Response Codes and Error Codes

HTTP Response Codes

Successfully processed API requests will result in response messages with HTTP code 200 (OK). A transaction response with an 'APPROVED' status (`"status": "APPROVED"`) indicates that the transaction was successful. In some situations, a transaction response can have an 'UNKNOWN' status, see Transaction Responses with an 'UNKNOWN' Status.

If the transaction is declined, the API response is a 402 error with `"ReasonCode": "DECLINE"`.

Below is a complete list of the response codes that the application may return for requests. In the event of network or infrastructure issues, other response codes may be returned by the infrastructure.

NOTE: For further information about 4xx/5xx response codes and possible resolutions, see Gateway Error Codes. The error response message parameters are described in Error Codes.

HTTP Response Codes	Description
200 OK	The request was completed successfully.
201 CREATED	Successful creation occurred via a POST. The Location header will contain a link to the newly-created resource.
202 ACCEPTED	The request was accepted but did not complete during the allotted timeframe. Processing of the request will continue asynchronously. Submitting a GET on the resource specified in the Location header will provide the current status of the underlying request, returning a status of PENDING until the request completes (successfully or not).
400 BAD REQUEST	General error when the request could not be fulfilled due to errors such as validation errors or missing required data.
401 UNAUTHORIZED	Error code response for missing or invalid authentication token.
402 REQUEST FAILED	Financial transaction was declined. Parameters were valid but request failed.

HTTP Response Codes	Description
403 FORBIDDEN	The user is not authorized to perform the operation or the resource is unavailable for some reason (e.g. time constraints).
404 NOT FOUND	The requested resource is not found.
405 METHOD NOT ALLOWED	Used to indicate that the requested URL exists, but the requested HTTP method is not applicable. For example, POST /users/12345 where the API doesn't support creation of resources this way (with a provided ID). The Allow HTTP header must be set when returning a 405 to indicate the HTTP methods that are supported. In the previous case, the header would look like "Allow: GET, PUT, DELETE"
409 CONFLICT	Whenever a resource conflict would be caused by fulfilling the request. Duplicate entries, such as trying to create two customers with the same information, and deleting root objects when cascade-delete is not supported are a couple of examples.
429 TOO MANY REQUESTS	The 429 status code indicates that the user has sent too many requests in a given amount of time ("rate limiting").The response will include a Retry-After header indicating how long to wait before making a new request.This is a courtesy response. When the service is receiving a very large number of requests from a single party the system may just drop connections to minimize resource monopolization.
500 INTERNAL SERVER ERROR	The server encountered an unexpected condition which prevented it from fulfilling the request. It indicates an error that the caller cannot address from their end. Requests resulting in a 500 response code will generally include the Mastercard Merchant Presented QR API Errors structure in the response.
5XX SERVER ERROR	Errors that occur in the network infrastructure between the client and Mastercard Merchant Presented QR API server will typically result in a response code in the 500 range. Note that errors returned by the network infrastructure will never contain the Mastercard Merchant Presented QR API Errors structure in the response.

Reason Codes

The following table contains the Reason Code values and their descriptions:

Reason Code	Reason Description
PARTNER_DAILY_LIMIT	Partner has exceeded the daily limit configured in the system
MAX_TRANSACTION_LIMIT	Per transaction maximum amount limit reached
MIN_TRANSACTION_LIMIT	Amount is less than the minimum configured for the partner
CONS_MONTHLY_TRAN_LIMIT	Consumers monthly transaction limit reached
MAX_TRAN_TYPE_LIMIT	Per transaction maximum amount limit for the transaction type
MIN_TRAN_TYPE_LIMIT	Amount is less than the minimum allowed for the transaction type
ACCOUNT_TYPE	Account Type not supported for the partner
ACCOUNT_NOT_ELIGIBLE	Account not eligible
NETWORK_NOT_ELIGIBLE	Partner not on boarded for the network to reach account
CURRENCY_NOT_SUPPORTED	Currency is not supported for the account

