



# **BELIZE BANK LIMITED CARD PAYMENT GATEWAY**

**Integration Guide**

**May 10, 2022  
Version 1.2**

# TABLE OF CONTENTS

|                                     |    |
|-------------------------------------|----|
| TABLE OF CONTENTS                   | 2  |
| CONFIDENTIALITY                     | 3  |
| HISTORY                             | 4  |
| INTRODUCTION                        | 5  |
| Purpose                             | 5  |
| Audience                            | 5  |
| SYSTEM ARCHITECTURE                 | 6  |
| Overview                            | 6  |
| Hosted Payment Page                 | 6  |
| Authentication                      | 9  |
| Postman Collection                  | 9  |
| Test Data                           | 9  |
| PAYMENT AUTHORIZATION ENDPOINT      | 10 |
| PAYMENT PRE-AUTHORIZATION ENDPOINT  | 13 |
| PRE-AUTHORIZATION CAPTURE ENDPOINT  | 16 |
| REVERSAL ENDPOINT                   | 18 |
| REFUND ENDPOINT                     | 20 |
| PAYMENT STATUS ENDPOINT             | 22 |
| PAYMENT VIA TOKENIZED CARD ENDPOINT | 25 |
| CALLBACK ENDPOINT                   | 27 |
| APPENDIX                            | 28 |
| Format of billingPayerData object   | 28 |
| List of values for operation field  | 28 |

# CONFIDENTIALITY

The information herein is confidential and proprietary. No disclosure, reproduction, or further dissemination of this document may be made without the express written consent of The Belize Bank Limited.

# HISTORY

| <b>Version</b> | <b>Date</b>    | <b>Description</b>           |
|----------------|----------------|------------------------------|
| 1.0            | March 25, 2022 | Initial document             |
| 1.1            | April 27, 2022 | Removal of certain features  |
| 1.2            | May 10, 2022   | Include tokenization feature |

# INTRODUCTION

## Purpose

This document contains the specifications to integrate to the Belize Bank Limited Card Payment Gateway. This gateway is used by the Bank to process credit and debit card payments on behalf of a merchant registered with the Belize Bank.

It must be noted no information contained in this document at any point supersedes the policies and procedures set forth in the Bank's Merchant Guidelines agreement, nor the regulations set forth by Visa and Mastercard.

## Audience

The primary audience of this document are software developers.

# SYSTEM ARCHITECTURE

## Overview

The Belize Bank Card Payment Gateway is a service available to merchants of the Belize Bank to process card payments via a merchant's system, more specifically a website or mobile app, in a completely automated fashion.

Communication with the Belize Bank Card Payment Gateway is done via REST based web services. All requests will be sent as POST requests in application/x-www-form-urlencoded type. All responses will be sent as JSON objects. This provides an operating system, programming language, and hardware platform independent interface.

Access to a test environment will be provided. Merchants must be able to demonstrate successful integration with the Belize Bank Card Payment Gateway test environment before being allowed to connect to the production environment of the same.

The URL and credentials to connect to the test and production environment will be provided outside of this document. The specifications provided below remain the same regardless of the environment being connected to; and will be indicated by the placeholder `{payment-url}`.

Integration is performed using the hosted payment page concept.

## Hosted Payment Page

Using the hosted payment page concept, the card information will be entered and processed entirely on the Belize Bank Card Payment Gateway server.

