PayUbiz
Integration Document

9th Floor, Bestech Business Tower
Sector 48, Sohna Road
Gurgaon, 122002
India
T: 0124-6749078
F: 0124-6749101

Table of Contents (Click on the topic for direct access)

OVERVIEW 3

PayU Payment Gateway 3

Payment Process Flow 4

SECTION I: WEBSITE INTEGRATION 4

Steps for Integration Process 5

Parameters to be posted by Merchant to PayU in Transaction Request 6

Seamless Integration – Parameters in Transaction Request 16

Additional Charges – Convenience Fee Model (To be used only if recommended by Account Manager at PayU) 17

Method 1: Enabled from backend at PayU 17

Method 2: Merchant Calculates and Posts Additional Charges to PayU 18

Important Things to remember: Characters allowed for parameters 19

Formula for hash (checksum) before transaction 19

Formula for hash (checksum) after transaction 19

Hash (Checksum) Algorithm Example codes 19

For PHP 19

For .NET 20

For JSP 20

Response Parameters posted by PayU to Merchant in redirection 20

Sequence Diagram for Cardless EMI 25

Cardless EMI Additional Response(Server to Server) 25

Whitelisting Required 29

Data Sharing between PayU and Merchant for Cardless EMI 29

Enabling HDFC Debit Card, Bajaj Finserv, Axis Debit Card and Zest Money EMIs 31

Shopping Cart Integration Kits 32

Platform based Integration kits 33

SECTION II: WEB SERVICES – APIs 34

Web Service Request Format: 34

Web Service Response Format 35

LIST OF APIs AND THEIR DESCRIPTION 35

1) verify_payment 35

3) cancel_refund_transaction 38

4) check_action_status (1ST Usage) 40

5) check_action_status (2nd Usage) 41

6) getAllRefundsFromTxnIds 43

7) capture_transaction 44

7) update_requests
8) cod_verify
9) cod_cancel 48
10) cod_settled 49
11) get_TDR 50
12) udf_update 51
13) create_invoice 52
14) expire_invoice 53
15) check_offer_status (1st Usage) 54
16) check_offer_status (2nd Usage) 55
17) getNetbankingStatus 57
18) getIssuingBankStatus 58
20) get_Transaction_Details 60
21) get_transaction_info 62
22) check_isDomestic 64
23) get_settlement_details 65
24) get_merchant_ibibo_codes 67
25) eligibleBinsForEMI 68
26) get_user_cards 69
27) save_user_card 70
29) edit_user_card 71
30) delete_user_card 71
Webhooks/Callbacks 76

OVERVIEW

This document describes the **steps** for technical integration process between merchant website and PayU Payment Gateway for enabling online transactions. This document is covered in two sections. Section I covers **website integration** and Section II covers **APIs** provided to the merchants.

PayU Payment Gateway

PayU offers electronic payment services to merchant website through its partnerships with various banks and payment instrument companies. Through PayU, the customers would be able to make electronic payments through a variety of modes which are mentioned below:

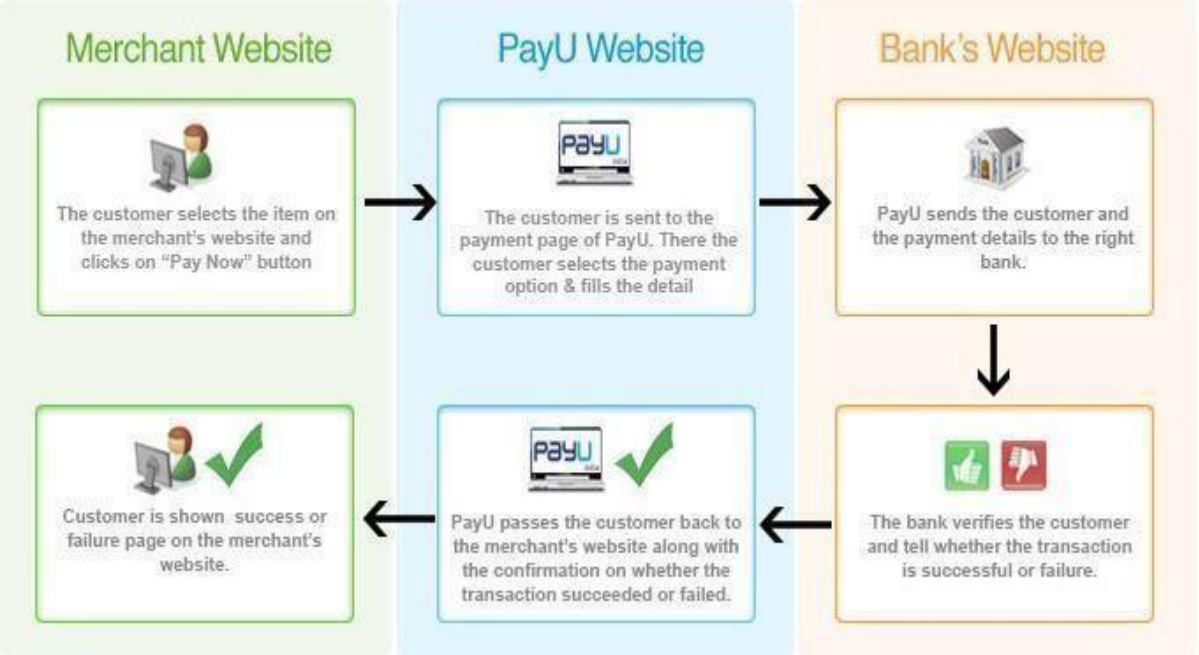
- Credit cards
- Debit cards
- Online net banking accounts
- EMI payments
- Cash Cards
- Email Invoicing

