Application Programming Interface

COPYRIGHT

Printed in Philippines
Version 1.10.10
Updated Release: August 20, 2020

CONTACT INFORMATION

For questions relating to this document please contact:

Paynamics Technologies Inc.
1108 Cityland 10 Tower 2
H.V. Dela Costa St. Makati City
P.C. 1227 Philippines

Phone: +632 330 8772
E-mail: technical@paynamics.net

Contents

1. INTRODUCTION

1.1 AUDIENCE

This specification is primarily intended for merchants connecting to the Paynamics Paygate Platform via the Responsive Payment Frontend Solution.

1.2 DOCUMENT CONVENTIONS

This document uses the following conventions:

- The Courier New font is used for example code and code listings, file names, commands, path names, directory names, Hypertext Markup Language (HTML) tags, and any text that must be typed on the screen.
- The *italic* font is used in code to represent placeholder parameters (variables) that should be replaced with an actual value or items that require emphasis.
- Brackets ([]) are used to enclose optional parameters.

1.3 SOFTWARE REQUIREMENTS

To implement the HTTPS POST interface for standard card processing, the following requirements must be met:

- Internet connection supporting HTTP
- Working knowledge of POST and SOAP method
- SSL server supporting 128-bit (or stronger) encryption

1.4 REQUIRED SETTINGS

The exchange of POST messages is based on certain requirements. If these are not met, the request/response communication will fail. It is therefore imperative that the message elements are defined as required.

Mandatory*
A mandatory (man.) message is necessary to ensure the proper routine and posting of a POST / SOAP message. Any mandatory message element not included as requested will cause the process request type to be rejected.

Optional*
The inclusion or omission of an optional (opt.) message field is at the discretion of the merchant. A transaction request is also processed if an optional field is missing.

Conditional*
A conditional (con.) message field must be included in some instances. Its omission may cause the process request type to be rejected.

***Note:** What is being described as mandatory, optional and conditional fields refers to the parameter value being passed by the merchant system. The parameter name for all request elements are required to be sent regardless of the field is mandatory, optional or conditional.

Notation	Description
A	alphabetic A-Z, a-z
N	numeric digits, 0-9
An	alphanumeric characters
Ans	alphanumeric and special characters
DD	Day, 01 through 31
MM	Month, 01 to 12
YYYY	Year, 1999, 2000, 2001, etc.
Hh	Hours, 00 to 24
Mm	Minutes, 00 to 59
Ss	Seconds, 00 to 59
..17	Variable length up to a maximum of 17 bytes.
C	Collection of elements
T	A separator indicating that time-of-day follows
zzzzzz	Represents the timezone
F	Float

1.5 VERSION HISTORY

Date	Version	Description	Made by
May 4, 2020	1.10.4	• Updated Response Codes FR001 - FR012 , FR025, FR041 - FR045 , FR048 • Added Response Codes GR176 - GR178 • Updated payment method (i.e. grabpay, paymaya, coins, hsbinstall, etc). • Updated dispute code list.	RGM
May 25, 2020	1.10.7	• Added client_ip in the RPF Request. • Added Metrobank Installment payment method and dispute code. • Added Response Codes GR179 - GR180	RGM

Date	Version	Description	Made by
July 6, 2020	1.10.8	Added metadata2 parameter on the RPF Request. This is applicable for BDO Installment payments	LT
August, 20, 2020	1.10.10	• Deprecated the Notification Process call back response from the merchant. • Added GR181 response code.	RGM

1.6 URL OF TEST AND LIVE SYSTEM

Responsive Payment Frontend Test URL (POST Redirect):
https://testpti.payserv.net/webpayment/default.aspx

Responsive Payment Frontend Production URL:
To be requested

Refund, Reversal Settlement, Query
https://testpti.payserv.net/pnxquery/queryservice.asmx

Refund, Reversal Settlement, Dispute Query, Rebill Test URL (SOAP):
https://testpti.payserv.net/Paygate/ccservice.asmx

Refund, Settlement and Query Production URL:
To be requested

2. SECURE MESSAGING

2.1. OVERVIEW

Since the payment information is exchanged between the Merchant and the Paygate platform, it's important that the data exchange is safe and immune to hacking, man-in-middle attack possibilities. The following 3 aspects must be addressed.

- Integrity
- Non-repudiation
- Authentication

Integrity means that data cannot be modified without authorization. This is achieved by calculating the hash on the payload references.

Non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. This is achieved by calculating the SHA hash with 512 Bits from your sensitive data.

Authentication ensures that the identity of the sender can be determined by Paygate. This is achieved by using the SHA512 hash algorithm.

The high level process of signature generation and validation is depicted below:

2.2. WHAT IS SIGNATURE

RFC 2828 defines a digital signature as "a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

Open standard libraries are available that makes the signature generation and validation process rather seamless. Secondly the Signature has the meta information about the cryptographic algorithms used and which references used for the signature generation and validation. This eliminates the need of prior negotiation of the signature strategies.

2.3. AUTHENTICATION PROCESS

Merchant to Paygate authentication

Merchant to Paygate authentication is done by concatenating all the input parameters and signing the concatenated string.

Example:

```
Signature = Sign(mid + request_id + ip_address + notification_url + response_url + fname
+ lname + mname + address1 + address2 + city + state + country + zip + email + phone +
client_ip + amount + currency + secure3d + merchantkey)
```

Paygate to Merchant authentication

Paygate to Merchant authentication is done by signing the original XML response and appending the signature parameter to the XML.

Note: below is only a sample xml only, some nodes are omitted to shorten xml.

originalXMLResponse

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <saleResponse xmlns="http://test.payserv.net/">
      <saleResult>
        <application>
          <merchantid> </merchantid>
          <request_id> </request_id>
          <response_id> </response_id>
          <timestamp> </timestamp>
          <rebill_id> </rebill_id>
          <signature> </signature>
        </application>
        <responseStatus>
          <response_code> </response_code>
          <response_message> </response_message>
          <response_advise> </response_advise>
        </responseStatus>
      </saleResult>
    </saleResponse>
  </soap:Body>
</soap:Envelope>
```

signedXMLResponse

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <saleResponse xmlns="http://test.payserv.net/">
      <saleResult>
        <application>
          <merchantid> </merchantid>
          <request_id> </request_id>
          <response_id> </response_id>
          <timestamp> </timestamp>
          <rebill_id> </rebill_id>
```

```
            <signature>
  awto73YtoaL/408qbqvsrEMmkDFhnn3rJJ4SFBm+4ev4RtySTMdOmvOo8w6DHbJxvf9PIL+XInFZ+155V1ncqul
  L6V6AYC8UWEYDeCYXTdFhe3JmLkT23HQ4d/2q9XSUW49E4b6P+4b/VV6JOs6cmRc1Af8n5YDgIXumr/VHIjo=
  </signature>
          </application>
          <responseStatus>
            <response_code> </response_code>
            <response_message> </response_message>
            <response_advise> </response_advise>
          </responseStatus>
        </saleResult>
      </saleResponse>
    </soap:Body>
  </soap:Envelope>

Signature = Sign(merchantid + request_id + response_id + response_code + response_message
+ response_advise + timestamp + rebill_id +  merchantkey)
signedXMLResponse = Signature
```

3. TEST INTERFACE

Any merchant planning to integrate the Paynamics platform (Paygate) can test the integration on a dedicated test gateway and test URL. It is basically identical to the live HTTPS / SOAP gateway with the exception that none of the submitted payment requests actually trigger a movement of moneys.

As part of the Paynamics quality assurance, merchants are requested to perform several tests on the test gateway in cooperation with the Paynamics support organization prior to connecting to the live HTTPS / SOAP Gateway. This is to ensure a smooth and flawless communication and transaction data flow between the integrating company and Paynamics.

When sending test transaction you would encounter a dedicated Test response codes and format related codes. These return codes would assist you in sending the correct message format to our Paygate.

You can send test transactions to our system with varying amounts and in any currency using any of the transaction types described in this specification.

3.1 TEST ACCESS

To set up your test account access please contact technical@paynamics.net .

3.2 DEMOTEST PAGE

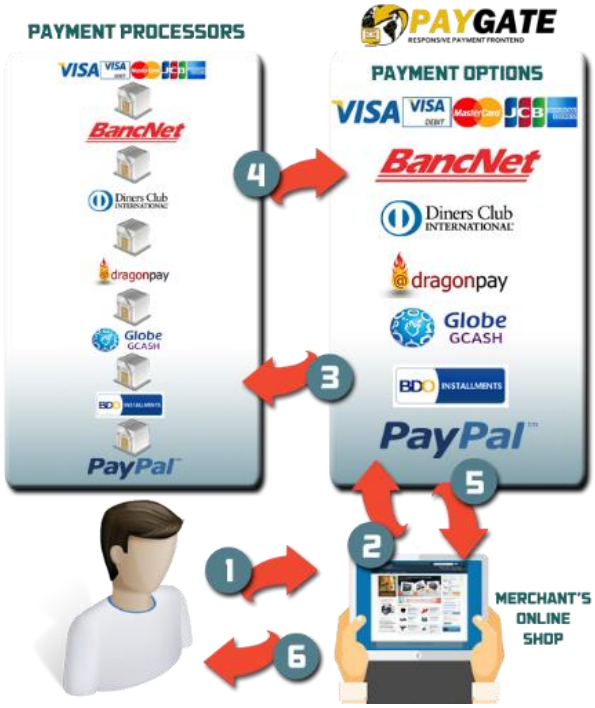
For a better workflow understanding, a demo page is provided at

https://testpti.payserv.net/paytravel/default.aspx

The demo page is fully implemented in ASP.Net and runs under IIS 8.5.

4. RESPONSIVE PAYMENT FRONTEND FLOW

The Illustration below would show a simple technical process flow of how the Merchant and PAYGATE Platform would connect and interact.



1. Customer visits merchant website and shops.
2. After shopping, customer proceeds to checkout page. Customer will be redirected to a Responsive Payment selection page that will allow him to choose what Payment type (i.e. Credit cards, Bancnet, Gcash) they would use.
3. Depending on the payment type that was chosen, customer will be redirected to the authorization process.
4. If the authorization is successful, Customer will be returned to an initial landing page displaying the transaction result status. Customer is then prompted to click "continue."
5. Paygate will return a response to the Merchant system and would redirect the customer back to the merchant website.
6. Merchant website will display result to the customer.

5. RESPONSIVE PAYMENT TRANSACTION (RPF)

5.1 REQUEST PROCESS

When initiating a WPF transaction, the merchant will be redirecting its customer to a payment selection page hosted with Paygate. The customer would need to select which payment method he/she would like to use.

The default transaction type for all payment methods under WPF is a "Sale" Transaction in which the customer's preferred payment method will be deducted immediately of the amount being paid during the payment process. For credit card, it is possible to do an Authorization and Pre-authorization (kindly refer to the request parameter table below for more information), kindly consult with your Paynamics Project Manager for more information about this functionality.