Error Codes

4xx/5xx error response messages have the following format (the `Error` array may contain multiple error items):

```
{
  "Errors": {
    "Error": [
      {
        "RequestId": "rqst_73HB-5RO5-0OGS-53SG",
        "Source": "account_uri",
        "ReasonCode": "INVALID_INPUT_VALUE",
        "Description": "Invalid Account URI",
        "Recoverable": "false",
        "Details": {
          "Detail": [
            {
              "Name": "ErrorDetailCode",
              "Value": "082000"
            }
          ]
        }
      }
```

```
    ]
  }
}
<Errors>
   <Error>
      <RequestId>rqst_73HB-5RO5-0OGS-53SG</RequestId>
      <Source>account_uri</Source>
      <ReasonCode>INVALID_INPUT_VALUE</ReasonCode>
      <Description>Invalid Account URI</Description>
      <Recoverable>false</Recoverable>
      <Details>
         <Detail>
            <Name>ErrorDetailCode</Name>
            <Value>082000</Value>
         </Detail>
      </Details>
   </Error>
</Errors>
```

Field	Description
RequestId	An application-specific request identifier. Example: rqst_73HB-5RO5-0OGS-53SG
Source	The unique identifier that attempts to define the field in error, when available. If an error is not associated with a specific field, System will be returned. If an error is produced because of required data, it would be presented with the field missing data. Examples: SYSTEM_ERROR, amount, account_uri
ReasonCode	The general cause of the error; see the table below. Examples: INVALID_INPUT_FORMAT, INVALID_INPUT_LENGTH, INVALID_INPUT_VALUE, SYSTEM_ERROR
Description	A textual description of the error. This is optional and will only be displayed if more information is available than is stored in the data identifier and reason code. Examples: Invalid Account URI, Destination Currency ISO code must be within 3 characters length
Recoverable	A true/false indicator stating whether your API request might be successful if you re-sent the API request with the same parameters and data. For example, an unsuccessful API request caused by a server error (5xx response code) might be successful when re-sent. Valid values: true, false
Details	Each Open API service has an option to add extra service-specific error information in the Details section. The details are optional and might not be present for every error message. If present, the details are returned in the form of individual detail items, each containing a Name and Value pair:

Field	Description
	• The Name element will explain what data you will find in the Value element. Example: ErrorDetailCode • The Value element will hold the actual data. Valid values shown in the table below. Example: 082000

Error Detail Codes

The following table shows the `ErrorDetailCode`, `ReasonCode` and `Description` values that can be returned in 4xx and 500 error response messages. Other values might also exist or be introduced periodically. For more information about 4xx/5xx response codes and possible resolutions, see Gateway Error Codes.

Error Detail Code	Reason Code	Description
050005	AUTHORIZATION_FAILED	Transaction processing suspended
050007	AUTHORIZATION_FAILED	Unauthorized access
062000	INVALID_INPUT_FORMAT	Value contains invalid character
072000	INVALID_INPUT_LENGTH	Invalid length
082000	INVALID_INPUT_VALUE	Invalid value
092000	MISSING_REQUIRED_INPUT	Value is required
110501	RESOURCE_ERROR	Duplicate value

Error Detail Code	Reason Code	Description
110502	RESOURCE_UNKOWN	No default account is defined for the consumer
110503	RESOURCE_ERROR	Account not eligible
110504	RESOURCE_ERROR	Card type is not supported for merchant
110506	RESOURCE_ERROR	Network routing preference disabled
110507	RESOURCE_UNKOWN	Record not found
110508	RESOURCE_ERROR	Primary contact cannot be deleted
110509	RESOURCE_ERROR	Updating a different type of URI is not allowed
110510	RESOURCE_ERROR	Invalid Request
110511	RESOURCE_ERROR	Operation not allowed
110515	RESOURCE_ERROR	Multiple resources found
110516	RESOURCE_ERROR	Country not supported for merchant
110522	RESOURCE_ERROR	Acquiring credential used for the funding transaction is no longer valid
110523	RESOURCE_ERROR	Payment cannot be processed since the sending PAN does not match the funding transaction’s sending PAN
130001	DECLINE	Card declined This error code can be returned for many different issuer reasons. To get further details, use a Retrieval