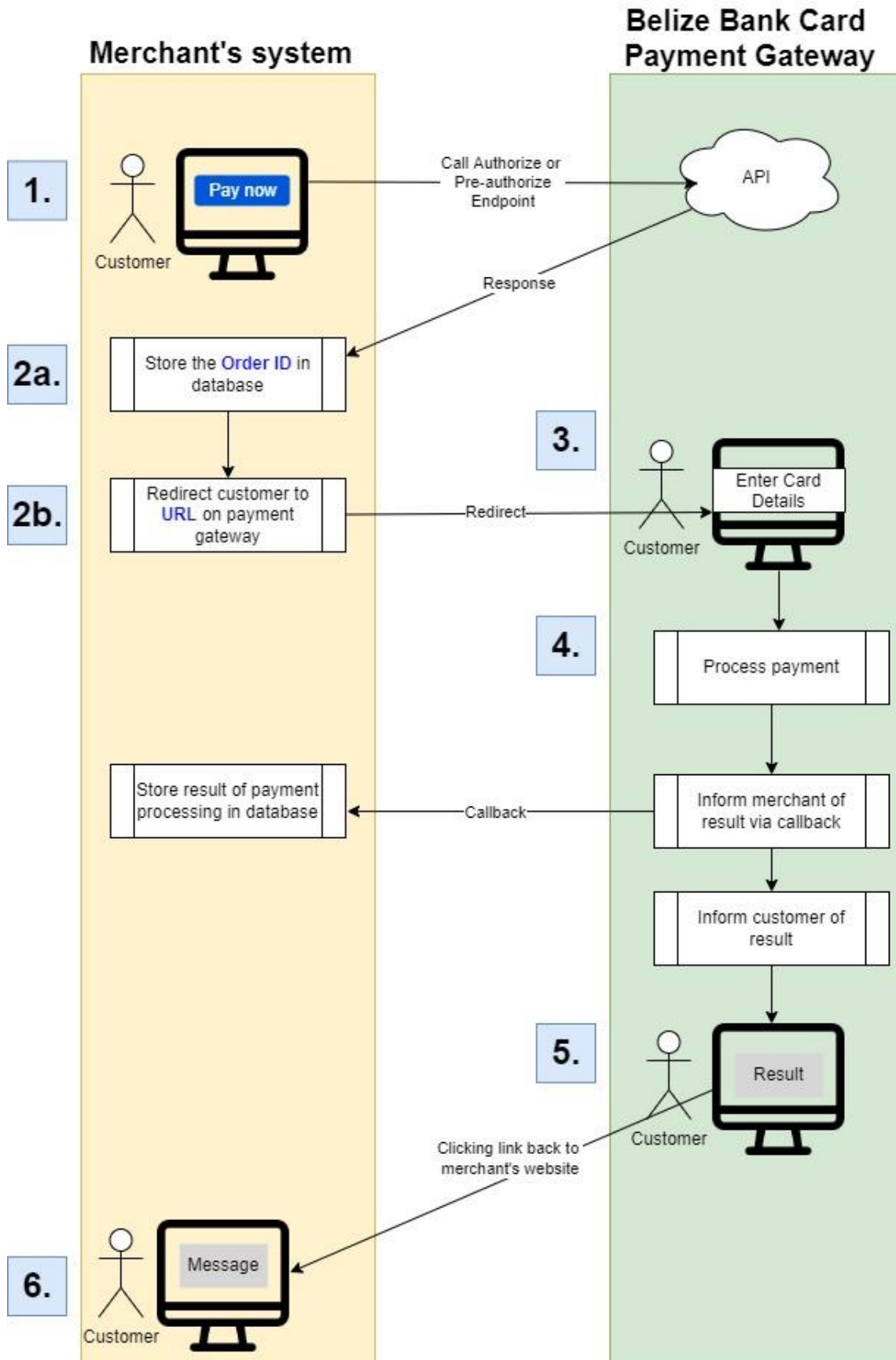
This method does not require the merchant's system to be PCI DSS compliant.

The flow between the merchant's website and the payment gateway is as follows:

1. When a customer is ready to perform payment, the merchant's website must call the [authorization](#) or [pre-authorization](#) endpoint
2. This endpoint in its response will return:
  - a. an order ID which must be stored in the merchant's system
  - b. A URL to a page hosted on the payment gateway to which the customer must be redirected
3. The customer will now enter the card information on this page
4. The payment gateway will process the payment and can optionally inform the merchant's system of the result via a callback function

5. The payment gateway will also inform the customer of the result of the processing of the payment
6. The page containing the result of the payment will also contain a link to direct the customer back to the merchant's website

A diagram of this flow is shown below





## Authentication

Each merchant will be provided with a username and password which must be used when sending a request to the payment gateway. It is the responsibility of the merchant to safeguard these credentials.

## Postman Collection

A Postman collection is available for download and use for testing all endpoints of the payment gateway. This Postman collection can be downloaded [here](#).

There are 3 variables defined in the Postman collection that must be set before calling any endpoint: `server`, `username`, and `password`. The values to place in these variables will be provided by The Belize Bank.

## Test Data

The following card numbers can be used when performing transactions in the test environment.

| Card Number      | Expiration Date | CVC | Expected Result   |
|------------------|-----------------|-----|---|
| 5555555555555599 | 12/24           | 123 | Successful transaction                                  |
| 4444444444446666 | 12/24           | 123 | Denied due to card limit                                |
| 4444444411111111 | 12/24           | 123 | Declined by network                                     |
| 4111111111111111 | 12/24           | 123 | This transaction will be subject to 3DS authentication. |

# PAYMENT AUTHORIZATION ENDPOINT

**Purpose:** This endpoint must be used by the merchant's system to accept and process a payment being made by its customer.