Depending on the Merchant Account Setup, the Merchant would be able to allow its customer to do the following payment method:

1. Credit Card transactions (Sale, Authorization, Pre-Authorization) – This transaction will allow customer to use their credit card to pay. Transaction type may vary according to the acquiring bank's acceptable transaction policy. For credit card transaction, the default transaction type is a "Sale"
2. Credit Card Transaction with 3d Secure (Sale, Authorization, Pre-Authorization) – This transaction will allow customer to use their credit card to pay along with a 3dsecure verification. Transaction type may vary according to the acquiring bank's acceptable transaction policy.
3. Bancnet (Sale) – Allows the customer to use Philippine based ATM cards associated with the Bancnet network. Customer would need to select his/her issuing bank and input their ATM Personal Identification Number (PIN) to complete the authorization process.
4. Gcash (Sale) – Allows the customer to use their Gcash mobile wallet. Customer would need to input their Globe mobile number. Gcash will send a Short Messaging Service (SMS) to the user prompting the user to key-in its MPIN (Mobile Personal Identification Number) to authorize the transaction.
5. Paynamics Over the Counter (Sale) – A Payment Network created by Paynamics that allows customer to perform over the counter payments through banks, convenience stores and alike. Paynamics allows the merchant to set expiry date and expiry time to make payment.
6. Paypal (Sale through Paypal Express Checkout) – Allows the customer to pay using his Paypal account. Customer will need to key his Paypal account information and password to authorize the transaction.
7. Other Payment Methods (i.e. ECONTEXT, ENETS, EGHL, ALIPAY etc) – Allows the customer to use online bank transfers, cash e-vouchers, e-wallet, Cash in-payment and alike. Kindly refer to Appendix B for updated list of payment methods.

Please check with your Paynamics Project Manager as to what type of Payment methods and transaction types will be allowed with your merchant account.

You can email technical@paynamics.net to request for sample integration codes.

RPF request parameters

Element	Settings	Type	Description
mid	man.	an..32	The merchant identifier with Paygate. This is equivalent to the "merchantid" parameter in the response.
request_id	man.	ans..32	Unique transaction identifier that the merchant has sent.
ip_address	con.	ans..20	This is the merchant's host i.p. address. This value is dependent on the merchant account configuration.
notification_url	man.	ans..255	This is the merchant URL where PAYGATE would POST base64 encoded xml notification update for their transaction or its final status. Data will be placed in "paymentresponse" variable.
response_url	man.	ans..255	This is the URL where Paygate will redirect the transaction after the result page.
cancel_url	man.	ans..255	This will be the merchant return URL that Paygate will call once the customer pressed cancel button.
mtac_url	opt.	ans..255	This URL will be a link to the Merchant's Terms and Conditions Page and must be hosted in https environment. If this value is filled, this link will be located during the payment selection process.
descriptor_note	con.	ans..255	Allows the merchant to input its credit card billing descriptor (and other information) to be displayed to the customer before the payment is processed. This value needs to be filled up if the merchant id is enabled for credit card processing.
fname	man.	an..30	The cardholder's first name.
lname	man.	an..32	The cardholder's last/surname.
mname	opt.	an..32	The cardholder's middle name
address1	man.	ans..100	The first line of the cardholder's billing address.
address2	opt.	ans..100	The second line of the cardholder's billing address.
city	man.	a..30	The town/suburb/city of the cardholder's billing address.
state	man.	a..30	The state/region/district/province of the cardholder's billing address. If the country is U.S. , kindly follow strictly the ISO 2 character format specified in this URL: https://faq.usps.com/s/article/What-are-the-USPS-abbreviations-for-U-S-states-and-territories
country	man.	a...3	The ISO 3166 two (2) character code for the country of the cardholder's billing address.
zip	con.	ans..12	The zip/post code of the cardholder's billing address. If the country is United States or Canada, this parameter is mandatory. For the postal code format of United States and Canada, refer to guidelines below: For Canada: -6 alpha-numeric value (ANA-NAN) A for alphabet, N for number. -Sample Format ANA NAN For United States, it can either be a -5 or 9 digit zip code

Element	Settings	Type	Description
			-When a 9-digit zip is passed, the dash character ("-") is mandatory -Sample Format five characters: NNNNN nine characters: NNNNN-NNNN
email	man.	ans..100	The email address of the cardholder. Format should be abc@abc.com. If this parameter is not available to be collected, kindly coordinate with your Paynamics Project Manager for possible solution.
phone	con.	ns..32	The telephone number for the cardholder. +xxx(yyy)zzz-zzzz-ppp where: xxx = Country code yyy = Area or city code zzz-zzzz = Local number ppp = PBX extension For example, a typical U.S. or Canadian number would be "+1(202)555-1234-739" indicating PBX extension 739 at phone number 5551234 within area code 202 (country code 1).
mobile	opt.	ns..32	Mobile number of the cardholder +xxx(yyy)zzz-zzzz where: xxx = Country code yyy = Mobile operator code zzz-zzzz = mobile number For example, a typical U.S. or Canadian number would be "+1(202)555-1234-739" indicating PBX extension 739 at phone number 5551234 within area code 202 (country code 1). This value will be needed if the transaction will undergo risk validation or SMS verification.
client_ip	con.	ans..20	This is the customer's browser assigned i.p. address. This value is required if the payment method is credit card (cc).
amount	man.	F..2	Amount of the transaction with decimal point. For transactions in cents, kindly input the 2 decimal place after the point (i.e. for $0.50 = 0.50). Pls take note that some international currencies would not accept transactions with decimal points (i.e. Japanese Yen)
currency	man.	a..3	The three (3) character ISO 4217 currency code used for the transaction. Please take note that in some cases, the currency type can be modified (i.e. non ISO) to cater specific payment methods. Please consult with your Paynamics Project Manager for more details on this setup.
pmethod	con.	ans..20	This field will allow the merchant to restrict the payment method being displayed to the customer in the payment selection page. The merchant can also set to display multiple payment methods to their customer by separating the values with a comma in this parameter (i.e. if merchant wants his/her customer to select Credit card and Gcash as a payment type, value of this parameter should be CC, GC). If the value of this parameter is null, Paygate will display the default payment methods that is enabled in the merchant id. Kindly refer Appendix B to know the other Payment method value.

Element	Settings	Type	Description
expiry_limit	con.	yyyy-MM-ddTHH:mm	This field is applicable for Paynamics Over the Counter Payment option. Merchant may specify the exact date and time the Transaction reference token will be valid for payment.
trxtype	con.	as..20	This parameter will allow the merchant to do an authorization / pre-authorization once the user selected credit card payment method during the checkout process. The allowable values are the following: • authorized (for Authorization) • preauthorized (for Pre-authorization) Kindly make sure that credit card payment method is enabled for your merchant id.
mlogo_url	opt.	ans..255	URL of merchant logo must be hosted in **https** environment. This will be displayed on the responsive payment frontend payment page. The ideal dimensions of the logo should be at 400 pixels (length) by 100 pixels (height).

orders	man.	ans..255	List of customer orders in xml format. Orders contain the Item name/Product Name, quantity, and amount.
			`<orders>`
			`<items>`
			`<Items>`
			`<itemname>Item 1</itemname>`
			`<quantity>0</quantity>`
			`<amount>5.00</amount>`
			`</Items>`
			`<Items>`
			`<itemname>item 2</itemname>`
			`<quantity>0</quantity>`
			`<amount>3.00</amount>`
			`</Items>`
			`</items>`
			`</orders>`
			This information will be displayed on the Responsive payment payment page as an order information. The data sent in this request can also be used by the merchant as a storage of customer's order details.
			Note that total order amount should be equal to the total transaction amount otherwise the transaction will be declined. After creating the xml request and before sending it to the responsive payment facility, the xml string should be base64encoded.

secure3d	opt.	an..6	Acceptable values are as follows: • **enabled** - Allows the merchant to enable 3d-secure transaction for the transaction. • **try3d** – Another acceptable value applied for specific acquiring bank that has a custom workflow. Paynamics project manager will advise merchant if this is the value to be used.
metadata2	con.	ans..255	This parameter will allow the merchant to define the BDO installment mode and term of the transaction. Format: `<metadata2>[mode]:[term]</metadata2>` **BDO 0% Installment**: mode: 1 Ex. `<metadata2>1:3,6,9,12</metadata2>` **BDO Regular Installment**: mode: 2 Ex. `<metadata2>2:3</metadata2>`
signature	man.	an..200	Hash (SHA512) computations of string concatenation of request parameters of this transaction and merchant certificate (downloaded on the Merchant Backend).

Note :
After creating the xml request and before sending it to the responsive payment facility, the xml string should be base64encoded.

5.2 GATEWAY RESPONSE

After processing the transaction, Paygate will send a post (server to server communication) to notification_url and a browser redirect to the response_url. It is preferred that the notification URL is on a SSL environment to ensure high confidentiality of data.

RPF Response parameters

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent with the original transaction.
response_id	man.	ans..32	Processor generated transaction ID
response_code	man.	an..5	Please see Appendix A for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
ptype	man.	ans..20	This is the payment channel that the customer has used for the transaction. Refer to Appendix B to know the list of payment channels.
rebill_id	opt.	an..50	This is the token to be used in rebilling and subscription
token_id	con.	an..32	This token represents the card info from the initial sale transaction. <MetaData> <SubItem> <item>token_id</item> <value></value> </SubItem> </MetaData>
token_info	con.	an..20	This is the card type and last 4 digits of the card that was used that is associated with the token_id. This data will only be returned if a token_id is generated. <MetaData> <SubItem> <item>token_info</item> <value></value> </SubItem> </MetaData>

Element	Settings	Type	Description
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor. For Paynamics Over the counter payment method, this parameter will contain the reference token that the customer will need to make payment.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

NOTE: Please take note that in some payment methods, you may not have a response coming from Paygate. The reason is that the customer may have discontinued the payment process.

5.3 NOTIFICATION PROCESS

Since Paygate is integrated with multiple payment methods. There can be an instance in which the payment method does not return a real time response. This normally applies to payment methods that require customer to do a cash-in to a designated payment center or an over the counter bank deposit. If the customer has fulfilled the payment instruction, Paynamics will receive an updated status of the transaction. Once this happens, Paygate will notify the merchant by sending a post to the notification url that was sent by the merchant in this format: (xml format). Please see below:

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent with the original transaction.
response_id	man.	ans..32	Processor generated transaction ID
response_code	man.	an..5	Please see Appendix A for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
ptype	man.	ans..20	This is the payment channel that the customer has used for the transaction. Refer to Appendix B to know the list of payment channels.
rebill_id	opt.	an..50	This is the token to be used in rebilling and subscription

Element	Settings	Type	Description
token_id	con.	an..32	This token represents the card info from the initial sale transaction.
token_info	con.	an..20	This is the card type and last 4 digits of the card that was used that is associated with the token_id. This data will only be returned if a token_id is generated.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor. For Paynamics Over the counter payment method, this parameter will contain the reference token that the customer will need to make payment.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

Paygate will only send the notification once. But notification process can be configured to send a notification again up to 4 re-attempts (5 minute interval). If we didn't receive a correct response from the Merchant's end. In case the merchant did not receive the notification, it is recommended that the merchant would integrate the query function to know the final status of the transaction.

