform and the recording out of the data path.
- **Use a terminal** only on a device the acquirer has approved, and treat the employee's ear and screen as in scope.
- **Prefer masking over pause-and-resume** when payment must happen during the call, because pause-and-resume depends on an employee remembering a step.
- **Keep digits out of messages.** A link may be texted; a card number may not.
- **Check every inbox.** Voicemail email, transcripts and notifications are separate from the payment method.
- **Write it down.** Keep the acquirer's answers and the test date with the handoff checklist.

A routing-only number, a business mobile and a cloud phone system all carry the call; none of them determines how the card is collected. The plain-language rule from the sources is that every system the digits touch comes into the conversation about scope, and the hosted-link path touches the fewest.

Standards will keep moving. PCI SSC has already retired v4.0 and set future-dated requirements that took effect in March 2025, and acquirers may change the questionnaires they ask for. The supplement is dated 2018, and vendors describe newer capabilities, such as automatic redaction in logs (www.twilio.com), that the supplement does not address. Owners should expect to re-ask the acquirer's questions annually, and whenever the phone provider adds transcription or summaries.

Two open issues remain. First, no independent data compares completion and abandonment across paths, so claims that links convert better or worse than keypad flows are unsupported here. Second, jurisdictional privacy and consumer-protection rules for recording and transcribing calls vary and are outside this report; they should be reviewed separately with the recording material already linked.

Frequently Asked Questions (FAQs)

How can a small business take credit card payments over the phone?

Choose the path first: send a payment link the customer completes, key the card into a virtual terminal on an approved device, or use a keypad service that masks tones. Then ask the acquirer which workflows are approved for your account.

What is the difference between a payment link and a virtual terminal?

With a link, the customer types card details on the provider's hosted page. With a virtual terminal, an employee keys the details, such as the card number, expiration date, security code and postal code (squareup.com).

What is secure keypad or DTMF masking?

Masking replaces keypad tones with a random or flat tone, and vendors say the agent never hears the digits (sycurio.com); Twilio documents a PCI Mode with built-in DTMF redaction (www.twilio.com).

Is it PCI compliant to take payments over the phone as a small business?

It depends on the workflow, the acquirer's requirements and the configuration. PCI DSS is intended for entities of any size, and the questionnaire is not decided from a marketing label.

Can a business take payments without storing card numbers?

A hosted link or a masked keypad flow can keep the digits off your systems in the vendors' descriptions (squareup.com), but sensitive authentication data must not be retained after authorization.

Can a payment link be sent during a call?

Yes, through a provider that issues links by text or email (www.paypal.com). A link is not a card number, and cardholder data must not be sent over unencrypted messaging.

Are call recordings of payments always illegal?

No. FAQ 1210 requires every effort to prevent sensitive authentication data being recorded (www.pcisecuritystandards.org), and says PCI DSS does not override local audio retention laws.

What is the best way to accept payments by phone for a small business?

There is no single best method in the sources reviewed. A hosted link suits remote payment; keypad masking suits payment during the call; a terminal suits an isolated, trained setup, and Stripe lists Payment Links as an alternative to entering cards manually (support.stripe.com).

Conclusion

The choice among a payment link, a virtual terminal and a secure keypad flow is a choice about where card details travel. A link keeps them on the provider's page, a terminal keeps the employee and the device in the path, and a masked keypad flow keeps the digits away from the employee when it is designed and deployed as the vendors and the supplement describe. In every case the phone platform's recordings, transcripts and voicemail email must be checked on the real configuration, because those are separate paths from the payment itself.

The documents that matter are current ones. The 2018 supplement is background, FAQ 1210 and FAQ 1153 are the starting points, and the acquirer decides what the merchant must validate. A routing-only phone number can direct the call and say what to expect, but it does not collect payment details. The next step is the question list in Table 3, a synthetic-data test and a short written handoff, kept with the acquirer's written approval.