**URL:** {payment-url}/register.do

## Request Body:

| Field name          | Use       | Description  |
|---------------------|-----------|--|
| userName            | Mandatory | This is the user name. It is used to authenticate the origin of the request message.   |
| password            | Mandatory | This is the password. Used to authenticate the origin of the request message.  |
| amount              | Mandatory | The amount of the transaction. The amount must be 2 decimal places implied. For example \$45.00 must be sent as 4500   |
| description         | Optional  | A description of the goods or services being purchased associated with the payment.  |
| returnURL           | Mandatory | This is the URL the merchant will be redirected to upon clicking the "Return to Merchant" link in the page showing the result of the payment.  |
| orderNumber         | Mandatory | This is the unique identifier of this order in the merchant's system. You cannot submit multiple authorization requests with the same order number.  |
| clientId            | Optional  | This is the unique identifier of the merchant's customer in the merchant's system. This value is used as part of the tokenization feature to link a saved card to a customer. Extreme care must be used when populating this field to ensure a saved card for one customer is not shown to another customer. |
| email               | Optional  | The email of the customer performing the payment. If specified, the payment gateway will send an email receipt of the payment performed to this specified email address.   |
| dynamicCallback Url | Optional  | The URL on the merchant's system that will be called by the card payment gateway to inform the merchant of an event on this authorization.   |

|                  |          |   |
|------------------|----------|---|
| billingPayerData | Optional | The billing address of the cardholder, used for the address verification service (AVS) check. The format of this field is defined in the <a href="#">Appendix</a> . |
|------------------|----------|---|

### Request Example:

```
(
  "userName":"testuser",
  "password":"testpassword",
  "amount":4500,
  "description":"Order #52. Hollister Shirt.",
  "returnURL":"https://merchant-website.com",
)
```

### Response Body:

| Field name   | Description  |
|--------------|--|
| orderId      | Order ID of this payment in the card payment gateway. This value must be stored in the merchant's system as it is used when performing related actions for this payment such as <a href="#">reversals</a> , <a href="#">refunds</a> , and inquiring about the <a href="#">payment status</a> . |
| formURL      | The URL of the payment page on the payment gateway the merchant's system needs to direct its customer to.  |
| errorCode    | This field will only be present if the endpoint call was unsuccessful. It will contain a code to help identify the reason for the error.   |
| errorMessage | This field will only be present if the endpoint call was unsuccessful. It will contain a description of the error.   |

### Successful Response Example:

```
{
  "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
  "formURL":"https://gateway-website.com/payment.html?mdOrder=669e55c4-f72b-729c-be53-b7e100b0b260&language=en",
}
```

### Unsuccessful Response Example:

```
{
  "errorCode":4,
  "errorMessage":"The amount field is empty",
}
```

}

# PAYMENT PRE-AUTHORIZATION ENDPOINT

**Purpose:** This endpoint must be used by the merchant's system to process a pre-authorization on the card. This endpoint will not charge the card but place a hold so a charge can be placed later when the final payment amount is known. This pre-authorization can subsequently be converted to a charge on the account using the [pre-authorization capture](#) endpoint.

**URL:** {payment-url}/registerPreAuth.do

## Request Message Body:

| Field name      | Use       | Description  |
|-----------------|-----------|--|
| userName        | Mandatory | This is the user name. It is used to authenticate the origin of the request message.   |
| password        | Mandatory | This is the password. Used to authenticate the origin of the request message.  |
| amount          | Mandatory | The amount of the transaction. The amount must be 2 decimal places implied. For example \$45.00 must be sent as 4500   |
| description     | Optional  | A description of the goods or services being purchased associated with the payment.  |
| returnURL       | Mandatory | This is the URL the merchant will be redirected to upon clicking the "Return to Merchant" link in the page showing the result of the payment.  |
| orderNumber     | Mandatory | This is the unique identifier of this order in the merchant's system. You cannot submit multiple authorization requests with the same order number.  |
| clientId        | Optional  | This is the unique identifier of the merchant's customer in the merchant's system. This value is used as part of the tokenization feature to link a saved card to a customer. Extreme care must be used when populating this field to ensure a saved card for one customer is not shown to another customer. |
| email           | Optional  | The email of the customer performing the payment. If specified, the payment gateway will send an email receipt of the payment performed to this specified email address.   |
| dynamicCallback | Optional  | The URL on the merchant's system that will be called by the  |

|                  |          |   |
|------------------|----------|---|
| Url              |          | card payment gateway to inform the merchant of an event on this pre-authorization.  |
| billingPayerData | Optional | The billing address of the cardholder, used for the address verification service (AVS) check. The format of this field is defined in the <a href="#">Appendix</a> . |