On very rare occasions, Paygate may send a reversal notification from a previous successful transaction. This is because the acquiring processor may have applied the bank transfer incorrectly or there was a reconciliation incident in which the payment was reversed. For disputes regarding these occurrences, you may contact your Paynamics Project Manager.

6. OTHER TRANSACTION TYPES

Merchants will also have the capability to do Refund, Settlement (settle authorized, settle pre-authorized) and Query to their transactions. To do this, merchant would need to initiate a direct server SOAP request to Paygate. Please take note that the production URL for this these transaction types are different from the Webpayment frontend production URL.

Before integrating this functions, kindly consult with your Paynamics Project manager for more information.

6.1 REFUND /REVERSAL

A **Reversal** of a monetary transaction (e.g. 'sale', 'settle authorization') is only allowed on the same calendar day as of the original request. Currently this is only applicable for credit card payment method only. The cut-off time for reversal is normally defined by the acquiring bank. Kindly contact your Paynamics project manager for the cut-off time.

The reversed transactions do not appear on the cardholder's card statement. A reversal of an authorization transaction (e.g. 'authorization', 'preauthorization') can be made up to 14 days following the original request.

Please contact Paynamics Technical Support for further information on the expiration period.

For a reversal request, a valid response id from a previous request is required. The amount defined in the 'reversal' request has to match the amount given in the respective request that needs to be cancelled.

Refund functionality will allow the merchant to design an application in their back office to process this transaction request. The refund functionality will only be enabled for the Credit card payment method for now.

For Paypal, you can process a refund through your Paypal Business account access.

For a **Refund** this would be allowed after the calendar day (or after the reversal period).
In the event that you wish to refund a customer, use the Refund request to credit the funds back to the payment method. In some cases, refund request are being batch for further action, in this case an initial return response would be responded back to the customer indicating this type of status. Depending on the acquiring bank/payment solution this may be possible for up to three months following the transaction.

For credit card processing, a Refund may have already been initiated by the card company as a result of a "chargeback" request from the cardholder. A chargeback is a refusal of the cardholder's bank to accept a transaction presented by the merchant's processor. This occurs when a customer disputes a card purchase. The merchant may be asked for proof of Authorization. The end result may be that the merchant's account is debited for the transaction. It is recommended that merchants check their chargeback records before processing a Refund transaction.

To post a refund request, a valid response_id from a former Sale transaction is required. For credit cards, if the initial transaction was an Authorization or a Pre-Authorization, the valid response id from the settlement authorized / settlement pre-authorized is required. Depending on the acquiring bank, it is

possible to refund an amount less than or equal to the initial transaction using the same currency as with the original transaction.

A refund is listed and will be posted separately on the cardholder's card statement.

6.1.1 REQUEST MESSAGE PARAMETERS (REFUND/REVERSAL)

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate
request_id	man.	ans..32	Unique transaction identifier that the merchant has sent.
org_trxid	man.	ans..32	This is the Paygate response id of the original credit card sale transaction only For credit card transaction that was processed as an authorization (cc_auth) or pre-authorization (cc_preauth), refund will only be possible if these transactions were process for settlement, in which case the org_trxid parameter should refer to the response_id of the settlement authorization or settlement pre-authorization. .
ip_address	man.	ans..20	This is the merchant's host i.p. address.
notification_url	con.	ans..255	This is the merchant URL where PAYGATE would send notification update for their transaction or its final status. The notification system can also send the final status of these transactions
response_url	opt.	ans..255	In case the transaction is asynchronous in nature (i.e. 3D Secure), this is the URL where Paygate will redirect the transaction.
amount	man.	F..2	Amount of the transaction with decimal point. For transactions in cents, kindly input the 2 decimal place after the point (i.e. for $0.50 = 0.50). Please take note that some international currencies would not accept transactions with decimal points (i.e. Japanese Yen)
signature	man.	an..200	Hash (SHA512) computations of string concatenation of request parameters of this transaction and merchant certificate (downloaded on the Merchant Backend).

6.1.2 GATEWAY RESPONSE (REFUND/REVERSAL)

After validating the connection, and transaction Paygate returns an xml response to the merchant's application.

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent with the original transaction.
response_id	man.	ans..32	Processor generated transaction ID
response_code	man.	an..5	Please see Appendix A for table element

Element	Settings	Type	Description
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

There can be some instances that the response code that is returned for refunds will indicate that the transaction is pending. This is because some acquiring bank process refunds on a batch basis. To know the final status of the refund you can check your Merchant Backend or do a Query.

6.2 SETTLE AUTHORIZED, SETTLE PRE-AUTHORIZED

A **Settle Authorized** allows you to settle a previous Authorization. After an order is shipped, the transaction can be settled, a procedure that is also handled by the card processor. The capture process completes the transaction: the issuing financial institution credits the merchant's bank account with the funds for the transaction and updates the cardholder's statement. Authorization and Settle Authorization are separate because it takes time to prepare goods for shipment. In contrast, a brick and mortar store gets the Authorization at the time of purchase, the customer receives the goods, and the merchant can submit the sale for Capture immediately.

For a Settlement Authorization request, a valid response id from a former Authorization request is required. The transaction amount which is to be captured must be identical to the amount.

A **Settle Pre-authorized** is similar to the Settle Authorization. For a Settle Pre-authorization request, a valid response id from a former Pre-authorization request is required. The amount settled may be less than the amount authorized. The amount remaining on the authorization is available for further captures as long as the authorization period does not expire. Please note that in some cases a pre-authorization can only be captured once. This is dependent of the acquirer policies.

An amount higher than the authorized may also be captured but there is no guarantee. It depends on the acquirer whether a greater amount may be captured and how much greater this can be. The recommended value is up to 5% of the original amount.

A capture of an authorization transaction (e.g. 'authorization', 'preauthorization', 'preauthorization supplement') can be made up to 7 days following the original request. In exceptional cases this period may be longer (depending on the acquirer and issuing bank).

Please check with your Paynamics Project Manager as to what type of transactions will be allowed with your merchant account.

6.2.1 REQUEST MESSAGE PARAMETERS (SETTLE AUTHORIZED, SETTLE PRE-AUTHORIZED)

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	Unique transaction identifier that the merchant has sent.
org_trxid	man.	ans..32	This is the Paygate response id of the original Authorization or Pre-Authorization transaction
ip_address	man.	ans..20	This is the merchant's host i.p. address.
amount	man.	F..2	Amount of the transaction with decimal point. For transactions in cents, kindly input the 2 decimal place after the point (i.e. for $0.50 = 0.50). Please take note that some international currencies would not accept transactions with decimal points (i.e. Japanese Yen).
notification_url	con.	ans..255	This is the merchant URL where PAYGATE would send notification update for their transaction or its final status. The notification system can also send the final status of these transactions
response_url	opt.	ans..255	In case the transaction is asynchronous in nature (i.e. 3D Secure), this is the URL where Paygate will redirect the transaction.
signature	man.	an..200	Hash (SHA512) computations of string concatenation of request parameters of this transaction and merchant certificate (downloaded on the Merchant Backend).

6.2.2 GATEWAY RESPONSE (SETTLE AUTHORIZED, SETTLE PRE-AUTHORIZED)

After validating the connection, and transaction Paygate returns an xml response to the merchant's application.

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent with the original transaction.
response_id	man.	ans..32	Processor generated transaction ID
response_code	man.	an..5	Please see Appendix A for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

6.3 QUERY

This functionality will allow the merchant to design an application in their back office to process this transaction request.

In a scenario where the merchant want to know the current status or the merchant have not received a response from Paygate, this transaction type can be used to query the status of a previously submitted transaction. The response that would be generated by the query will be the actual response string that the merchant have failed to receive.

The query function can also be used to know the final status of the transaction, in case you have received bank processor time-outs or pending requests (i.e. refund request, batch processing, and transaction in progress) as response.

6.3.1 REQUEST MESSAGE PARAMETERS (QUERY)

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	Unique transaction identifier that the merchant.
org_trxid	con.	ans..32	This is the response_id parameter of any previous transaction. (i.e. Sale, authorized, settle authorized, refund etc.). For normal query transactions, this value should be commonly used.
org_trxid2	con.	ans..32	This is the request_id parameter of any previous transaction. Merchant can use this parameter as another reference in case the response_id is unknown.
signature	man.	an..200	Hash (SHA512) computations of string concatenation of request parameters of this transaction and merchant certificate (downloaded on the Merchant Backend).

6.3.2 GATEWAY RESPONSE (QUERY)

After validating the connection, and transaction Paygate returns an xml response to the merchant's application.

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent in the query request.
response_id	man.	ans..32	Processor generated transaction ID of the query transaction.
response_code	man.	an..5	Please see Appendix A for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

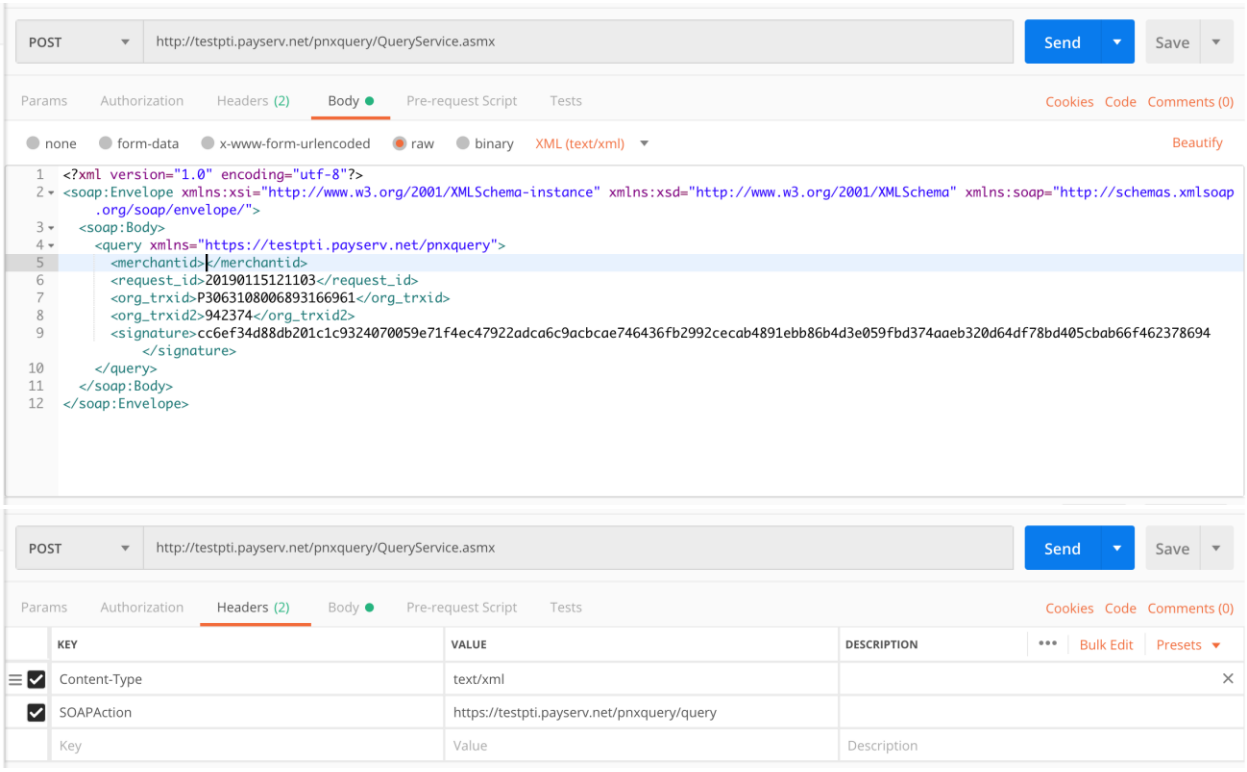
If the Query transaction is successful, it would include the updated transaction elements of the org_trxid / org_trxid2 parameter.

