

BUSINESS / MERCHANT NAME	SITE OR LOCATION	DATE
INSPECTOR NAME (PRINT)	ROLE / STAFF ID	TIME STARTED

#	Terminal (make / model)	Serial number	SEALS	LABELS	SERIAL	CASING	WIRING	OVERLAY	circle one Outcome	PHOTO	Notes
1									P F S		
2									P F S		
3									P F S		
4									P F S		
5									P F S		
6									P F S		
7									P F S		
8									P F S		
9									P F S		
10									P F S		
11									P F S		
12									P F S		
13									P F S		
14									P F S		

P = pass · F = fail · S = suspicious. A terminal is only a PASS when all six checks pass.
 Any failed or suspicious check means the terminal is not a pass — complete the finding block on page 2 and act before the next customer pays.

Sign off

INSPECTOR SIGNATURE	TIME FINISHED	REVIEWED BY (MANAGER)	DATE REVIEWED

Retain this sheet with your inspection records. Your assessor or acquirer decides what evidence they require; keep it for at least the period they specify.

The six checks

Work terminal by terminal, in the same order every time. Look and feel — most tampering is found by touch, not by sight.

- Seals.** Security seals or tamper-evident tape intact, unbroken, and matching the number you recorded when the device was deployed.
- Labels.** Manufacturer and asset labels present, unpeeled, not doubled up, and not covering a screw or a seam.
- Serial.** The serial on the device matches the serial in your inventory for that position. A swapped device is the failure this check exists to catch.
- Casing.** No gaps, no fresh scratches around the seams, no colour or texture mismatch, nothing that flexes or clicks when pressed.
- Wiring.** Cables are the ones you installed, seated properly, with no spliced, dangling, or unfamiliar connectors behind or under the unit.
- Overlay.** Nothing sits on top of the card slot, keypad, or reader face. Pull gently on the bezel and the keypad; an overlay usually lifts.

If a check fails

Stop using the terminal, keep it as you found it, photograph it before anything is moved or removed, and escalate to whoever owns payment security at your organisation. Note the terminal number from page 1 here.

FINDING DETAIL		
TERMINAL # FROM PAGE 1	SERIAL	WHICH CHECK(S) FAILED
WHAT YOU SAW / ACTION TAKEN / WHO WAS NOTIFIED AND WHEN		

What to keep

Requirement 9.5.1.2 asks you to keep evidence that inspections actually happened. In practice an assessor looks for: which device (by serial), who inspected it, when, what the outcome was, and what you did about anything that was not a pass. This sheet is laid out to capture exactly those five things. Requirement 9.5.1.2.1 lets you set your own inspection frequency — but the frequency has to come from a documented risk analysis, in writing, not from habit.

What this sheet cannot do

Paper is not append-only. A sheet can be re-written, replaced, or lost, and nothing about it proves the record is the original — which is the gap between having a routine and being able to evidence it. Digital records that are append-only, timestamped, and attributable to a named inspector close that gap. SkimGuard's business tiers include a terminal inspection logbook that records these same six checks, keeps an immutable audit trail of who did what and when, and exports to CSV or PDF for an assessor: skimguard.io/pci-terminal-inspection-log

Not sure how often to inspect?

A free 2-minute assessment estimates a starting cadence from your own risk factors and gives you the written justification 9.5.1.2.1 expects: skimguard.io/poi-inspection-schedule-wizard

SkimGuard, Inc. is not a Qualified Security Assessor and does not perform PCI assessments. This sheet is a free record template intended to help you document and evidence inspection activity under PCI DSS v4.0.1 Requirement 9.5.1.2. It is not an attestation or certification of PCI compliance, it does not cover the other requirements in your cardholder-data environment, and using it does not make an organisation compliant. Your compliance is assessed by your QSA or acquirer. Reproduce and distribute this sheet freely.