- IVR
- Cash on Delivery (COD)
- Cardless EMI
- Pre-Auth and Capture

PayU also offers an **online interface** (known as **PayU Dashboard**) where the merchant has access to various features like viewing all the transaction details, settlement reports, analytical reports etc. Through this interface, the merchant can also execute actions like capturing, cancelling and refunding the transactions. This online interface can be accessed through https://www.payubiz.in by using the username and password provided to you.

Payment Process Flow

The following diagram explains how the customer makes the payment and how the process flows:



SECTION I: WEBSITE INTEGRATION

The merchant can integrate with PayU by using one of the below methods:

1) **Non-Seamless Integration** – In this mode during the transaction, the customer would be redirected from merchant website to PayU payment page. On the PayU payment page, he would need to select the payment option and enter the respective card details. After this, PayU would re-direct the customer to the desired payment option webpage for further authentication.

1) **Seamless Integration** - In this mode, the merchant needs to collect the customer card details on their own website and post them to PayU. Here, the customer would not be stopped at PayU payment page at all, as the payment option and card detailsare already received from the merchant. The merchant must be **PCI-DSS certified** in this case. For further information on PCI-DSS certification please contact your Account Manager at PayU.

Also, the merchant website can be based either on a **shopping cart** or can be developed by the merchant **(not based upon any shopping cart).** Based on the type (out of these two), PayU would provide integration kit (code) to the merchant which they needs to incorporate at their end. The list of Integration kits supported by PayU at present is mentioned in later sections of the document.

Steps for Integration Process

The steps for integrating with PayU can technically be described as below:

1) To start off the integration process, you would be provided a **test setup** by PayU where you would be given a test merchant account and test credit card credentials to have a first-hand experience of the overall transaction flow. Here, you need to make the transaction request on our **test server (and not the production server)**. Once your testing is complete, **then only** you will be ready to move to the PayU production server.

2) To initiate a transaction, the merchant needs to generate a **POST REQUEST** - which must consist of mandatory and optional parameters mentioned in the **later section**. This POST REQUEST needs to be hit on the below mentioned PayU URLs:

   For PayU Test Server:
   POST URL: **https://test.payu.in/_payment**
   For PayU Production (LIVE) Server:
   POST URL: **https://secure.payu.in/_payment**

3) In the merchant initiated **POST REQUEST**, one of the mandatory parameters is named as **hash.** The details of this hash parameter have been covered in the later section. But it is **absolutely critical** for the merchant to calculate the hash correctly and post to us in the request.

4) When the transaction **POST REQUEST** hits the PayU server, a new transaction entry is created in the PayU Database. To identify each new transaction in the PayUDatabase, a unique identifier is created every time at PayU's end. This identifier is known as the **PayU ID (or MihPayID).**

5) With the POST REQUEST, customer would be re-directed to PayU's payment page. Customer now selects the particular payment option on PayU's page (Credit Card/Debit Card/Net Banking etc) and clicks on 'Pay Now'. PayU re-directs the customer to the chosen bank. The customer goes through the necessary authorization/authentication process ast bank's login page, and the bank gives the success/failure response back to PayU.