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent in the value of the org_trxid and org_trxid2 parameter.
response_id	man.	ans..32	Processor generated transaction ID of the org_trxid and org_trxid2 parameter.
response_code	man.	an..5	Please see Appendix A for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	YYYY-MM-DD-T-hh:mm:sszzzzzz	This is the completion time of the transaction.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

Note: There can be some instances that the transaction elements parameters response_code, response_message and timestamp would be different. Below are some sample instances:

- The initial response from Paygate was a “bank/processor timeout” and during the daily reconciliation, the bank/processor status updated the status to success.
- The initial response from Paygate was a “transaction pending” and on a later date, the transaction was updated to success. This can happen especially for refund transactions that are being handled by Paygate on a batch basis.

Sample Postman (Query):



Sample Request:

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <query xmlns="https://testpti.payserv.net/pnxquery">
      <merchantid>YOURMID</merchantid>
      <request_id>20190115121103</request_id>
      <org_trxid>P306310800689316696l</org_trxid>
      <org_trxid2>942374</org_trxid2>

<signature>cc6ef34d88db201c1c9324070059e71f4ec47922adca6c9acbcae746436fb2992cecab4891ebb8
6b4d3e059fbd374aaeb320d64df78bd405cbab66f462378694</signature>
    </query>
  </soap:Body>
</soap:Envelope>
```

Sample Response:

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

```
    <soap:Body>
        <queryResponse xmlns="https://testpti.payserv.net/pnxquery">
            <queryResult>
                <application>
                    <merchantid>YOURMID</merchantid>
                    <request_id>20190115121103</request_id>
                    <response_id>P212844200611514598 6</response_id>
                    <timestamp>2019-06-04T15:46:50.3501799+08:00</timestamp>

<signature>263226add78d9816eff937a2251c43dc97320cf6ab7b2fc7bb1edd93173d06a5e2dc746718b4e9
7a232f38a2b6397bd0547deaddbf83a296f700962820cfb2a8</signature>
                </application>
                <responseStatus>
                    <response_code>QM001</response_code>
                    <response_message>Query successful - test mode</response_message>
                    <response_advise>Query successful - test mode</response_advise>
                    <processor_response_id>2090004737</processor_response_id>
                    <processor_response_authcode>493575</processor_response_authcode>
                    <processor_response_code>0</processor_response_code>
                    <processor_response_mess>Approved</processor_response_mess>
                </responseStatus>
                <txns>
                    <ServiceResponse>
                        <application>
                            <merchantid>YOURMID</merchantid>
                            <request_id>942374</request_id>
                            <response_id>P30631080068931669 61</response_id>
                            <timestamp>2018-12-28T01:44:55</timestamp>
                            <ptype>CC</ptype>
                        </application>
                        <responseStatus>
                            <response_code>GR001</response_code>
                            <response_message>Transaction Successful</response_message>
                            <response_advise>Transaction is approved</response_advise>
                            <processor_response_id>2090004737</processor_response_id>