#### Request Message Example:

```
(
  "userName":"testuser",
  "password":"testpassword",
  "amount":4500,
  "description":"Order #52. Hollister Shirt.",
  "returnURL":"https://merchant-website.com",
)
```

#### Response Message Body:

| Field name   | Description  |
|--------------|--|
| orderId      | Order ID of this payment in the payment gateway. This value must be stored in the merchant's system as it is used when performing related actions for this payment such as <a href="#">pre-authorization captures</a> , <a href="#">reversals</a> , <a href="#">refunds</a> , and inquiring about the <a href="#">payment status</a> . |
| formURL      | The URL of the payment page on the payment gateway the merchant's system needs to direct its customer to.  |
| errorCode    | This field will only be present if the endpoint call was unsuccessful. It will contain a code to help identify the reason for the error.   |
| errorMessage | This field will only be present if the endpoint call was unsuccessful. It will contain a description of the error.   |

#### Successful Response Message Example:

```
{
  "orderId":"669e55c4-f72b-729c-be53-b7e100b0b260",
  "formURL":"https://gateway-website.com/payment.html?mdOrder=669e55c4-f72b-729c-be53-b7e100b0b260&language=en",
}
```

#### Unsuccessful Response Message Example:

```
{
```

```
"errorCode":4,  
"errorMessage":"The amount field is empty",  
}
```

# PRE-AUTHORIZATION CAPTURE ENDPOINT

**Purpose:** This endpoint must be used when settling a pre-authorization performed using the [payment pre-authorization](#) endpoint; and converting said pre-authorization to a charge on the card.

**URL:** {payment-url}/deposit.do

## Request Body:

| Field name | Description | Detail  |
|------------|-------------|---|
| userName   | Mandatory   | This is the user name. It is used to authenticate the origin of the request message.  |
| password   | Mandatory   | This is the password. Used to authenticate the origin of the request message.   |
| orderId    | Mandatory   | This must be the same the order ID obtained in the response message of the pre authorization endpoint   |
| amount     | Mandatory   | This is the amount to charge to the card. The amount must be 2 decimal places implied. For example \$45.00 must be sent as 4500. The maximum amount that can be charged to the card using the pre-authorization capture must adhere to Visa and Mastercard regulations. |

## Request Body Example:

```
(  
  "userName": "testuser",  
  "password": "testpassword",  
  "orderId": "669e55c4-f72b-729c-be53-b7e100b0b260",  
  "amount": 4525  
)
```

## Response Message Body:

| Field name | Description   |
|------------|---|
| errorCode  | A code indicating if the endpoint call was successful. A value of 0 means the call was successful. Any other value means the call was not successful. |



|              |   |
|--------------|---|
| errorMessage | This field will contain a description of the error if the endpoint call was unsuccessful. |
|--------------|---|

**Successful Response Message Example:**

```
{  
  "errorCode":0,  
  "errorMessage":"Success",  
}
```

**Unsuccessful Response Message Example:**

```
{  
  "errorCode":5,  
  "errorMessage":"Deposited amount is exceeding approved amount",  
}
```

# REVERSAL ENDPOINT

**Purpose:** This endpoint can be used to void or reverse a payment. A payment can only be voided or reversed if it has not been settled.

**URL:** {payment-url}/reverse.do

## Request Body:

| Field name | Description | Detail  |
|------------|-------------|---|
| userName   | Mandatory   | This is the user name. It is used to authenticate the origin of the request message.                                |
| password   | Mandatory   | This is the password. Used to authenticate the origin of the request message.                                       |
| orderId    | Mandatory   | This must be the same order ID obtained in the response message of the authorization or pre authorization endpoint. |

## Request Body Example:

```
(  
  "userName": "testuser",  
  "password": "testpassword",  
  "orderId": "669e55c4-f72b-729c-be53-b7e100b0b260",  
)
```

## Response Message Body:

### Successful Response Message Example:

```
{  
  "errorCode": "0",  
  "errorMessage": "Success",  
}
```

### Unsuccessful Response Message Example:

```
{  
  "errorCode": 7,
```

```
"errorMessage": "Reversal is impossible for current transaction  
state",  
}
```

# REFUND ENDPOINT

**Purpose:** This endpoint can be used to perform a refund. A payment can only be refunded after it has been settled. A refund must be associated with a previously processed payment and can be partial or in full but cannot at any point exceed the amount of the related payment.