6) PayU marks the transaction status on the basis of response received from Bank. PayU provides the final transaction response string to the merchant through a **POST RESPONSE.** The parameters in this response are covered in the subsequent sections.

7) In the POST RESPONSE sent by PayU, you would receive the final status of the transaction. You will receive the hash parameter here also. Similar to step 3, it is

absolutely crucial to verify this hash value at your end and then only accept/reject the invoice order. This is done to strictly avoid any tampering attempt by the user.

Please Note:

It is absolutely mandatory that the hash (or checksum) is computed again after you receive response from PayU and compare it with request and post back parameters. This will protect you from any tampering by the user and help in ensuring a safe and secure transaction experience. It is also a mandate that you secure your integration with PayU by implementing Verify webservice and Webhook/callback as a secondary confirmation of transaction response. Detailed integration process of Verify webservice and webhook and be found further in this document.

Please note that PayU will not be responsible for any security breaches (including any data breaches) that may occur due to non-implementation of the aforesaid security features at your end or any loss or damage arising therefrom, to you or to any third party.

DISCLAIMER:

1. Test URL: The Test URL is provided to PayU merchants to test the integration of their server with that of PayU or Bank. It is understood that since this is merely a Test URL, the Merchant should not treat any transactions done on this Test server as liveand should not deliver the products/services with respect to any such test transactions even in the case your server receive a successful transaction confirmation from PayU/Bank.

2. Merchants are herein forth requested to set up required control checks on their (merchant) systems/servers to ensure that only those transactions should get routed to the PayU test server which are initiated with sole intention of test the environment.

Sr. No	Variable	Description
1)	key **(Mandatory)**	This parameter is the unique Merchant Key provided by PayU for your merchan account. The Merchant Key acts as the unique identifier (primary key) to identify a particular Merchant Account in our database. While posting the data to us, you need to put this Merchant Key value for you merchant account in this parameter. Also, please note that during integration with PayU, you would need to first integrate with our Test Server. PayU would be providing you the necessary Merchant Key for test server. Please do not use your live account's merchant key here. It would not work. Once testing is done, you are ready to move to live server. Here, you would need to replace the test Merchant Key with Live Merchant Key. This is a critical step for successfully moving to live PayU server. Example: C0Ds8q
2)	txnid **(Mandatory)**	This parameter is known as Transaction ID (or Order ID). It is the order reference number generated at your (Merchant's) end. It is an identifier which you (merchant) would use to track a particular order. If a transaction using a particular transaction ID has already been successful at PayU, the usage of same Transaction ID again would fail. Hence, it is essential that you post us a unique transaction ID for every new transaction. (Please make sure that the transaction ID being sent to us hasn't been successful earlier. In case of this duplication, the customer would get an error of 'duplicate Order ID'). Data Type – Varchar Character Limit – 25 characters Example: fd3e847h2
3)	amount **(Mandatory)**	This parameter should contain the payment amount of the particular transaction. This amount must be greater than Rs. 8000 for Cardless EMI option. Note: Please type-cast the amount to float type Example: 10.00
4)	productinfo **(Mandatory)**	This parameter should contain a brief product description. It should be a string describing the product (The description type is entirely your choice). Data type - Varchar Character Limit – 100 characters Example: tshirt100
5)	firstname **(Mandatory)**	Self-Explanatory (Must contain the first name of the customer) Data Type – Varchar Character Limit – 60 characters Example: Ankit
6)	email **(Mandatory)**	Self-explanatory (**Must contain the email of the customer**) Data type – Varchar Character Limit – 50 Example: ankitverma@gmail.com This information is helpful when it comes to issues related to fraud detection and chargebacks. Hence, it is must to provide the correct information