<processor_response_authcode>493575</processor_response_authcode>
                            <processor_response_code>0</processor_response_code>
                            <processor_response_mess>Approved</processor_response_mess>
                        </responseStatus>
                        <sub_data />
                        <secure3d />
                        <MetaData/>
                    </ServiceResponse>
                </txns>
                <disp />
            </queryResult>
        </queryResponse>
    </soap:Body>
</soap:Envelope>
```

6.4 DISPUTE QUERY

Dispute Query allows you to retrieve disputes coming from your merchant account. Below is a brief summary of this functionality:

- Paygate classifies dispute into different types depending on the payment method (Credit card, Chinese Debit Card, Bancnet, Gcash etc.) that was used.
- Paygate may provide the dispute reason. Depending on the payment method that was used, the dispute reason can be associated to the chargeback reason code (for Credit card payment methods) or other information.
- Paygate may provide information as to the effect of the dispute to your merchant account settlement reporting (i.e. Add, Subtract or No Effect).
- Paygate may provide as to when the dispute may take effect in the merchant account balance
- Paygate may provide if the status of the dispute, either it is new, pending or closed/resolved.

It is recommended that the merchant would use this functionality on a daily basis to know immediately the dispute request so that the merchant can take action in representing/resolving the dispute.

6.4.1 REQUEST MESSAGE PARAMETERS (DISPUTE QUERY)

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate
request_id	man.	ans..32	Unique transaction identifier that the merchant has sent.
ip_address	man.	ans..20	This is the merchant's host i.p. address.
notification_url	con.	ans..255	This is the merchant URL where PAYGATE would send notification update for their transaction or its final status. The notification system can also send the final status of these transactions
response_url	opt.	ans..255	In case the transaction is asynchronous in nature (i.e. 3D Secure), this is the URL where Paygate will redirect the transaction.
dispute_start_date	man.	YYYY-MM-DD-T-hh:mm:sszzzzzz	Beginning date of the disputes being queried. This date should not exceed the end date.
dispute_end_date	man.	YYYY-MM-DD-T-hh:mm:sszzzzzz	Ending date of the dispute being queried. This date should not be before the dispute starting date.
signature	man.	an..200	Hash (SHA512) computations of string concatenation of request parameters of this transaction and merchant certificate (downloaded on the Merchant Backend).

6.4.2 GATEWAY RESPONSE (DISPUTE QUERY)

After validating the connection, and transaction Paygate returns an xml response to the merchant's application.

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent with the original transaction.
response_id	man.	ans..32	Processor generated transaction ID
response_code	man.	an..5	Please see Appendix B for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man.	an..200	Hash (SHA512) computations of xml response message elements.

If the dispute query is successful, below will be the transaction elements.

Element	Settings	Type	Description
dispute_id	man.	an..14	Main identifier of the dispute transaction.
dispute_date	man.	YYYY-MM-DD-T-hh:mm:ssZzzzzz	Current date of when the dispute was created. For Credit cards, this is the date the dispute has been submitted to the acquiring bank (or known as the "impact date"). In some instances this date may come before the dispute_upload_date.
dispute_upload_date	man.	YYYY-MM-DD-T-hh:mm:ssZzzzzz +GMT	Date of when the dispute was retrieved by Paygate with the acquiring processor/bank. This will also be the basis of the start date and end date of the dispute query.
org_proc	man.	ans..32	Identifies as to which acquiring processor did the dispute originated. Kindly contact your Paynamics Project Manager to know the value to this parameter.
dispute_payment_method	man.	an..20	Identifies as to what payment method the dispute originated. Kindly refer to Appendix C for table element
org_request_id	man.	ans..32	The original merchant transaction identifier associated in the dispute ticket

Element	Settings	Type	Description
org_response_id	man.	ans..32	The original Paygate transaction identifier associated in the dispute ticket.
org_name	man.	an..256	This is the first name and last name that was sent by the merchant on the original requested sale or settled transaction.
dispute_type	man.	a..10	Identifies what is the dispute type. Kindly refer to Appendix C for table element.
dispute_amount	man.	F..2	Amount that was disputed. In some instances the dispute amount may be lower or larger the original transaction amount.
dispute_currency	man.	a..3	The three (3) character ISO 4217 currency code used for the transaction.
dispute_reason	opt.	ans..256	Reason for the dispute.
dispute_other_reason	opt.	ans..256	Other reason for the dispute.
dispute_action	opt.	a..20	This value indicates if the dispute amount would either ADD, DEDUCT or NO EFFECT on the merchant settlement.
dispute_effectivity_date	opt.	YYYY-MM-DD-T-hh:mm:sszzzzzz	Identifies the date of when the dispute action would be applied
dispute_status	opt.	a..20	Identifies the status of the dispute. The value can either be NEW, PENDING, or CLOSED.
dispute_further_details	opt.	ans..256	This field provides additional information about the dispute. The value will also depend on what payment method the dispute has originated. (i.e. For dispute related to credit card, the masked credit card number is provided in this parameter).

Please take note that the dispute items that will be part of the response will be up to 200 items at any given time period. It is suggested that if the merchant would like to query dispute items above this limit, the merchant should either adjust the start date or end date of the dispute query or they can view/download the dispute items in their merchant back office access.

6.5 REBILL

Merchants that have their own rebilling system can use Rebill Token transaction type to perform succeeding rebilling of their future clients. Merchant must use the Paygate response id from an original successful sale and the token_id to initiate this rebill transaction.

In addition, rebill also allows you to perform authorization / pre-authorization transaction by inputting a response id from an original successful authorization or pre-authorization. To perform settlement, please refer to item 6.2 .

Kindly contact your Paynamics Project Manager if this transaction type can be enabled in your merchant account.

6.5.1 REQUEST MESSAGE PARAMETERS (REBILL)

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	Unique transaction identifier that the merchant has sent.
ip_address	man.	ans..20	This is the merchant's host i.p. address.
org_trxid	man.	ans..32	This is the Paygate response id of the original Sale, Authorization or Pre authorization transaction
token_id	con.	an..32	This token represents the card info from the initial sale transaction. Kindly fill up this parameter if provided from the initial transaction.
trx_type	man.	a..10	This parameter allows the merchant to set what transaction will the rebill be routed. The allowable values are the following: • sale • authorized (for Authorization) • preauthorized (for Pre-authorization) Please take note that if the merchant has performed authorized/preauthorized, kindly perform a settlement to capture the transaction.
amount	man.	F..2	Amount of the transaction with decimal point. For transactions in cents, kindly input the 2 decimal place after the point (i.e. for $0.50 = 0.50). Please take note that some international currencies would not accept transactions with decimal points (i.e. Japanese Yen).
notification_url	con.	ans..255	This is the merchant URL where PAYGATE would send notification update for their transaction or its final status. The notification system can also send the final status of these transactions
response_url	opt.	ans..255	In case the transaction is asynchronous in nature (i.e. 3D Secure), this is the URL where Paygate will redirect the transaction.
signature	man.	an..200	Hash (SHA512) computations of string concatenation of request parameters of this transaction and merchant certificate (downloaded on the Merchant Backend).

6.5.2 GATEWAY RESPONSE (REBILL)

After validating the connection, and transaction Paygate returns an xml response to the merchant's application.

Element	Settings	Type	Description
merchantid	man.	an..32	The merchant identifier with Paygate.
request_id	man.	ans..32	The original merchant transaction identifier sent with the original transaction.
response_id	man.	ans..32	Processor generated transaction ID
response_code	man.	an..5	Please see Appendix B for table element
response_message	man.	an..100	Corresponding response message of the response code
response_advise	opt.	an..150	In some cases, Paygate would advise the merchant what to do in case a given response code is received.
timestamp	man.	yyyy-MM-ddTHH:mm:ss.ffffffZ	This is the completion time of the transaction.
processor_response_id	opt.	ans..60	This is the response id generated by the acquiring processor.
processor_response_authcode	opt.	an..6	This is the authorization code generated by the issuing bank of the cardholder. This value is applied for successful credit card transactions.
signature	man	an..200	Hash (SHA512) computations of xml response message elements.

APPENDIX A: RESPONSE CODES

The response code/response message is returned by Paygate and is classified into 3 categories

- **Format Message Response Codes (FR):** These response codes are related to format errors of the parameters you are passing to Paygate. You would receive this if the parameters you are passing will not comply with the proper messaging format of Paygate. The format message response codes can both be seen on the test production and production environment.
- **General Message Response Codes (GR)** – These return codes are generally transaction related. Once your merchant account is live, GR response codes will be the one mostly responded by Paygate to your system.
- **Risk Management Response Codes (RM)** – These response codes are related to the Fraud Validation system of Paygate. If the Fraud Validation System is enabled in your merchant account, kindly refer to this table.
- **Query Message Response Codes (QM)** – These response codes are related to the Query Validation. This is applicable for Query and Query Subscription API calls only.

The following table contains all of Paygate response codes and descriptions that might be returned while sending transaction requests.

Format Message Response Codes

Response Code	Response Message	Meaning
FR001	Check Request_id format (an / Length < 32)	Request id is not in alpha numeric characters or the Length < 32
FR002	Check Amount format (n / Length < 5.2)	Amount is not in numeric characters or the Length is incorrect
FR003	Check First name format (a / Length < 30)	First name is not in alpha characters or the Length < 30
FR004	Check Last name format (a / Length < 32)	Last name is not in alpha characters or the Length < 32
FR005	Check Addr 1 format (ans / Length < 100)	Addr 1 is not alpha numeric special characters or the Length < 100
FR006	Check Addr 2 format (ans/ Length < 100)	Addr 2 is not in alpha numeric special characters or the Length < 100
FR007	Check State format (a/ Length < 30)	State is not alpha characters or the Length < 30
FR008	Check City format (a/ Length < 30)	City is not alpha characters or the Length < 30
FR009	Check ZipCode format (an / Length < 12)	ZipCode is not alpha numeric characters or the Length < 12
FR010	Check I.P. Address format (ans/ Length < 20)	Ip address is not in alpha numeric special characters or the Length < 20
FR011	Check Exp month format (n / Length < 2)	Expiry month is not numeric characters or the Length < 2
FR012	Check Exp Year format (n / Length < 4)	Expiry Year is not numeric characters or the Length < 4
FR013	Invalid Phone format	Phone Format is invalid. Format should be country code (area code) phone number. Sample: 1(240) 652-5009
FR014	Check Date and Time Format	Date and Time format is incorrect. Format should be YYYY-MM-DD HH:MM:SS:000. Sample: 2010-03-23 18:06:44.493
FR015	Check email format	Email Format is incorrect. This should be character@character.character
FR016	Check notification url format	URL format is not valid. Format should be http://domain.com or https://domain.com
FR017	Invalid Card Number	Card Number is invalid. For Visa, Mastercard, JCB, card number should be 16 digits. AMEX should be in 15 digits.
FR018	Invalid Luhn Check Sum	Card number submitted did not pass the Luhn formula
FR019	Check Card Type	This means the card type is not valid for this Merchant ID/Merchant Account.

Response Code	Response Message	Meaning
FR020	Check Client_id format	This means that the Client_id format is not valid
FR021	Check Client_token format	This means that the Client_token format is not valid
FR022	Invalid Rebill Period	The rebill period that was sent is not defined in the Paygate System.
FR023	ABA is X and length of account number is not Y	The ABA and Account number being placed has a format error.
FR024	ABA is X and account number does not start with Y	The ABA and Account number being placed has a format error at the beginning.
FR025	Account number length < 17	The Account number length should not be greater than 17 characters.
FR026	Account number contains invalid numerals.	Account number contains invalid numeras (i.e. 123456)
FR027	Fractional Length is not Correct	Parameter that was passed on the Fractional length was not valid.
FR028	Invalid ABA number	ABA number provided was invalid.
FR029	Invalid Fractional	Invalid Fractional
FR030	Missing Fields – ACH	Request contains missing fields (I.e. processtype, parent_id, mersubid, accttype, consumername, accountname, host_ip, or client_ip, etc)
FR031	Check Country Parameter	This means that the country parameter is required to be passed in order for the transaction to proceed.
FR032	Invalid Request Fields Format.	Request contains invalid field or value(i.e request_id, accountnumber, fname, lname, city, address1, etc). The root cause could also be related to format restriction from acquiring processor or host.
FR033	Transaction request contain invalid parameter values.	This means that transaction request sent contain values that did not follow certain logic conditions. Please contact Paynamics Technical support to investigate further.
FR034	Notification payload incorrect format or data objects non existent.	This means the formatting of values in the notification order payload is incorrect or data objects being used does not exist or was not passed by merchant.
FR035	Parameter value too long	he length of the value for parameter is longer than the maximum limit. Refer to response advise for details.
FR036	Invalid Request Format	The request you are submitting has an invalid format. Please refer to API documentation for proper request format.
FR037	Invalid Request Id	The response code submitted to update transaction is not existing on request id list.
FR038	Invalid Expiry Limit	Expiry limit has an invalid value. Possible reason is invalid date or date provided already passed.
FR039	Reference Number Already Exist	The reference number you have provided already exist on our records. Please provide a unique reference number and try again.
FR040	No Reference Number Provided	The merchant linked to this transaction requires to provide its own reference number but no values was given to the request. Please provide a unique reference number and try again.
FR041	Check Mobile format (an / Length < 32)	Mobile is not in alpha numeric characters or the Length < 32
FR042	Check ClientIp format (an / Length < 40)	Client IP is not in alpha numeric characters or the Length < 40
FR043	Check 3D Secure format (an / Length < 10)	3D Secure Policy is not in alpha numeric characters or the Length < 20
FR044	Check Original Request Id format (an / Length > 32)	Original Request Id is not in alpha numeric characters or the Length < 32
FR045	Check ClientId format (an / Length < 32)	Client Id is not in alpha numeric characters or the Length < 32
FR046	No Idempotency Key Found	Please provide Idempotency-Key value on request header.
FR047	Invalid Idempotency Key	It is required that Idempotency key is equal to Request ID.
FR048	Check Original Gateway Id format (an / Length < 32)	Original Gateway Id is not in alpha numeric characters or the Length < 32
FR049	Check responseUrl format	URL format is not valid. Format should contain http:// or https:// at the beginning of the address.

General Message Response Codes

Response Code	Response Message	Meaning
GR001	Transaction Successful	Transaction is approved
GR002	Transaction Successful with 3DS	This means that the transaction was successful and is protected with 3D Secure.
GR003	Transaction Failed	Transaction has failed.
GR004	Invalid Card Number against Card type	The Card number that was provided doesn't match the appropriate Card type
GR005	Expired Card	Card that was provided is already expired.
GR006	CVC is incorrect.	The CVC code (3 digits for Visa, Mastercard JCB or 4 digits for AMEX) provided is incorrect.
GR007	MID incorrect or not found	Merchant ID that was provided is incorrect or unregistered.
GR008	Currency not allowed.	Currency that was provided is not allowed with the Merchant id or the currency that was used is not allowed by the payment method.
GR009	Transaction type not allowed	Transaction Type is not available for the Merchant ID or the Transaction type is invalid.
GR010	Invalid Country Code	Country code that was provided is unknown or is incorrect ISO format.
GR011	Request_id already processed	The request id that was sent is not unique or is already processed.
GR012	Bank / Network Host not reachable	The Bank Processor is not available or there is a connectivity problem.
GR013	Bank / Processor Timeout	The Bank Processor did not respond back to the system.
GR014	Request Message String Incomplete	The request string provided is not valid or has an incomplete parameter.
GR015	Original Trx ID missing or invalid	Original Trx ID is required or the Original Trx ID that was provided was not found. This can happen with a query transaction in which the merchant request might not have reached Paygate.