**URL:** {payment-url}/refund.do

## Request Body:

| Field name | Description | Detail  |
|------------|-------------|---|
| userName   | Mandatory   | This is the user name. It is used to authenticate the origin of the request message.                                |
| password   | Mandatory   | This is the password. Used to authenticate the origin of the request message.                                       |
| orderId    | Mandatory   | This must be the same order ID obtained in the response message of the authorization or pre authorization endpoint. |
| amount     | Mandatory   | The amount of the refund. The amount must be 2 decimal places implied. For example \$45.00 must be sent as 4500     |

## Request Body Example:

```
(  
  "userName": "testuser",  
  "password": "testpassword",  
  "orderId": "669e55c4-f72b-729c-be53-b7e100b0b260",  
  "amount": 4500  
)
```

## Response Message Body:

### Successful Response Message Example:

```
{  
  "errorCode": "0",  
  "errorMessage": "Success",  
}
```

### Unsuccessful Response Message Example:

```
{  
  "errorCode":7,  
  "errorMessage":"Refund is impossible for current transaction  
state",  
}
```

# PAYMENT STATUS ENDPOINT

**Purpose:** This endpoint can be used to obtain the status of a payment.

**URL:** {payment-url}/getOrderStatusExtended.do

## Request Body:

| Field name | Description | Detail   |
|------------|-------------|--|
| userName   | Mandatory   | This is the user name. It is used to authenticate the origin of the request message.                                   |
| password   | Mandatory   | This is the password. Used to authenticate the origin of the request message.  |
| orderId    | Mandatory   | This must be the same the order ID obtained in the response message of the authorization or pre authorization endpoint |

## Request Body Example:

```
(  
  "userName": "testuser",  
  "password": "testpassword",  
  "orderId": "669e55c4-f72b-729c-be53-b7e100b0b260",  
)
```

## Response Message Body:

| Field name   | Description  |
|--------------|--|
| errorCode    | A code indicating if the endpoint call was successful. A value of 0 means the call was successful. Any other value means the call was not successful.  |
| errorMessage | Error Message. This field will contain a description of the error if the endpoint call was unsuccessful.   |
| orderStatus  | The status of the transaction. It can have the possible following values: <ul style="list-style-type: none"><li>● 0 - transaction was registered but not paid</li><li>● 1 - pre-authorized amount is on hold on the buyer's account (for two-phase payments)</li><li>● 2 - transaction amount is fully authorized</li><li>● 3 - transaction canceled</li></ul> |

|                  |   |
|------------------|---|
|                  | <ul style="list-style-type: none"> <li>● 4 - transaction refunded</li> <li>● 5 - access control server of the issuing bank initiated authorization procedure</li> <li>● 6 - authorization declined</li> </ul> |
| date             | The date and time the transaction was initiated in epoch. For example a value of 1648501318153 means Mon Mar 28 2022 15:01:58 GMT-06:00   |
| refundedDate     | The date and time the transaction was partially or fully refunded. In the scenario of multiple partial refunds, this field contains the date and time of the most recent refund.                              |
| authDateTime     | The date and time the transaction was authorized.   |
| ip               | The IP address from where the merchant's customer initiated the transaction   |
| bindingID        | The tokenized value of the card used if the cardholder decided to save his card on the card payment gateway for future use  |
| cardAuthInfo     | This is a parent tag. The child fields are below.   |
| ->maskedPan      | The card number in masked form used to perform the transaction. For example 555555**5599  |
| ->cardholderName | The name entered when performing the transaction.   |
| ->approvalCode   | The approval code issued for this transaction.  |

#### Successful Response Message Example:

```

{
  "errorCode": "0",
  "errorMessage": "Success",
  "orderStatus": 4,
  "amount": 4500,
  "date": 1648501318153,
  "refundedDate": 1648501672000,
  "ip": "179.42.221.32",
  "cardAuthInfo": {
    "maskedPan": "555555**5599",
    "cardholderName": "JOHN TEST",
    "approvalCode": "123456",
  },
}