7)	phone **(Mandatory)**	Self-explanatory (**Must contain the phone number of the customer**) Data type – Varchar Character Limit – 50 (numeric value only) Example:9843176540 This information is helpful when it comes to issues related to fraud detection and chargebacks. Hence, it is must to provide the correct information
8)	lastname (Mandatory)	Self-Explanatory (only alphabets a-z are allowed). (Must contain the last name of the customer). Data Type – Varchar Character Limit – 20 characters Example: Verma
9)	address1	Self-Explanatory. This parameter is mandatory for Cardless EMI option. This will be used for billing address. Data Type – Varchar Character Limit – 100 Characters allowed : A to Z, a to z, 0 to 9, @, - (Minus), _ (Underscore), / (Backslash), (Space), (Dot)
10)	address2	Self-explanatory. Data Type – Varchar Character Limit – 100 (Allowed characters are same as for address1 parameter)
11)	city	Self-explanatory. This parameter is mandatory for Cardless EMI option. This will be used for billing address. Data type – Varchar Character Limit – 50 (Allowed characters are same as for address1 parameter)
12)	state	Self-explanatory. This parameter is mandatory for Cardless EMI option. This will be used for billing address. Data type – Varchar Character Limit – 50 (Allowed characters are same as in address parameter)
13)	country	Self-explanatory. This parameter is mandatory for Cardless EMI option. This will be used for billing address. Data type – Varchar Character Limit – 50 (Allowed characters are same as in address parameter)
14)	zipcode	Self-explanatory. This parameter is mandatory for Cardless EMI option. This will be used for billing address. Data type – Varchar Character Limit – 20 (Only numeric value allowed)
15)	udf1	User defined field 1 – This parameter has been made for you to keep any information corresponding to the transaction, which may be useful for you to keep in the database. UDF1-UDF5 fields are for this purpose only. It's completely for your usage and you can post any string value in this parameter. udf1-udf5 are optional parameters and you may use them only if needed Data type – Varchar Character Limit – 255

16)	udf2	User defined field 2 – Same description as UDF1 Data type – Varchar Character Limit – 255
17)	udf3	User defined field 3 – Same description as UDF1 Data type – Varchar Character Limit – 255
18)	udf4	User defined field 4 – Same description as UDF1 Data type – Varchar Character Limit – 255
19)	udf5	User defined field 5 – Same description as UDF1 Data type – Varchar Character Limit – 255
20)	surl (Mandatory)	Success URL - This parameter must contain the URL on which PayU will redirect the final response if the transaction is successful. The response handling can then be done by you after redirection to this URL
21)	furl (Mandatory)	Failure URL - This parameter must contain the URL on which PayU will redirect the final response if the transaction is failed. The response handling can then be done by you after redirection to this URL
22)	curl	Cancel URL - This parameter should contain the URL on which PayU will redirec the response if the transaction is cancelled by the customer on PayU page. The response handling can then be done by you after redirection to this URL
23)	hash (Checksum) **(Mandatory)**	Hash is a crucial parameter – used specifically to avoid any tampering during the transaction. There are two different methods to calculate hash. **Please follow method 1 only.** Method 2 is just there for the documentation and is not to be used Method 1 - This is the simplest way of calculating the hash value. Here, please make sure that the **api_version** parameter is **NOT POSTED** from your end. For hash calculation, you need to generate a string using certain parameters and apply the sha512 algorithm on this string. Please note that you have to use pipe (|) character in between these parameters as mentioned below. The parameter order is mentioned below: **sha512(key|txnid|amount|productinfo|firstname|email|udf1|udf2|udf3|udf4|udf5||||||SALT)** All these parameters (and their descriptions) have already been mentioned earlier in this table. Here, SALT (to be provided by PayU), key, txnid, amount, productinfo, firstname, email are **mandatory** parameters and hence **can't be empty** in hash calculation above. But, udf1-udf5 are **optional** and hence you need to calculate the hash based upon the fact that whether you are posting a particular udf or not. For example, if you are NOT posting udf1. Then, in the hash calculation, udf1 field will be left empty. Following examples will clarify various scenarios of hash calculation: Case 1: If all the udf parameters (udf1-udf5) are posted by the merchant. Then, hash=sha512(**key|txnid|amount|productinfo|firstname|email|udf1|udf2|udf3|udf4|udf5||||||SALT**)