GR016	Refund Period Expired	The transaction being refunded has already exceeded the Refund period. Standard Refund period is 3 months unless otherwise specified by Bank processor.
GR017	Refund allotment exceeded	Refund transaction not allowed. The refund request would exceed the 80 percent weekly sales volume allotment.
GR018	Refund Transaction already processed	This means that the transaction (sale or settled transaction) was already refunded
GR019	Refund Amount exceed original transaction	This means the refund amount being requested is greater than the original sale or settled transaction
GR020	3D Secure Enrollment Successful	The transaction has been successfully enrolled for 3D Secure.
GR021	3D Secure Enrollment Failed	The transaction has not been successfully enrolled for 3D Secure.
GR022	Reference amount not valid	The Transaction amount of the referencing transaction is higher or lower than the transaction amount of the original transaction. This response code is applicable for Authorization and Settle Authorization.
GR023	PIN / PAN Incorrect	PIN/PAN Provided is incorrect (applicable for ATM or Click2pay Transactions).
GR024	Subscription Billing Successful	The Subscription Billing was successfully enrolled or was successfully updated.
GR025	Subscription Billing Declined	This means that the subscription billing enrollment was declined. This can be due to the following factors: Transaction failed, card number was blacklisted, Card holder was blacklisted, check sum final date logic did not passed, the rebill start date was before the date of creation of the subscription etc.
GR026	Subscription Billing Cancellation Successful	This means that the request to cancel a subscription billing was successful.
GR027	Invalid original subscription id.	The rebill id that was provided is invalid or does not exist.

Response Code	Response Message	Meaning
GR028	Subscription cancelled by merchant	This response is explains the status of the Subscription being queried. The subscription was cancelled by the merchant.
GR029	Subscription cancelled due to failed attempts	This response is explains the status of the Subscription being queried. This response is specific to "query subscription" transaction. The subscription was automatically cancelled by Paygate since the transaction failed (i.e. due to card blacklisting, due to unsuccessful sale transaction)
GR030	Subscription active.	This response is explains the status of the Subscription being queried. The Subscription is active. This response is specific to the "query subscription" transaction.
GR031	Key Invalid	The Merchant Key or certificate is already invalid. Please contact Paynamics Technical Support for updated information.
GR032	Merchant Processing Suspended	Merchant ID is temporarily suspended.
GR033	Transaction Pending	The transaction is on pending status. This is either because the transaction is being batched by the acquiring bank or the transaction requires the customer to perform a manual payment fulfillment (i.e. deposit over the counter to a bank account or perform a cash-in to a designated payment center). This can also be applicable to refund transaction being requested. It is advisable to do a query for this transaction to know the final result status.
GR034	Card Stolen	It means that the card number being processed was reported stolen.
GR035	Merchant Host I.P. not registered or not matching	This means the merchant's host i.p. address is not registered in the Paygate system or the validation of the merchant i.p. address does not match from the transaction parameters that was passed.
GR036	Signature Verification failed	The signature provided by the merchant is invalid or was not parsed successfully by Paygate.
GR037	Batch Processing on going	This means Paygate might be conducting its batch or settlement processes, please try sending a transaction later.
GR038	Transaction Failed	This response code is reserve for other non –credit card transactions (i.e. e-wallets, Debit cards) in which the response code mapping can be specific to Paygate's connecting processor.
GR039	Transaction Failed due to Insufficient funds	This means the card that was used has insufficient funds.
GR040	Card not protected with 3D secure	This means that the card enrollment has failed and the transaction is not eligible for 3D secure
GR041	3D Secure service not available	3d Secure service in not available at the moment.
GR042	3D Secure error	Unhandled error related to 3d secure
GR043	Acquiring Processor related error	Acquiring bank specific error. (i.e. bank downtime or other incidents)
GR044	Card Issuer not reachable at the moment	There is a network connectivity problem to the card issuer
GR045	Pick up card	Card was reported pick-up.
GR046	Lost card	Card was reported lost
GR047	Restricted Card	Card is restricted to be used online
GR048	Retained Card	Card can only be used domestic
GR049	Card Issuer Declined	Card was declined by card issuer. You can contact Issuing Bank.
GR050	Insufficient Authorization Time period	Settle authorization not allowed due to insufficient time period.
GR051	Allowable Authorization period elapsed	Transaction failed because authorization period is expired by acquiring bank.
GR052	System Error	This means there is an undefined/unhandled system error.
GR053	Transaction cancelled by user	The transaction was cancelled by the user.

Response Code	Response Message	Meaning
GR054	No response received from processor	A null value was returned.
GR055	Payment type not allowed	This means the payment type that was submitted was not allowed under the current merchant configuration.
GR056	Transaction Failed Securecode Process Filtered	This means that the securecode process is being filtered by Paygate.
GR057	Transaction Failed Merchant Not Active	This means the merchant account was updated to non-active status. Please contact your Paynamics Account manager for more information.
GR058	Unable to refund from failed transaction.	This means that the transaction being refunded came from failed transaction. Please enter a successful org_trxid.
GR059	Refund transaction is already in queue.	Duplicate refund request was received by the Paygate.
GR060	Subscription billing already cancelled	This means that the request to cancel a subscription billing has been previously cancelled.
GR061	Subscription billing updated	The subscription billing was successfully updated.
GR062	Refund not possible at the moment	Refund not allowed due to bank settlement process
GR063	Transaction in progress	The transaction is currently in progress. This return code can happen for solutions that are asynchronous in nature (which means the user is redirected to another URL for further authorization of transaction).
GR064	Transaction Query Successful	This means that the subscription query process was successful.
GR065	Partial Refund not enabled	Please set refund amount equal to the original transaction amount.
GR066	Transaction Declined Paypal Express Checkout Error	Please refer for Paypal API
GR067	Transaction Declined Paypal General Error	Please refer for Paypal API
GR068	Transaction Declined Paypal Validation Error	Please refer for Paypal API
GR069	Incomplete Transaction Parameter	There Is/Are Missing Transaction Parameter
GR070	Gcash Transaction Failed. Black Listed Wallet/Non Globe or TM Number	Sorry, we have encountered an error in your transaction. Your GCASH wallet is invalid. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR071	Gcash Transaction Failed. Insufficient Balance	Sorry, we have encountered an error in your transaction. Please fund your GCASH account by visiting the nearest GCASH outlet or through BPI Mobile Banking. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR072	Gcash Transaction Failed. Expired Wallet	Sorry, we have encountered an error in your transaction. Your GCASH wallet is invalid. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR073	Gcash Transaction Failed. Insufficient Balance	Sorry, we have encountered an error in your transaction. Please fund your GCASH account by visiting the nearest GCASH outlet or through BPI Mobile Banking. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR074	Gcash Transaction Failed. Did not respond with the MPIN within allowable period	Sorry, we have encountered an error in your transaction. Please check your phone and reply with your MPIN within the allowable period. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR075	Gcash Transaction Failed. Did not respond with the MPIN within allowable period	Sorry, we have encountered an error in your transaction. Please check your phone and reply with your MPIN within the allowable period. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR076	Gcash Transaction Failed. Unregistered Wallet	Sorry, we have encountered an error in your transaction. Please register your Globe or TM mobile number to GCASH and try again. For assistance, you may call our Customer Service Hotline 2882 for FREE. Thank you!
GR077	No Dispute Items Available	The dispute item being queried on the time period specified did not produce any result.

Response Code	Response Message	Meaning
GR078	Transaction Declined Dispute Date Error	This means that the dispute start date or dispute end date that was sent to the request was not valid entry.
GR079	Transaction Declined Dispute Data being Queried Exceeded	This means that the dispute items being queried will exceed the maximum number of disputes allowed in the response. Kindly adjust dispute start date and end date to fit
GR080	Transaction failed. Amount limit exceeded for OCT.	This means that the amount being submitted by merchant for Original Credit Transfer (OCT) is exceeding the limit set by Paygate or the Acquiring Processor.
GR081	Transaction failed. Transaction amount exceeded Transaction limit for OCT.	This means that the total transaction amount has already exceeded the acquiring processor's policy for OCT transactions.
GR082	Transaction failed. Invalid card for OCT Transaction.	This means that the card number that was used for the OCT transaction was not yet used from a previously successful transaction.
GR083	Transaction failed. OCT not supported.	This means that the merchant is not allowed to submit OCT transactions.
GR084	Transaction failed. OCT not supported for this card.	This means that the card number does not support OCT.
GR085	Transaction failed. Transaction daily count limit exceeded for OCT.	This means that the transaction count submitted by the merchant for OCT had exceeded the daily limit set by Paygate or the Acquiring Processor.
GR086	Transaction Failed. Client_id already exists.	This means that the value in the Client_id being submitted in the Create Token transaction is not unique.
GR087	Transaction Failed. Client_token provided already exists.	This means that the value in the Client_token being submitted by the merchant in the Create/Add Token transaction is not unique.
GR088	Transaction Failed. Client_id or Client_token does not exist.	This means that the value in the Client_id or Client_token being submitted by the merchant in the Transact/Delete Token transaction does not exist or invalid.
GR089	Transaction Failed. Card Number being used for tokenization already exist in the specific Client_id.	This means that the Card Number being submitted for tokenization is already existing for that client_id. For update purpose (i.e. the merchant wants to submit the same Card Number but with a different expiry date) the merchant should delete previous token associated with the Card Number.
GR090	Transaction Failed. Transaction amount exceeds the Vcard amount.	This means that the amount being transacted exceeds the Vcard amount value. Transaction Amount and Vcard amount should be exact.
GR091	Transaction Reversed.	This means that the transaction was reversed by the acquiring processor.
GR092	Transaction Time Out.	This means that the transaction has timed out.
GR093	Refund Failed. Cannot Refund a previously reversed transaction.	This means the transaction being refunded has already been reversed.
GR094	Transaction Failed. Please contact customer's issuing bank.	This means the issuing bank declined the transaction. Merchant may advise its cardholder to contact their issuing bank for further verification and authorization.
GR095	Authorization Approved but Settlement Failed.	This means that the customer's credit was not charged due to settlement failure.
GR096	Rebill Transaction Failed due to Invalid Payment Method.	This means that the org_trxid being submitted in the Rebill transaction came from an unsupported payment method (i.e. Paypal, Gcash, Bancnet, etc
GR097	Transaction Failed. Unique Key Violation.	This is an exception handling error by Paygate in which the response_id value being stored is not unique. This is due to the fact that the Paygate response_id being used was already used/tagged from a previously marked transaction.
GR098	Refund Failed due to Chargeback Transaction.	This means that the transaction being refunded has already been applied as chargeback by the Acquiring Bank.
GR099	3D Secure Checking Failed for this Card Issuing Bank, Kindly use another Credit Card.	This means the customer's issuing bank returned an "Unavailabe" or "Error" response during the 3Dsecure enrollment checking process. We further advise that the customer to use another credit card.
GR100	3D Secure Attempted Authentication.	This means that the customer's credit card is enrolled for 3Dsecure however the issuing bank return an "Attempted Authentication". Merchant may perform Transaction Submission.

Response Code	Response Message	Meaning
GR101	Transaction Check Return.	This means that the RDFI (consumer's bank) has returned the item prior to the specified time period defining a Check Settlement (Settled Funds) indicated in the Actum Processing Service Agreement.
GR102	Transaction Check Late Return.	This means that a Return was received by Actum Processing after a Check Settlement.
GR103	Duplicate Check indicates that this transaction was previously declined (but not why)	Duplicate Check indicates that this transaction was previously declined (but not why)
GR104	Invalid merchant credentials	Merchant credential provided are invalid (ACH Processor)
GR105	Invalid billing profile	Invalid billing profile
GR106	Invalid cross sale ID	Invalid cross sale ID
GR107	Invalid Consumer Unique	Invalid Consumer Unique
GR108	Transaction Verify	This Transaction is marked by ACH Processor for further verification. Kindly call client.
GR109	Transaction Failed, Exceeds Amount Limit	The transaction limit of the card has already exceeded and was decline by their Issuing Bank.
GR110	Transaction Failed, Excessive PIN attempt	Transaction Failed due to excessive PIN retries.
GR111	Transaction Failed, Account Not Found	This means the merchant has provided an account number that cannot be found by the Issuing Bank.
GR112	Transaction Failed, Session Time Out	This means the browser session has already time out.
GR113	Invalid Current Account	Bancnet related error. Current Account is invalid.
GR114	Invalid Savings Account	Bancnet related error. Savings Account is invalid.
GR115	Card Record Invalid or Not Found	Bancnet related error. Card record specified is invalid or not found.
GR116	Duplicate transaction found	Acquiring processor rejected the transaction due to a duplicate entry.
GR117	Transaction Failed, Browser Closed	
GR118	Transaction Failed. Request is already in queue.	
GR119	Transaction Successful but not yet verified.	This means that the transaction is successful but not yet verified by the processor
GR120	Transaction Failed. Client Token not yet verified.	This means that the client_token being submitted is valid but needs verification. Client should verify card first before it can be used for transacting.
GR121	Transaction verified, awaiting payment.	Transaction verified, awaiting final status. This is for Paynamics Over the Counter.
GR122	Transaction Not Found	Transaction does not exist.
GR123	Incomplete Transaction.	Transactions is Incomplete.
GR124	Transaction did not reach processor.	Transaction did not reach processor.
GR125	Enrollment Failed, Bank Account does not exist.	This means Auto Debit Arrangement account enrollment failed due to the bank account already tagged does not exist.
GR126	Enrollment Failed, Bank Account dormant.	This means Auto Debit Arrangement account enrollment failed due to the bank account already tagged is dormant.
GR127	Enrollment Failed, Bank Name invalid or not found.	This means the bank being enrolled is not valid or not yet enabled.
GR128	Enrollment Failed, Bank Account Currency disclosed did not match Bank Account Profile.	This means Auto Debit Arrangement account enrollment failed due to the bank account currency did not match the actual currency.
GR129	Enrollment Failed, Bank Account Name and Bank Account number did not match.	This means Auto Debit Arrangement account enrollment failed due to the bank account name and bank account number did not match.
GR130	Enrollment Failed, Bank Account Type did not match.	This means Auto Debit Arrangement account enrollment failed due to the bank account type did not match the actual account type.
GR131	Enrollment Failed, Bank did not approved enrollment.	It means bank did not approve the enrollment process. This can be due to lacking of documents, kyc or any other reason.

Response Code	Response Message	Meaning
GR132	Transaction Failed, PayExpress ID is lock, invalid or does not exist.	It means the PayExpress ID provided by the merchant was tagged as lock, invalid, or does not exist.
GR133	Transaction Awaiting Approval	It means the transaction is awaiting approval from the customer.
GR134	Transaction Failed, ada_token invalid or does not exist.	It means the ada_token provided by the merchant was tagged is invalid, or does not exist.
GR135	Transaction Failed, PayExpress ID and ada_token does not match.	It means the PayExpress ID and ada_token provided by the merchant did not match.
GR136	Transaction Failed, AuthPay allowed time period expired.	This means the AuthPay Transaction has already expired and the payor did not put his approval. Please try again.
GR137	AuthPay Failed due to incorrect authentication.	This means the AuthPay Transaction has failed due the incorrect authentication info provided by the payor.
GR138	AuthPay Failed due to payor decline due to _____.	This means the AuthPay Transaction was declined by payor. Kindly contact payor directly.