Error Detail Code	Reason Code	Description
		API call to retrieve information about the transfer. The `network_status_code` and `network_status_description` response fields will indicate the issuer's reason for declining the transaction, see Network Response Codes.
130002	DECLINE	Fraud detected
130003	DECLINE	Card expired
130004	DECLINE	Per transaction maximum amount limit reached. Note: Additional details will be provided in some scenarios
130005	DECLINE	Partner has exceeded the daily limit configured in the system
130006	DECLINE	Transaction Limit is less than the minimum configured for the partner
130007	DECLINE	Consumer has exceeded the monthly limit configured in the system

Network Response Codes

Mastercard includes the Network Response Codes (ISO Codes) from the receiving networks in HTTP 200 response messages, in fields `network_status_code` and `network_status_description`. The Response Code indicates an issuer's reason for approving or declining a transaction, and it is passed to Mastercard in Data Element (DE) 39 of the issuer's network response message.

The table below lists the main valid codes for Mastercard network messages. Some codes might not be relevant to MPQR. Other codes might be provided and the descriptions might vary depending on the message system and network.

For more information about network response codes, refer to the *DE 39 (Response Code)* section in either of these documents, which are available in the Technical Resource Center on Mastercard Connect:

- *Mastercard Network Processing Dual Message Authorization System Guide*
- *Mastercard Network Processing Single Message System Guide*

NOTE: Remember that declined transactions result in a 402 error response at the time, which will not include these fields. However, subsequent retrieval lookup responses for those transactions, using the Retrieval API, will include these fields.

ISO Code	Description
00	Approved or completed successfully
01	Refer to card issuer
03	Invalid merchant
04	Capture card
05	Do not honor
08	Honor with ID
10	Partial Approval
12	Invalid transaction
13	Invalid amount
14	Invalid card number
15	Invalid issuer
30	Format error
41	Lost card
43	Stolen card
51	Insufficient funds/over credit limit
54	Expired card
55	Invalid PIN
57	Transaction not permitted to issuer/cardholder
58	Transaction not permitted to acquirer/terminal

ISO Code	Description
61	Exceeds withdrawal amount limit
62	Restricted card
63	Security violation
65	Exceeds withdrawal count limit
70	Contact Card Issuer
71	PIN Not Changed
75	Allowable number of PIN tries exceeded
76	Invalid/nonexistent “To Account” specified
77	Invalid/nonexistent “From Account” specified
78	Invalid/nonexistent account specified (general)
79	Life cycle (Mastercard use only)
80	System not available
81	Domestic Debit Transaction Not Allowed (Regional use only)
82	Policy (Mastercard use only)
83	Fraud/Security (Mastercard use only)
84	Invalid Authorization Life Cycle
85	Not declined
86	PIN Validation not possible
87	Purchase Amount Only, No Cash Back Allowed
88	Cryptographic failure
89	Unacceptable PIN—Transaction Declined—Retry
90	Cutoff is in progress
91	Authorization System or issuer system inoperative
92	Unable to route transaction
94	Duplication transaction detected
96	System error

ISO Code	Description
1Z	Authorization System or issuer system inoperative

Transaction Responses with an ‘UNKNOWN’ Status

A timeout can occur when Mastercard does not receive a response from the Receive Network within the expected timeframe (40 seconds). In rare cases, such as timeouts or network communication issues, a transaction response can have an ‘UNKNOWN’ status. Mastercard will continue to retrieve the status from the Receive Network. If the transaction was approved or declined, the status will be changed accordingly and will be reflected in the Retrieval API response.

We recommend that Originating Institutions/Transaction Originators perform an API lookup (Retrieval API request) on the relevant transaction after a minute of receiving the ‘UNKNOWN’ status response. Originating Institutions/Transaction Originators must not resubmit a transaction that has an ‘UNKNOWN’ status, because the original transaction may have been processed successfully.

> In rare situations, an API lookup call after a minute may also result in an ‘UNKNOWN’ status response. In such exception situations, the final status will be reflected when Mastercard receives the details from the appropriate system within 24 hours.