		Case 2: If only some of the udf parameters are posted and others are not. For example, if udf2 and udf4 are posted and udf1, udf3, udf5 are not. Then, hash=sha512(**key|txnid|amount|productinfo|firstname|email||udf2||udf4||||||SALT**) Case 3: If NONE of the udf parameters (udf1-udf5) are posted. Then, hash=sha512(**key|txnid|amount|productinfo|firstname|email||||||||||SALT**) Example: If key=**C0Dr8m**, txnid=**12345**, amount=**10**, productinfo=**Shopping**, firstname=**Test**, email=**test@test.com**, udf2=**abc**, udf4=**15**, SALT=**3sf0jURk** and udf1, udf3, udf5 are **not** posted. Then, hash would be calculated as Case 2 above: **sha512(C0Dr8m|12345|10|Shopping|Test|test@test.com||abc||15||||||3sf0jURk)** (This value comes out to be *ffcdbf04fa5beefdcc2dd476c18bc410f02b3968e7f4f54e8f43f1e1a310bb32e3b4dec9305232bb89db5b1d0c009a53bcace6f4bd8ec2f695baf3d43ba730ce*) IMPORTANT: For details related to hash at the time of post back from PayU to the merchant, please refer to later section. This is also absolutely mandatory to avoid any tampering. Method 2- Second method for hash calculation (***Don't use this method. It is only for internal documentation***). Here, parameter **api_version** should be equal to 2. hash = sha512(**key|txnid|amount|offer_key|api_version|SALT**) Method 3 - Third method for hash calculation - used specifically for Ola Postpaid mode transaction. Here, parameter **api_version** must be equal to 4. hash = sha512**(key|txnid|amount|productinfo|firstname|email|udf1|udf2|udf3|udf4|udf5|udf6|udf7|udf8|udf9|udf10|phone)**
24)	pg	This parameter signifies the payment category (tab) that you want the customer to see by default on the PayU page. Hence if PG='NB', then after redirection to PayU's payment page, the Net Banking option would be opened by default. (PG parameter may take different values like : **NB** for Net Banking tab, **CC** for Credit Card tab, **DC** for Debit Card tab, **CASH** for Cash Card tab and **EMI** for EMI tab) Note: PG = CC, i.e. Credit Card tab is recommended. If PG is left empty, CC will be taken as default.
25)	codurl	**Cash on delivery URL** – This parameter is used when a transaction attempt fails. In this case, if retries have been enabled for you (done by PayU for your merchant account), our PayU page is shown (to provide another attempt to customer to complete the transaction) with the 'failed transaction message' to the customer and also 'Pay by COD' option. To handle this 'Pay by COD' option, you can fill the COD URL parameter with a URL which we will redirect to, when the customer selects this option. This way, you can then provide the customer another attempt at the transaction through this URL.
27)	drop_category	This parameter is used to customize the payment options for each individual transaction. For example, if we consider the categories Credit Card, Debit Card and Net Banking for a merchant. If there are 30 net banking options available and the merchant wants to drop 2 of those net banking options (i.e. do not

display those 2 options on PayU page), then drop_category parameter can be used effectively. Below table denotes example of category and sub-categories at PayU

Category	Sub-category
Credit Card	MasterCard, Amex, Diners etc
Debit Card	Visa, Mastercard, Maestro etc
Net Banking	SBI Net Banking, HDFC Net Banking etc
EMI	CITI 3 Months EMI, HDFC 6 Months EMI etc
Cash Card	AirtelMoney, YPay, ITZ Cash card etc

Now, to drop the whole category, please use the following values:

Category	Value of 'drop_category' parameter
Credit Card	CC
Debit Card	DC
Net Banking	NB
EMI	EMI
Cash Card	CASH

To drop sub-categories, please use the respective bank codes for them. Please contact PayU to get the respective bank codes. Also note that the delimiter for categories is comma (,) character and for sub-categories it is the pipe (|) character. Examples for usage:

drop_category - DC|VISA|MAST, NB|ICIB : Here, for debit card category, only Visa and Master Card options would be dropped (and hence not displayed on the PayU page). In Net Banking option, only ICICI Net Banking would be dropped. All other active payment options would be displayed.

drop_category - CC|AMEX, DC|VISA, EMI|EMI6 : Here, for credit card category, only AMEX option would be dropped (and hence not displayed). In debit card category, only VISA option would be dropped. And in EMI category, only HDFC 6 months EMI option (bank code – EMI6) would be dropped. All the other active payment options would be displayed.

Note: Please make sure to use this parameter only after testing properly as an incorrect string will lead to undesirable payment options being displayed.

<table>
<tr>
<td>28)</td>
<td>enforce_paymethod</td>
<td>This parameter allows you to customize the payment options for each individual transaction. For example, if we consider the categories Credit Card, Debit Card and Net Banking. If the merchant wants to display only 4 debit card options and only 2 Net Banking options for a transaction A and wants to display only 2 debit card option and 5 Net Banking options for another transaction B, the customization is needed and this parameter (enforce_paymethod) provides exactly that feature.