GR139	AuthPay or DirectPay failed due to Bank specific deciline.	This means the ADA AuthPay or DirectPay failed due to Bank Rejection. This is an aggregated response in case Bank has not provided Paynamics a specific reason for the decline.
GR140	Transaction failed, ADA Recurring Payment was cancelled by Paygate due to excessive payment reattempts.	This means ADA Recurring payment was cancelled automatically by Paygate since it has exceeded more than 3 failed attempts.
GR141	Cancellation Failed, ADA Recurring Payment is already tagged as cancelled as per Customer request due to _____.	This means ADA Recurring payment was cancelled or discontinued by the user.
GR142	Cancellation Failed, Recurring Payment has already been cancelled or was already marked as fullfilled by Paygate.	This means the recurring payment was already cancelled or was tagged as fullfilled by Paygate.
GR143	Cancellation Failed due to invalid recurring_id.	Recurring_ID specified by merchant was invalid.
GR144	Transaction Failed, Client ID / Client Token not related to previous original request id or not found.	This means the call back token api resulted to a failure. Either the client id/client token does not relate to the previous original request id, or the Paygate did not receive this request at all.
GR145	Transaction Failed, Workflow API cannot be cancelled.	This means the Workflow Cancel API has failed, due to restrictions.
GR146	Transaction Failed, Deposit amount and Transaction amount did not match.	Transaction failed due to missing mandatory parameters.
GR147	Over the Counter Payment not completed by customer.	This means the customer have clicked on the OTC (Bank or non bank) payment channel but has failed to make the actual payment on the allowable time.
GR148	Bank Allowable authorization period elapsed.	Authorization period is expired.
GR149	Invalid Payment Method	Please make sure that the correct pmethod value is supplied
GR150	Payment Method Not Allowed	The payment method you are requesting is not allowed. Kindly contact your Paynamics Project Manager for more information.
GR151	Payment Channel Not Found	The payment channel that you have specified does not exist. Refer to response advise for details
GR152	Transaction Expired	Cannot process transaction (OTC) because it was expired prior to payment. Refer to response advise for details.
GR153	Invalid Authentication	The authentication token doesn't match any of our authorized merchants, payment channels, or integrators. Please check if your username and password is correct
GR154	Payment Reference Not Found	Payment reference is not existing in any pending transactions.
GR155	Invalid Response Code	The response code submitted to update transaction is not existing on standard response code list.
GR156	Invalid Update Action	The transaction must be validated before status update.
GR157	Transaction failed. Transaction amount exceeded Transaction limit for Over The Counter.	This means that the total transaction amount has already exceeded the acquiring processor's policy for OTC transactions.
GR158	Transaction Cancelled by Merchant	This means that the transaction is cancelled by merchant

Response Code	Response Message	Meaning
GR159	Transaction Paid from other Channel	You cannot process this transaction because it's already paid on another payment channel.
GR160	Acknowledgement Received	Your acknowledgement has been received by our server.
GR161	Acknowledgement Rejected	Sending acknowledgement is not allowed when the transaction is not yet paid; or the payment channel sending acknowledgement is not the one who accepted the payment.
GR162	Subscriber Upload Success	All subscribers specified in request was uploaded successfully to recurring payments list.
GR163	Subscriber Upload Failed	Subscriber(s) specified in the request failed to upload.
GR164	Some Subscribers Did not upload	From the submitted csv file, there are records that did not save to recurring payments list. Possible reason is the reference number already exist or the record contains an invalid data.
GR165	Transaction Failed. Micro charge amount did not match.	Transaction Failed. Micro charge amount did not match.
GR166	Unsubscribe Success	Subscriber(s) specified in the request successfully to deactivated.
GR167	Unsubscribe Failed	Subscriber(s) specified in the request failed to deactivated.
GR168	Transaction Failed. Micro charge amount did not match.	This means the Micro charge amount that was submitted on the verify token process was did not match the original debited amount.
GR169	Installment payment quote provided	This means Paynamics has provided the merchant installment payment quote.
GR170	Installment reversal or refund failed due to previous action.	This means that the Installment payment being reversed, refunded or adjusted has already been tagged.
GR171	Installment reversal / refund not allowed due to lapsed period.	This means: (1) Installment payment cannot be reversed since the 24 hour allowable period has lapsed. (2) Installment payment cannot be refunded / adjusted since the 30 day allowable period has lapsed.
GR172	Transaction Failed; Policy ID invalid or not found.	This means the policy id that was sent is invalid or not found in Paynamics System.
GR173	Transaction Failed due to discontinued process.	This means that Transaction failed because the merchant did not proceed to the next process. For example, non execution of 3Dsecure URL returned during payment flow.
GR174	Transaction Failed, Customer not allowed to make payment in the payment channel.	This means the customer attempted to make a deposit to a payment channel that is not assigned to their payment reference.
GR175	Transaction Failed. Invalid Expiry Date.	This means that the expiry date being passed by the merchant failed to meet Paynamics Over-the-Counter minimum/maximum expiry limit.
GR176	Transaction has been locked out due to a previous success transaction. Please try again.	Transaction being submitted has already a previous approval. This is to avoid system abuse. If this is a unique separate transaction from the previous approval, kindly try again after 10 minutes.
GR177	Transaction failed. 3dsecure URL not redirected or opened.	This means the transaction is tagged as failed, and the 3dsecure url that was sent to the merchant was not redirected or opened for the user.
GR178	This means the transaction is tagged as failed, and the 3dsecure url that was sent to the merchant was not redirected or opened for the user.	Paynamics cannot complete the Query or Query Token API call at this moment due to incompleted process. Kindly retry the transaction again to get the actual final status.
GR179	Transaction failed. Signature object not valid or mismatch.	This means Paynamics detected a signature mismatch between 2 or more application process. Kindly contact Paynamics Tech Team for more information.
GR180	Subscription Billing Cancellation Success	This means that the request to cancel a subscription billing was successful.
GR181	Transaction Failed due to incorrect page load.	This means the payment page that was rendered was incorrect for the given session. Kindly try again.

Risk Management Response Codes

Response Code	Response Message	Meaning
RM001	I.P. address restricted	The Client I.P. Address was blacklisted. Transaction is filtered.
RM002	BIN restricted	The Issuing Bank name or BIN number that was provided was restricted. Transaction is filtered.
RM003	I.P Country restricted	The Client's I.P. country was blacklisted. Transaction is filtered.
RM004	BIN country restricted	The Issuing Bank Country was blacklisted. Transaction is filtered.
RM005	Card number or Cardholder restricted	The Card number or Cardholder name that was provided was blacklisted. Transaction is filtered.
RM006	I.P. Country and Customer Country mismatch	The Client's I.P. country and the Customer's country do not match. Transaction is filtered.
RM007	Anonymous Proxy I.P. restricted.	The Client's I.P. address was identified as an anonymous I.P. address. Transaction is filtered.
RM008	BIN Country and I.P. Country mismatch	The Issuing Bank Country and the Client's I.P. country does not match. Transaction is filtered.
RM009	BIN Country and Customer Country mismatch	IP country of customer and billing country of the customer does not match. Transaction is filtered.
RM010	BIN Phone mismatch	Customer inputted a wrong BIN Phone (or Customer Support number). Transaction is filtered.
RM011	BIN name mismatch	Customer has inputted a wrong Issuing bank name. Transaction is filtered.
RM012	Customer I.P. address and Billing address distance exceeded	The Client's I.P. address host location has exceeded its allotted distance from its disclosed billing location. Transaction is filtered.
RM013	City, State mismatch Postal Code	The Customers disclosed Postal Code and did not match to the given City and State. Transaction is filtered.
RM014	Fraud score exceeded	The transaction detail that was passed by the customer has exceeded its allowable score. Transaction is filtered.
RM015	Proxy score exceeded	The I.P. address that was passed by the customer has exceeded the allowable proxy score. Transaction is filtered.
RM016	Risk Score is High	The transaction has exceeded its allowable risk score. Transaction is filtered.
RM017	Host I.P. not registered	The Merchant is using an I.P. address which is not registered in the system. Transaction is filtered.
RM018	Card Type Restricted	The Merchant ID is not to accept this card type. Transaction is filtered.
RM019	Decline due to exceeded Client I.P. allowable limit.	The client's I.P. address being passed exceeded the velocity restriction. Transaction is filtered.
RM020	Decline due to exceeded account use.	The card account being passed has exceeded the velocity restriction. Transaction is filtered.
RM021	Decline due to exceeded amount ticket item.	The customer has passed a transaction amount that is less or greater than the minimum / maximum amount ticket policy restriction. Transaction is filtered.
RM022	Decline due to exceeded allowable transaction count in a day.	The merchant has exceeded its allowable transaction count for the day. Transaction is filtered.
RM023	Fraud Scoring Passed	The merchant transaction has passed the Fraud Score.
RM024	Decline due to AVS result failure	Address verification system filtered the transaction.
RM025	Decline by Acquiring Bank Fraud system	Transaction was decline by Acquiring bank's fraud validation.
RM026	Decline by Paypal Fraud control system	Please refer to Paypal API
RM027	Decline due to card account user policy The card account being used was already used by a previous customer.	The card account being used was already used by a previous customer. Transaction is filtered.

Response Code	Response Message	Meaning
RM028	Decline due to Suspected Fraud Pattern	Reserved
RM029	Decline due to Suspected Fraud Pattern	Reserved
RM030	Decline due to Suspected Fraud Pattern	Reserved
RM031	Customer Phone and Postal Code mismatch	The given Customer Phone is not found in the provided Postal code. Applicable for U.S. Address Only. Transaction is filtered.
RM032	Telephone Verification Failed	This means that the customer did not provide a valid telephone or contact number. Transaction is filtered.
RM033	Risk Check Failed. Fraud Processor Unavailable.	This means that the Fraud processor cannot be reached during the transaction process.
RM034	Transaction Failed, Card number being enrolled for tokenization already exist under a different client_id.	This is a fraud policy check that prohibits merchant from enrolling the same card number to be used with different customers.
RM035	Transaction subject to manual review.	This is a fraud policy check initiated by Paygate system or its acquiring bank. It filtered the transaction for manual review. Transaction may be accepted or rejected depending on risk result. Kindly re-query for further information.
RM036	Decline due to exceeded merchant volume	This means that the merchant account has exceeded the allowed volume limit of a given time period.
RM037	Transaction Failed, Device ID Blackisted.	This means that the device's IMEI being passed by the merchant is blacklisted in Paynamics Payment Gateway.
RM038	Transaction Failed, User ID Blacklisted.	This means that the user_id being passed by the merchant is blacklisted in Paynamics Payment Gateway.
RM039	Transaction Failed, Email domain restricted.	This means that the email being used is fake or blacklisted by Fraud Gate.
RM040	Failed to meet minimum/maximum amount.	The customer has passed a transaction amount that is less than the minimum or greater than the maximum amount ticket policy restriction. Transaction is filtered.
RM041	Decline due to Suspected Security Breach.	This means the transaction was flagged due to unenrolled i.p. address or domain. Kindly contact PTI Technical team for possible I.P. or domain whitelisting
RM042	Transaction Failed. Credit Card Not Allowed.	This means the card that was used was not allowed under merchant restriction.
RM043	Transaction Failed. Debit Card Not Allowed.	This means the card that was used was not allowed under merchant restriction.
RM044	Declined due to failed validation or session timeout	Declined due to failed validation or session timeout
RM045	Transaction Failed. Prepaid Card Not Allowed.	This means the card that was used was not allowed under merchant restriction.
RM046	Transaction has an invalid response message from the acquirer or acquiring processor. Kindly contact acquirer for more information.	This means the acquirer or acquiring processor has sent an invalid response message (i.e. incorrect signature) when doing a callback to Paynamics. Please take note that Paynamics is treating this as a “pending state” since Paynamics did not account for the actual response message. Merchant must wait for the final notification status from Paynamics.

Query Message Response Codes

Response Code	Response Message	Meaning
QM001	Query Successful	The query transaction was successful executed, refer to the response status body for further transaction result.

In addition, here are the other General Message Response Codes that can be used by the query.

Response Code	Response Message	Meaning
GR007	MID incorrect or not found	Merchant ID that was provided is incorrect or unregistered.
GR011	Request_id already processed	The request id that was sent is not unique or is already processed.
GR015	Original Trx ID missing or invalid	Original Trx ID is required or the Original Trx ID that was provided was not found. This can happen with a query transaction in which the merchant request might not have reached Paygate.
GR036	Signature Verification failed	The signature provided by the merchant is invalid or was not parsed successfully by Paygate.
GR064	Transaction Query Successful	This means that the subscription query process was successful.
GR123	Transactions is Incomplete.	Transactions is Incomplete.

APPENDIX B: PAYMENT METHOD LIST

No		Pmethod value	Description
1	**bank_otc**	**bdootc**	Banco De Oro Bank Philippine Branches
		pnbotc	Philippine National Bank Branches
		ucpbotc	United Coconut Planters Bank Branches
		sbcotc	Security Bank Branches
2	**nonbank_otc**	**ecpay**	Ecpay Network Philippines
		da5	Direct Agents 5 Network Philippines
		expresspay	Expresspay Network Philippines
		dp	DragonPay Philippines
		7eleven	711 Network Philippines
		cliqq	711 Cliqq Network Philippines
		ml	Mlhuillier Pawnshop Network
		ceb	Cebuana Pawnshop Network
		sm	SM Bills Payment Network
		truemoney	True Money Network
		posible	Posible.net Network
		etap	Etap Network
3	**creditcard**	**cc**	Credit Card
4	**onlinebillspyament**	**bdoobp**	BDO Online Bills Payment
		pnbobp	Philippine National Bank Online Bills Payment
		ucpbobp	United Coconut Planters Online Bills Payment
		sbobp	Security Bank Online Bills Payment
5	**onlinebanktransfer**	**bn**	Bancnet Philippines
		ents	Enets Singapore
		eghl	E-GHL Thailand and Malaysia
		poli	Polipayments Australia and New Zealand
		bpionline	Bank of the Philippine Islands
		ubponline	Unionbank of the Philippines
6	**wallet**	**pp**	Paypal
		vcard	Virtual Card
		gc	Gcash
		paymaya	Paymaya
		coins	Coins PH
		grabpay	Grabpay PH
		alipay	Alipay
		wechatpay	Wechat Pay
7	**installment**	**bdoinstall**	BDO Installment
		hsbinstall	HSBC Installment
		mtrinstall	Metrobank Installment

APPENDIX C: DISPUTE CODE LIST

Dispute Payment Method List

No		Pmethod value
1	bank_otc	bdootc
		pnbotc
		ucpbotc
		sbcotc
2	nonbank_otc	ecpay
		da5
		expresspay
		dp
		7eleven
		cliqq
		ml
		ceb
		sm
		truemoney
		posible
		etap
3	creditcard	cc
4	onlinebillspyament	bdoobp
		pnbobp
		ucpbobp
		sbobp
5	onlinebanktransfer	bn
		ents
		eghl
		poli
		bpionline
		ubponline
6	wallet	pp
		vcard
		gc
		paymaya
		coins
		grabpay
		alipay
		wechatpay
7	installment	bdoinstall
		hsbinstall
		mtrinstall

Dispute Type List

Value	Description
RETRIEVAL	Stands for Retrieval request. It means the cardholder has sent an inquiry through its issuing bank clarifying the transaction they have made with the merchant. Merchant should normally present evidence of the transaction. Applicable for credit card transactions. Default dispute action for this is NO EFFECT.
CHB	Stands for Chargeback. It means the cardholder has filed a refund from their issuing bank which was forwarded to the acquiring bank. Applicable for Credit card transactions. Default dispute action for this is DEDUCT.
CHBR	Chargeback Representment. It means the merchant has successfully represented the chargeback with valid documents, and the cardholder's issuing bank has no objections. Applicable for Credit card transaction. Default dispute action for this is ADD.
ARBT	Stands for Arbitration. This means that the dispute is in arbitration mode with the card scheme. Default dispute action for this is NO EFFECT.
RR	Stands for Refund Request. This means that merchant's client is requesting for refund. Default dispute action is NO EFFECT, however if the refund is processed, the dispute action will be updated to DEDUCT if the merchant has agreed to have the refund deducted on the merchant settlement balance.
DR	Stands for Dispute Request. This is similar to Chargeback however it applies to alternative forms of payment method (i.e. Bancnet, Gcash, and Chinese Debit cards). Default dispute action would be DEDUCT.
DRR	Stands for Dispute Represented. This is similar to Chargeback representment however it applied to alternative forms of payment method (i.e. Bancnet, Gcash, and Chinese debit cards). Default dispute action would be DEDUCT.

APPENDIX D: SAMPLE REQUEST AND RESPONSE

Request Format:

