PCI Card Handling & MOTO Guidance Policy (Merchant Version)

Effective Date: December 2020

Last Revised: July 2026

Document Control

- Policy Owner: Jenny Ball - Compliance Officer
- Approval Authority: Raman Sethi - Chief Payments Officer
- Version: 1.3
- Review Cycle: Annually

1. Purpose

Vesta Merchant Services ("VMS") is committed to helping merchants protect payment card information and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS v4.0.1).
This guidance outlines the minimum standards merchants must follow when accepting, processing, transmitting and destroying payment card information.
The objectives of this guidance are to:

- protect cardholder information;
- reduce the risk of fraud and data compromise;
- support merchants in meeting PCI DSS obligations;
- minimise chargebacks resulting from poor payment handling practices;
- maintain secure payment processing across all payment channels.

2. Scope

This guidance applies to all merchants using payment services provided by Vesta Merchant Services.

It applies to all payment channels including:

- Face-to-Face Payments
- Mail Order
- Telephone Order (MOTO)
- Online Payments
- Virtual Terminals
- Mobile Payment Devices

3. Policy Statement

Merchants must process payment card information securely and in accordance with:

- PCI DSS Version 4.0.1
- Visa Core Rules
- Mastercard Rules
- Merchant Agreement
- Applicable Data Protection legislation

Merchants are responsible for ensuring their employees understand and follow these requirements.

Failure to comply may increase fraud risk, result in financial loss, and could lead to additional monitoring, restrictions or termination of merchant services.

4. PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is the global security standard developed by the major payment card schemes.

PCI DSS helps protect payment card information throughout the payment process.

Compliance with PCI DSS significantly reduces the risk of:

- payment fraud;
- cardholder data theft;
- data breaches;
- financial penalties;
- reputational damage.

Merchants should ensure they understand the PCI DSS requirements applicable to their business.

5. Cardholder Data

Payment cards contain two categories of information.

Cardholder Data (CHD)

Cardholder Data consists of:

- Primary Account Number (PAN)
- Cardholder Name
- Expiry Date
- Service Code

Sensitive Authentication Data (SAD)

Sensitive Authentication Data includes:

- CVV/CVC/CID
- PIN
- PIN Block
- Full Track Data
- Chip Authentication Data

Sensitive Authentication Data **must never be stored after authorisation**, even if encrypted.

6. Merchant Responsibilities

Merchants must:

- process payments using approved payment solutions;
- protect customer payment information;
- ensure staff receive appropriate training;
- restrict access to payment information;
- inspect payment terminals regularly;
- report suspected security incidents immediately;
- comply with PCI DSS requirements.

7. Cardholder Data Principles

Merchants should always follow these principles:

- Collect only the information required to process the payment.
- Never request unnecessary payment card information.
- Never store card information unless specifically permitted by PCI DSS.
- Never transmit card information using insecure communication methods.
- Restrict access to authorised personnel only.
- Securely destroy payment information once no longer required.

8. Storage of Cardholder Data

VMS strongly recommends that merchants do not store payment card **information electronically**.

Card information must **never** be stored in:

- Email
- Outlook folders
- Excel spreadsheets
- Word documents
- PDF files
- CRM systems
- Mobile phones
- USB drives
- Cloud storage
- Local computer drives

Sensitive Authentication Data must **never** be stored under any circumstances.

Where merchant receipts are retained:

- only masked PAN should be visible;
- receipts must be stored securely;
- access must be restricted;
- receipts should be destroyed securely once the retention period expires.

9. Payment Terminal Security

Payment terminals should:

- display only masked PAN;
- never retain Sensitive Authentication Data;
- be inspected daily;
- remain under staff supervision;
- be securely stored when not in use.

Daily inspections should include checking:

- serial numbers;
- security seals;
- cables;
- signs of tampering;
- unauthorised devices.

Inspection records should be maintained.

