P A Y T I A

The Complete **PCI DSS Compliance Checklist for Phone Payments**

2025/2026 Edition | PCI DSS v4.0 Compliant

Your step-by-step guide to achieving and maintaining PCI DSS compliance when processing card payments over the phone.

Inside this guide:

- ✓ Complete PCI DSS v4.0 compliance checklist
- ✓ SAQ selection guide for phone payment environments
- ✓ DTMF masking explained: how it reduces your compliance scope
- ✓ Phone payment security best practices
- ✓ Common compliance mistakes and how to avoid them

www.paytia.com
PCI DSS Level 1 Certified | Barclaycard & Stripe Integration Partner

Why PCI DSS Compliance Matters for Phone Payments

Every business that accepts card payments over the phone is required to comply with PCI DSS (Payment Card Industry Data Security Standard). Non-compliance puts your business at risk of data breaches, fines of up to £100,000, and loss of the ability to process card payments altogether.

PCI DSS version 4.0 introduced significant changes that affect how phone payments must be handled. This checklist covers every requirement relevant to telephone payment environments, helping you understand where your business stands and what steps you need to take.

Whether you operate a call centre with hundreds of agents or a small team taking occasional phone orders, this guide gives you a clear, actionable path to compliance.

Section 1: Understand Your Compliance Scope

Before you can become compliant, you need to understand exactly what falls within your PCI DSS scope. Every system, person, and process that touches cardholder data is in scope.

1.1 DEFINE YOUR CARDHOLDER DATA ENVIRONMENT

- ☐ **Identify all systems that store, process, or transmit cardholder data**
  Include phone systems, CRM, call recording, payment terminals, and any connected networks.
- ☐ **Map the flow of cardholder data through your organisation**
  Document how card numbers move from the caller to the payment processor, including every touchpoint.
- ☐ **Identify all personnel who handle or could access cardholder data**
  This includes agents taking payments, IT staff with system access, and managers with reporting access.
- ☐ **Document all third-party service providers involved in payment processing**
  Payment gateways, hosting providers, telecoms providers, and any outsourced functions.
- ☐ **Determine which SAQ (Self-Assessment Questionnaire) applies to your environment**
  See Section 2 for SAQ selection guidance specific to phone payment environments.

PAYTIA TIP

The single most effective way to reduce your PCI scope is to prevent cardholder data from entering your environment in the first place. DTMF masking technology allows callers to enter card details using their phone keypad while your agents remain on the line — but never hear or see the card numbers. This can reduce your SAQ from the 329-question SAQ D to the 26-question SAQ A.

Section 2: SAQ Selection Guide for Phone Payments

The Self-Assessment Questionnaire you need to complete depends on how card data is handled in your environment. Choosing the wrong SAQ is one of the most common compliance mistakes.

SAQ Type	Questions	Applies When	Phone Payment Example
SAQ A	26	All card data handled by third-party; no electronic storage, processing, or transmission	Using DTMF masking (e.g. Paytia) where card data goes directly to processor
SAQ A-EP	191	E-commerce with third-party processing but website could affect transaction security	Rarely applies to phone payments; more relevant to web-based payment pages
SAQ C-VT	79	Using a web-based virtual terminal on a single computer, not connected to other systems	Single agent using isolated virtual terminal for occasional phone orders
SAQ D	329	Any environment not covered by other SAQs, or where card data is stored/processed locally	Agents hearing card numbers, writing them down, or entering into non-isolated systems

1.2 SAQ SELECTION CHECKLIST

- ☐ **Determine if agents hear, see, or manually enter card numbers**
  If yes, you are likely SAQ D. If no (using DTMF masking), you may qualify for SAQ A.
- ☐ **Check whether call recordings capture card data**
  DTMF tones in recordings count as stored cardholder data. Pause-and-resume or DTMF masking eliminates this.
- ☐ **Verify whether card data passes through any of your systems**
  With DTMF masking, card data goes from the caller's phone directly to the payment processor, bypassing your systems entirely.
- ☐ **Confirm your payment service provider's PCI compliance status**
  Request their Attestation of Compliance (AOC) or listing on the PCI SSC website.
- ☐ **Consult your acquiring bank or QSA if unsure**
  Incorrect SAQ selection can result in non-compliance even if all questions are answered correctly.

Section 3: Core PCI DSS v4.0 Requirements

PCI DSS v4.0 has 12 core requirements grouped into 6 goals. Below are the requirements most relevant to phone payment environments, with specific actions for each.