```
<?xml version="1.0" encoding="utf-8" ?>
<Request>
  <orders>
    <items>
      <Items>
        <itemname>JuanLife 300 0002</itemname>
        <quantity>1</quantity>
        <amount>300</amount>
      </Items>
    </items>
  </orders>
  <mid></mid>
  <request_id></request_id>
  <ip_address></ip_address>
  <notification_url></notification_url>
  <response_url></response_url>
  <cancel_url></cancel_url>
  <mtac_url></mtac_url>
  <descriptor_note></descriptor_note>
  <fname></fname>
  <lname></lname>
  <mname></mname>
  <address1></address1>
  <address2></address2>
  <city></city>
  <state></state>
  <country></country>
  <zip></zip>
  <secure3d></secure3d>
  <trxtype></trxtype>
  <email></email>
  <phone></phone>
  <mobile></mobile>
  <client_ip></client_ip>
  <amount></amount>
  <currency>PHP</currency>
  <expiry_limit></expiry_limit>
  <mlogo_url></mlogo_url>
  <pmethod></pmethod>
  <signature></signature>
</Request >
```

Response Format:

```
<?xml version="1.0" encoding="utf-8"?>
<ServiceResponseWPF xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <application>
    <merchantid></merchantid>
```

```
    <request_id></request_id>
    <response_id></response_id>
    <timestamp></timestamp>
    <rebill_id></rebill_id>

<signature>f221a76d194c9f14a19f4bcf8357f8a55cebb5d7b49e30c93667b625a986341f5e1ba0b
358033acab872364e68a3b18f14f8998a10d029d7ac1c2e7f670ad921</signature>
    <ptype></ptype>
  </application>
  <responseStatus>
    <response_code></response_code>
    <response_message></response_message>
    <response_advise></response_advise>
    <processor_response_id></processor_response_id>
    <processor_response_authcode></processor_response_authcode>
  </responseStatus>
  <MetaData />
</ServiceResponseWPF>
```