10. Face-to-Face Payments

For card-present transactions:

- customers should insert, tap or present their own payment card whenever possible;
- staff should only handle payment cards with the customer's permission;
- payment terminals should remain visible to customers;
- terminals should be inspected before use;
- suspicious behaviour around payment terminals should be reported immediately.

11. Mail Order & Telephone Order (MOTO)

MOTO transactions present a higher fraud risk than Chip & PIN transactions.

When processing MOTO payments, merchants should:

- enter payment details directly into the approved payment terminal or virtual terminal;
- never record payment card details electronically;

- never repeat the full PAN back to the customer;
- ensure telephone systems do not record payment information;
- collect only the information required to process the payment.

Telephone systems used for MOTO payments should not retain call recordings containing payment card information.

For higher-value MOTO transactions merchants should consider:

- additional customer verification;
- delivery to the verified billing address;
- proof of delivery;
- signed delivery confirmation;
- retaining supporting customer correspondence.

12. Online Payments

Online payments should only be processed through PCI DSS compliant payment gateways approved by VMS.

Merchants should never:

- manually collect online payment details;
- bypass approved payment gateways;
- ask customers to email payment card information.

13. Unsolicited Card Data

Customers occasionally provide payment card information unexpectedly via:

- email;
- voicemail;
- post;
- messaging applications.

Where this occurs:

- do not forward the information;
- process the payment only where appropriate;
- securely destroy the card information immediately afterwards;
- advise the customer not to send payment card information using that method again.

14. Refunds

Refunds should:

- be authorised by an appropriate member of staff;

- be returned to the original payment card wherever possible;
- never be paid to an unrelated payment card;
- be recorded within the merchant's financial records.

15. Incident Reporting

Merchants must notify Vesta Merchant Services immediately if they suspect:

- payment terminal tampering;
- unauthorised access to payment information;
- malware affecting payment systems;
- loss of payment receipts;
- accidental storage of payment card information;
- any compromise of cardholder data.

Early reporting allows appropriate action to reduce potential risk.

16. Training

Merchants should ensure that all personnel who process payment card transactions:

- receive PCI awareness training before handling payments;
- complete refresher training annually;
- understand how to recognise payment security incidents;
- understand their responsibilities under this guidance.

17. Compliance Monitoring

VMS may periodically review merchant compliance with this guidance.

This may include:

- payment terminal inspections;
- merchant questionnaires;
- PCI compliance evidence;
- fraud monitoring;
- chargeback monitoring.

Failure to comply may result in:

- enhanced monitoring;
- additional fraud controls;
- suspension of payment facilities;
- termination of merchant services where appropriate.

18. Policy Review

This guidance will be reviewed:

- annually;
- following updates to PCI DSS;
- following changes to card scheme requirements;
- following significant payment security incidents.

References

- PCI DSS Version 4.0.1
- Visa Core Rules
- Mastercard Rules
- Merchant Agreement
- UK GDPR
- Data Protection Act 2018

Appendix A – Cardholder Data

Cardholder Data (CHD)	Sensitive Authentication Data (SAD)
Primary Account Number (PAN)	Full Track Data
Cardholder Name	CVV/CVC/CID
Expiry Date	PIN
Service Code	PIN Block

Appendix B – Daily Payment Terminal Checklist

- Inspect terminal casing for damage or tampering.
- Check serial numbers and security seals.
- Ensure only masked PAN is displayed.
- Confirm no unauthorised devices are attached.
- Verify the terminal is operating correctly.
- Record the inspection.

Appendix C – MOTO Best Practice Checklist

Before processing a telephone or mail order payment:

- Verify the customer's identity where appropriate.
- Enter payment details directly into the approved payment system.
- Never write down or electronically store payment card information.
- Do not repeat the full PAN back to the customer.
- Ensure telephone systems do not retain payment card information.
- Obtain proof of delivery for dispatched goods where applicable.
- Retain supporting transaction records in accordance with your retention policy.