PAYMENTS GUIDE · 2026

PCI DSS and Card Payments Over the Phone

Where a spoken card number ends up, the security code rule, six ways to take phone payments ranked, and the questions to ask your phone provider and bank.

PCI DSS is set by the card industry and enforced through **your bank or payment provider**. Version **4.0.1** applies now. Phone payments are the hardest channel to keep tidy, because a card number read aloud can be copied into far more places than one typed into a payment page.

Where a spoken card number can end up

- In the head and notes of whoever answers
- On a notepad or sticky note
- In the audio carried by the phone system
- In call recordings
- In transcripts and AI call summaries
- In voicemail and voicemail emails
- In cloud drives, exports and backups

The rule that catches most businesses

- The card security code must not be kept after authorisation
- Not on paper, not encrypted, not in a recording
- Only store the card number with a genuine need
- Fix the payment process before recording every call

Six ways to take a phone payment, ranked

Method	Card data exposure
Written on paper, keyed in later	Highest
Keyed into a terminal while recording runs	Very high
Recording paused while the card is read out	Medium, relies on staff
Keypad entry via a validated payment service	Low
Payment link sent by SMS during the call	Very low
No cards taken on calls	Lowest

Clean up the recordings you already have

1. Find every place recordings and voicemails are stored.
2. Identify the lines, staff and dates where cards were read out.
3. Search transcripts and summaries for card numbers first.
4. Delete anything holding card security codes, including copies.
5. Shorten retention and turn on automatic deletion.
6. Remove access for anyone who does not need it.

Ask your phone provider

- Can recording be off for a payments line or user?
- Can it pause, ideally automatically?
- Can transcription be off for payment calls?
- How long is everything kept?
- Is multi-factor sign-in available?
- Can we send SMS from a verified sender ID?

Ask your bank

- Which questionnaire (SAQ) should we complete?
- Do you offer payment links by SMS?
- Do you recommend a validated keypad entry service?
- What changes if we move to payment links?
- Are we paying a non-compliance fee?
- What do we do about old recordings?

General information only

Based on PCI Security Standards Council guidance as read in November 2026. Not legal advice and not a QSA assessment. Your acquirer decides what you need to complete.

Uniden Voice

Australian owned and operated. Send payment links from your business number with verified SMS sender IDs, and set up recording and summaries with payment calls in mind. Book a demo at unidenvoice.com/get-started/book-a-demo or call 1300 881 662.