```

### Unsuccessful Response Message Example:

```
{  
  "errorCode":6,  
  "errorMessage":"Order not found",  
}
```



# PAYMENT VIA TOKENIZED CARD ENDPOINT

**Purpose:** This endpoint can be used to perform an authorization or pre-authorization using a tokenized card.

**URL:** {payment-url}/paymentOrderBinding.do

## Request Body:

| Field name | Description | Detail   |
|------------|-------------|--|
| userName   | Mandatory   | This is the user name. It is used to authenticate the origin of the request message.   |
| password   | Mandatory   | This is the password. Used to authenticate the origin of the request message.          |
| mdOrder    | Mandatory   | This must be the orderID returned from the authorization or pre-authorization endpoint |
| bindingID  | Mandatory   | This must be the bindingID returned from the payment status endpoint                   |

## Request Body Example:

```
(  
  "userName": "testuser",  
  "password": "testpassword",  
  "orderId": "669e55c4-f72b-729c-be53-b7e100b0b260",  
  "bindingID": "9ca72329-f228-7b6b-81c2-032e00b0b260",  
)
```

## Response Message Body:

| Field name   | Description   |
|--------------|---|
| errorCode    | A code indicating if the endpoint call was successful. A value of 0 means the call was successful. Any other value means the call was not successful. |
| errorMessage | Error Message. This field will contain a description of the error if the endpoint call was unsuccessful.  |
| redirect     | The URL of a page on the card payment gateway that can be shown to  |

|           |   |
|-----------|---|
|           | the cardholder indicating the payment was successful    |
| info      | An optional message that can be shown to the cardholder |
| bindingID | The bindingID sent in the request message               |

#### Successful Response Message Example:

```
{
  "redirect": "https://sandbox.radarpayment.online/payment/merchants/e.com/finish.html?orderId=367ad754-1c27-778a-a109-7f6d00b0b260&lang=en",
  "info": "Your order is proceeded, redirecting...",
  "errorCode": 0,
  "bindingId": "9ca72329-f228-7b6b-81c2-032e00b0b260"
}
```

#### Unsuccessful Response Message Example:

```
{
  "error": "No order found",
  "errorCode": 2,
  "errorMessage": "No order found"}
}
```

# CALLBACK ENDPOINT

**Purpose:** This endpoint can be used by the merchant's system to be informed when an event has occurred on a previously submitted authorization or pre-authorization on the Belize Bank Card Payment Gateway.

This endpoint must be accessible on the merchant's system via a HTTP post method.

A callback is triggered when any of the following actions occur on a authorization or pre-authorization:

- A pre-authorization has been approved
- An authorization has been approved
- A pre-authorization has been captured
- An authorization has been reversed or voided
- A refund has occurred

**URL:** Value provided in the dynamicCallbackUrl field in the authorization or pre-authorization request

**Request Body:**  
Not applicable

## Response Body:

| Field name  | Description | Detail   |
|-------------|-------------|--|
| orderNumber | Mandatory   | The order number assigned to this payment by the merchant's system   |
| mdOrder     | Mandatory   | The order ID assigned to this payment by the card payment gateway  |
| operation   | Mandatory   | The operation which triggered the callback. The possible values for this field are defined in the <a href="#">Appendix</a> . |
| status      | Mandatory   | The status of the transaction. A value of 0 means success. A value of 1 means error.   |

## Successful Response Message Example:

```
orderNumber=65436&mdOrder=2593e67b-f5cc-7fc3-a85d-98f400b0b260&operation=deposited&status=1
```

# APPENDIX

## Format of billingPayerData object

| Field name          | Mandatory | Description  |
|---------------------|-----------|--|
| billingCity         | Yes       | The city registered on a specific card of the Issuing Bank.  |
| billingCountry      | No        | The country registered on a specific card of the Issuing Bank ( ISO 3166-1, numeric).  |
| billingAddressLine1 | No        | The address registered on a specific card of the Issuing Bank. Line 1. Mandatory to be passed in order AVS verification works. |
| billingAddressLine2 | No        | The address registered on a specific card of the Issuing Bank. Line 2.   |
| billingAddressLine3 | No        | The address registered on a specific card of the Issuing Bank. Line 3.   |
| billingPostalCode   | Yes       | Postal code registered on a specific card of the Issuing Bank. Mandatory to be passed in order AVS verification works.         |
| billingState        | No        | The state registered on a specific card of the Issuing Bank (ISO 3166-2).  |

Example of object: {"billingCity":"City", "billingPostalCode":"12345"}

## List of values for operation field

| Value     | Comment  |
|-----------|--|
| approved  | Used when a pre-authorization has been approved  |
| deposited | Used when an authorization has been approved, or a pre-authorization has been captured |
| reversed  | Used when an authorization has been reversed or voided                                 |
| refunded  | Used when a refund has occurred  |

