MOTO Merchant User Policy

Version: 1.0

Effective date: [20/8/2026]

Policy URL: [Legal Documents | DNA Payments]

This policy is a procedure guide for the purposes of the Merchant Conditions. It applies where DNAP has approved a merchant to process mail-order or telephone-order transactions. If there is any inconsistency between this policy and the Merchant Conditions, the Merchant Conditions prevail.

Purpose

This policy sets out the controls merchants must follow to protect cardholder data and reduce the risk of fraud, disputes and Chargebacks when processing MOTO Transactions.

What is a MOTO Transaction?

A MOTO Transaction is a card-not-present transaction where card details are provided by the cardholder through a live telephone call or mail order and are entered manually by authorised merchant personnel into DNAP-approved payment functionality.

MOTO Transactions may not benefit from standard 3D Secure authentication. They therefore carry a materially higher risk of fraud, disputes and Chargebacks than card-present or appropriately authenticated online transactions.

dnapayments

Approval and permitted use

The merchant may process MOTO Transactions only where DNAP has expressly approved MOTO for that merchant. The merchant must process MOTO Transactions only:

- for its approved business activities and transaction profile;
- through DNAP-approved terminal or virtual-terminal functionality;
- in accordance with the Merchant Conditions, this policy, applicable law and Payment Scheme Rules; and
- using properly trained and authorised personnel.

DNAP may suspend MOTO approval or require the merchant to use Pay by Link or another DNAP-approved payment method where DNAP reasonably considers the merchant's MOTO risk profile unacceptable.

Cardholder data and sensitive authentication data

Cardholder Data includes a cardholder's primary account number, name and expiry date. **Sensitive Authentication Data** includes CVV/CVC and any other authentication data associated with a payment card.

The merchant must not write down, record, photograph, screenshot, copy, retain, transmit or store Cardholder Data or Sensitive Authentication Data except through DNAP-approved payment functionality and strictly in accordance with applicable PCI DSS requirements.

The merchant must never retain CVV/CVC after authorisation.

Prohibited channels

The merchant must not accept, or process card details received through:

- email;
- webchat;
- SMS or another messaging service;
- social-media message;
- paper form; or
- voicemail.

If card details are received through any prohibited channel, the merchant must not process the transaction using that message or record. The merchant must securely delete or destroy the message, record and any copies as soon as practicable and follow its incident-management process where required.

Before processing a MOTO Transaction

Before processing a MOTO Transaction, the merchant must take reasonable steps, appropriate to the nature and value of the transaction, to verify the customer and transaction. The merchant must give particular attention to transactions that are unusual, high value, repeated, inconsistent with the merchant's usual trading activity or otherwise suspicious.

The merchant must obtain clear customer authority for the transaction and must make clear:

- the merchant's identity;
- the goods or services being purchased;
- the total transaction amount;
- any material delivery, cancellation or refund terms; and
- a contact route for customer queries or refunds.

Records and co-operation

The merchant must retain non-card-data evidence sufficient to support fraud checks, customer complaints and Chargeback representment, including, where applicable:

- the customer order and contact details;
- the goods or services purchased;
- the transaction amount and date;
- delivery, collection or performance evidence;
- customer communications;
- cancellation and refund records; and
- any other information reasonably requested by DNAP, a relevant acquirer or a Payment Scheme.

The merchant must promptly notify DNAP of any suspected fraud, disputed MOTO Transaction, data-security incident or Chargeback, and provide all information and co-operation reasonably requested.

Chargebacks, disputes and risk

Authorisation of a MOTO Transaction does not guarantee payment or protection from Chargeback. The merchant remains liable under the Merchant Conditions for Chargebacks, Refunds, scheme fees, fines, losses and other Merchant Liabilities arising from or relating to MOTO Transactions, except to the extent caused by DNAP's fraud, negligence or breach of the Merchant Conditions.

DNAP may, but is not obliged to, assist the merchant with Chargeback representment. The merchant must not represent to a customer that a MOTO Transaction is irreversible or protected from dispute or Chargeback.

More secure alternatives

Where appropriate, the merchant should use DNAP's Pay by Link solution or another DNAP-approved payment method. These methods may provide stronger authentication and a lower fraud risk than MOTO Transactions.

Policy compliance

Failure to comply with this policy may result in suspension or withdrawal of MOTO approval, suspension of services, termination of the Merchant Conditions, withholding or recovery of funds, and any other remedy available to DNAP under the Merchant Conditions or applicable law.