Goal 1: Build and Maintain a Secure Network

REQUIREMENT 1: INSTALL AND MAINTAIN NETWORK SECURITY CONTROLS

- ☐ **Install and configure firewalls between your payment systems and untrusted networks**
- ☐ **Restrict inbound and outbound traffic to that which is necessary for payment processing**
- ☐ **Document all network connections and data flows involving cardholder data**
- ☐ **Review firewall and router configurations at least every six months**

REQUIREMENT 2: APPLY SECURE CONFIGURATIONS TO ALL SYSTEM COMPONENTS

- ☐ **Change all vendor-supplied default passwords before deployment**
  This includes phone systems, routers, VoIP equipment, and payment software.
- ☐ **Disable unnecessary services, protocols, and ports on all systems**
- ☐ **Maintain an inventory of all system components in scope**
- ☐ **Encrypt all non-console administrative access using strong cryptography**

Goal 2: Protect Account Data

REQUIREMENT 3: PROTECT STORED ACCOUNT DATA

- ☐ **Do not store cardholder data unless absolutely necessary**
  The best protection is not storing card data at all. DTMF masking achieves this by design.
- ☐ **If data must be stored, encrypt it using strong cryptography (AES-256 minimum)**
- ☐ **Never store the full contents of the magnetic stripe, CVV, or PIN**
  This applies even if data is encrypted. These elements must never be retained after authorisation.
- ☐ **Mask the PAN when displayed (show only first 6 and last 4 digits maximum)**
- ☐ **Implement a data retention and disposal policy**
  Define how long card data is kept and how it is securely destroyed when no longer needed.

REQUIREMENT 4: PROTECT CARDHOLDER DATA IN TRANSIT

- ☐ **Use strong cryptography (TLS 1.2+) for all transmission of cardholder data over public networks**
- ☐ **Never send unprotected cardholder data via email, instant messaging, or SMS**
- ☐ **Ensure VoIP systems carrying card data use encrypted protocols**
  Unencrypted VoIP calls carrying card numbers are a common compliance gap.
- ☐ **Verify that your payment processor connection uses current encryption standards**

PAYTIA TIP

With DTMF masking, card data is transmitted directly from the caller's handset to the payment processor over an encrypted channel. Your phone system, VoIP network, and call recording infrastructure never carry the card data — which means Requirements 3 and 4 are largely addressed by design.

Goal 3: Maintain a Vulnerability Management Programme

REQUIREMENTS 5 & 6: PROTECT SYSTEMS AND DEVELOP SECURELY

- ☐ **Deploy anti-malware on all systems commonly affected by malware**
- ☐ **Keep all system components and software patched and up to date**
  Apply critical security patches within one month of release.
- ☐ **Develop and maintain secure systems and applications**
  If you develop custom payment applications, follow secure coding guidelines.
- ☐ **Conduct internal and external vulnerability scans quarterly**
  External scans must be performed by a PCI-approved scanning vendor (ASV).

Goal 4: Implement Strong Access Controls

REQUIREMENTS 7, 8 & 9: CONTROL ACCESS

- ☐ **Restrict access to cardholder data to only those who need it for their role**
- ☐ **Assign unique IDs to each person with computer access**
  No shared or group accounts for payment systems.
- ☐ **Implement multi-factor authentication for all remote access and admin access**
  PCI DSS v4.0 requires MFA for all access to the cardholder data environment, not just remote.
- ☐ **Restrict physical access to systems containing cardholder data**
  Lock server rooms, secure workstations, and implement visitor logs.
- ☐ **Review user access rights at least every six months**
  Remove access promptly when employees change roles or leave the organisation.

Goal 5: Monitor and Test Networks

REQUIREMENTS 10 & 11: MONITORING AND TESTING

- ☐ **Log all access to cardholder data and network resources**
  Logs must include user identification, event type, date/time, success/failure, and data accessed.
- ☐ **Review logs daily using automated tools or manual processes**
- ☐ **Conduct penetration testing at least annually and after significant changes**
- ☐ **Deploy intrusion detection or prevention systems on networks carrying cardholder data**
- ☐ **Implement change detection on critical system files**

Goal 6: Maintain an Information Security Policy

REQUIREMENT 12: MAINTAIN A SECURITY POLICY

- ☐ **Establish and publish an information security policy covering all PCI DSS requirements**
- ☐ **Conduct a formal risk assessment at least annually**
- ☐ **Train all staff on security awareness at least annually**
  Include specific training on phone payment security procedures.
- ☐ **Screen potential employees with access to cardholder data (background checks)**
- ☐ **Maintain an incident response plan and test it annually**
  Include procedures for suspected card data breaches.
- ☐ **Document and acknowledge all third-party service provider PCI responsibilities**

Section 4: Phone Payment-Specific Requirements

These requirements address the unique risks of taking card payments over the telephone, beyond the general PCI DSS controls above.