Source links

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

1. https://www.pcisecuritystandards.org/faqs/1153
2. https://listings.pcisecuritystandards.org/documents/Protecting_Telephone_Based_Payment_Card_Data_v3-0_nov_2018.pdf
3. https://docs.stripe.com/payment-links/create
4. https://www.pcisecuritystandards.org/faqs/1604
5. https://securepayments.paypal.com/us/business/accept-payments/virtual-terminal
6. https://sycurio.com/blog/dtmf-masking
7. https://www.pcisecuritystandards.org/faqs/1210
8. https://learn.microsoft.com/microsoftteams/set-up-phone-system-voicemail
9. https://squareup.com/help/us/en/article/5068-square-virtual-terminal-faq
10. https://squareup.com/us/en/payment-links
11. https://www.pcisecuritystandards.org/faqs/do-small-merchants-with-limited-transaction-volumes-need-comply-with-pci-dss
12. https://advocacy.sba.gov/2026/02/03/advocacy-releases-frequently-asked-questions-about-small-businesses-2026
13. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
14. https://docs.stripe.com/payment-links
15. https://www.paypal.com/us/business/accept-payments/payment-links
16. https://help.sumup.com/en-US/articles/1bTBfAoe7SiaKiUxCo2uzP-payment-links-faq
17. https://stripe.com/pricing

18. https://docs.stripe.com/security/guide
19. https://docs.stripe.com/payment-links/share
20. https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/can-unencrypted-pans-be-sent-over-e-mail-instant-messaging-sms-or-chat
21. https://www.sumup.com/en-us/virtual-terminal
22. https://support.authorize.net/knowledgebase/article/KA-04441/en-us
23. https://squareup.com/us/en/virtual-terminal
24. https://squareup.com/help/us/en/article/5176-manually-key-in-card-payments-without-the-square-reader
25. https://support.stripe.com/questions/b7bd8ea6-d20c-40f8-a273-4d6c4902957a
26. https://docs.stripe.com/payments/payment-intents/moto
27. https://usa.visa.com/dam/VCOM/global/support-legal/documents/preventing-card-not-present-fraud.pdf
28. https://wvtreasury.gov/Portals/wvtreasury/content/Banking/state-agencies/Credit%20Card%20Handling%20Handbook.pdf
29. https://support.stripe.com/questions/manually-entered-card-payments
30. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-C-VT.pdf
31. https://bfs.ucsb.edu/cash-handling-banking/credit-card-acceptance/processing-methods
32. https://louisville.edu/policies/policies-and-procedures/pageholder/pol-credit-card-pci-merchants
33. https://www.pcipal.com/technology/dtmf-masking-solutions
34. https://static1.twilio.com/docs/voice/api/payment-resource
35. https://www.twilio.com/docs/voice/twiml/pay
36. https://developers.telnyx.com/docs/voice/programmable-voice/pay.md
37. https://www.twilio.com/en-us/blog/voice-agent-assisted-pay
38. https://www.twilio.com/docs/voice/tutorials/how-capture-your-first-payment-using-pay.md
39. https://www.twilio.com/docs/studio/widget-library/capture-payments
40. https://www.dialpad.com/au/features/call-recording
41. https://help.genesys.cloud/announcements/secure-pause-available-on-all-call-types
42. https://www.dialpad.com/trust/customer-data
43. https://www.pcipal.com/knowledge-center/resource/why-pause-and-resume-call-recording-isnt-enough
44. https://www.eckoh.com/dtmf-masking
45. https://www.twilio.com/docs/voice/api/recording
46. https://support.ringcentral.com/article-v2/8045.html?brand=RC_US&product=RingEX&language=en_US
47. https://support.google.com/voice/answer/9182115
48. https://wp.stolaf.edu/finance/pci-dss
49. https://www.pcisecuritystandards.org/faqs/1280
50. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-D-Merchant.pdf
51. https://support.stripe.com/questions/phone-orders
52. https://www.twilio.com/en-us/voice/pricing/us

53. https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/what-is-the-involvement-of-the-pci-ssc-on-the-compliance-validation-processes-for-pci-dss-assessments-and-scan-reports
54. https://www.fcc.gov/sites/default/files/711_for_telecommunications_relay_service.pdf
55. https://www.ada.gov/resources/effective-communication
56. https://www.ftc.gov/business-guidance/resources/start-security-guide-business
57. https://www.federalreserve.gov/paymentsystems/2024-November-The-Federal-Reserve-Payments-Study.htm
58. https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1
59. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-A.pdf
60. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4-0-SAQ-P2PE.pdf
61. https://www.umsystem.edu/departments-staff/finance/investments-treasury/treasury/credit-card-compliance/payment-card-industry-data-security-standards

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.