4.1 CALL RECORDING COMPLIANCE

- ☐ **If you record calls, ensure DTMF tones are masked or calls are paused during card entry**
  Stored DTMF tones in recordings constitute stored cardholder data and bring your entire recording system into PCI scope.
- ☐ **Implement automated pause-and-resume or DTMF suppression**
  Manual pause by agents is unreliable and still leaves your environment in scope.
- ☐ **Audit a sample of call recordings monthly to verify no card data is captured**
- ☐ **If using speech analytics, ensure card numbers spoken aloud are redacted**

4.2 AGENT ENVIRONMENT CONTROLS

- ☐ **Prevent agents from writing down card numbers (no pens/paper at desks)**
- ☐ **Disable copy/paste functionality on payment screens if agents see card data**
- ☐ **Block access to email, messaging, and external websites from payment workstations**
- ☐ **Disable USB ports and removable media on payment workstations**
- ☐ **Position screens so card data cannot be viewed by other staff or CCTV cameras**
- ☐ **Implement clean desk policies for payment processing areas**

4.3 DTMF MASKING IMPLEMENTATION

- ☐ **Select a PCI DSS Level 1 certified DTMF masking provider**
  Verify certification is current and covers the specific service you are using.
- ☐ **Verify that DTMF tones are replaced with flat tones before reaching your infrastructure**
  The masking must occur upstream of your phone system, not within it.
- ☐ **Confirm that card data routes directly from the caller to the payment processor**
  Card numbers should never pass through your telephony infrastructure or network.
- ☐ **Test that agents cannot hear distinguishable tones when callers enter card numbers**
- ☐ **Verify call recordings contain no decipherable DTMF tones**
- ☐ **Ensure the agent screen shows progress (e.g. asterisks) but never the full card number**

PAYTIA TIP

Paytia's DTMF masking technology is PCI DSS Level 1 certified and integrates directly with Stripe and Barclaycard. Card data flows from the caller's phone to the payment processor without touching your systems. This reduces your compliance scope from SAQ D (329 questions) to SAQ A (26 questions), cutting compliance effort by over 90%.

Section 5: Common Compliance Mistakes

These are the errors we see most frequently in phone payment environments. Avoiding them will save significant time and cost during your compliance assessment.

MISTAKES TO AVOID

- ☐ **Relying on agents to manually pause call recordings**
  Human error means card data inevitably ends up in recordings. Automated solutions are the only reliable approach.
- ☐ **Assuming your VoIP provider handles PCI compliance for you**
  Your VoIP provider transmits the data, but compliance responsibility for card data in transit remains yours.
- ☐ **Completing SAQ A when agents hear card numbers**
  If agents hear numbers spoken aloud, even if they don't enter them, you likely need SAQ D.
- ☐ **Not including the phone system in your network diagram**
  PCI assessors will ask. Your PBX, VoIP infrastructure, and SIP trunks are all in scope if they carry card data.
- ☐ **Storing card data in CRM notes or ticketing systems**
  Train agents never to record card numbers in any system. Implement field-level controls to detect and block card number patterns.
- ☐ **Ignoring PCI DSS v4.0 changes until the deadline**
  Several v4.0 requirements became mandatory on 31 March 2025. Ensure you are compliant with the current version.
- ☐ **Not validating third-party compliance annually**
  Your payment processor's compliance status can change. Request updated AOCs every year.

Section 6: Your Next Steps

Completing this checklist gives you a clear picture of your current compliance position. Here's how to move forward:

If You Have Gaps to Address

1. Prioritise items that reduce scope first. Implementing DTMF masking typically has the highest impact, moving you from SAQ D to SAQ A and eliminating the majority of requirements.

2. Address data storage issues next. If card data exists in recordings, CRM systems, or agent notes, this creates immediate risk.

3. Strengthen access controls and monitoring. These are the requirements most commonly failed during assessments.

If You Want Expert Help

Book a Free PCI Compliance Assessment

Paytia's compliance specialists will review your phone payment environment and show you exactly how to reduce your PCI scope. Most businesses save over 90% on compliance effort by implementing DTMF masking.

- ✓ Free, no-obligation assessment
- ✓ See a live demo of DTMF masking in action
- ✓ Get a personalised scope reduction roadmap

Visit: **www.paytia.com/demo**

Email: **info@paytia.com**

Call: **0330 131 0030**

About Paytia

Paytia provides PCI DSS Level 1 certified phone payment solutions for businesses of all sizes. Our DTMF masking technology enables secure card payments over the phone, reducing compliance scope by over 90%. We integrate directly with Stripe and Barclaycard, enabling businesses to start processing secure phone payments in minutes.