The merchant needs to put the necessary payment options in this parameter and post it to us at the time of transaction. All the categories and subcategories have specific values which need to be put in this string. The categories/subcategories are as follows:
<table>
<tr><th>Category</th><th>Sub-category</th></tr>
<tr><td>Credit Card</td><td>MasterCard, Amex, Diners etc</td></tr>
<tr><td>Debit Card</td><td>Visa, Mastercard, Maestro etc</td></tr>
<tr><td>Net Banking</td><td>SBI Net Banking, HDFC Net Banking etc</td></tr>
<tr><td>EMI</td><td>CITI 3 Months EMI, HDFC 6 Months EMI etc</td></tr>
<tr><td>Cash Card</td><td>AirtelMoney, YPay, ITZ Cash card etc</td></tr>
</table>
Now, to enforce complete categories, please use the following values:
<table>
<tr><th>Category</th><th>Value of enforced_paymethod</th></tr>
<tr><td>Credit Card</td><td>creditcard</td></tr>
<tr><td>Debit Card</td><td>debitcard</td></tr>
<tr><td>Net Banking</td><td>netbanking</td></tr>
<tr><td>EMI</td><td>emi</td></tr>
<tr><td>Cash Card</td><td>cashcard</td></tr>
</table>
To enforce sub-categories, please use the respective bank codes for them. Please contact PayU to get the respective bank codes. Please note that the delimiter is pipe (|) character here. Examples:

creditcard|debitcard|HDFB|AXIB – Here, all the credit card and debit card options would be displayed (as the whole category is enforced). In Net Banking category, only HDFC and AXIS Net Banking would be displayed. Rest of the categories would not be displayed at all (EMI, Cash card etc – as they are not being mentioned in the string).

creditcard|VISA|SMAE|netbanking|EMI6|EMI9|cashcard – Here, all the credit card options, net banking options and cash card options would be displayed (as the whole category is enforced for these). In Debit card category, Visa and SBI Maestro payment options would be displayed (as bank codes for only these options are mentioned in the string). In EMI category, only HDFC EMI (for 6 and 9 months) would be displayed.

Note: Please make sure to use this parameter only after testing properly as an incorrect string will lead to undesirable payment options being displayed.</td>
</tr>
</table>

29)	custom_note	This parameter is useful when you want to display a message string on the PayU Payment page. For example, if for a particular product X, you want your customer to know that an extra amount of Rs 100 would be charged afterwards, you can show the corresponding message on payment page. For this, you needto post that message in this parameter – custom_note. The note would be displayed just below the payment tabs (Credit Card/Debit Cards/Net Banking) For Example: custom_note = **You will be charged an extra amount of Rs 100 on this transaction** **Characters allowed:** A to Z, a to z, 0 to 9, % (percentage), , (comma), . (decimal), ' (apostrophe)
30)	note_category	This parameter gives you an option of showing the message string passed in custom_note parameter for only the selected Payment categories. Hence, this parameter should contain the comma separated list of the payment options for which the **custom_note** will appear. For example: **note_category = CC,NB** will show the custom_note for Credit Card & Net banking only
31)	api_version	Please don't use this parameter while posting the data. This is a deprecated parameter.
32)	shipping_firstname	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for shipping firstname only and this is mandatory for Cardless EMI.** Self-Explanatory (Constraints same as firstname parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
33)	shipping_lastname	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for shipping lastname only and this is mandatory for Cardless EMI.** Self-Explanatory (Constraints same as lastname parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
34)	shipping_address1	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for address only and this is mandatory for Cardless EMI** Self-Explanatory (Constraints same as address1 parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
35)	shipping_address2	**This parameter has to used in case of COD (Cash on Delivery) Only.** Self-Explanatory (Constraints same as address2 parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
36)	shipping_city	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for shipping_city only and this is mandatory for Cardless EMI.** Self-Explanatory (Constraints same as city parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
37)	shipping_state	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for shipping_state only and this is mandatory for Cardless EMI.** Self-Explanatory (Constraints same as **state** parameter). If this parameter is

		posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
38)	shipping_country	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for shipping_country only and this is mandatory for Cardless EMI.** Self-Explanatory (constraints same as **country** parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
39)	shipping_zipcode	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for firstname only and this is mandatory for Cardless EMI.** Self-Explanatory (constraints same as **zipcode** parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
40)	shipping_phone	**This parameter has to used in case of COD (Cash on Delivery) or Cardless EMI Only. Use this for firstname only and this is mandatory for Cardless EMI.** Self-Explanatory (constraints same as **phone** parameter). If this parameter is posted, the corresponding value would be filled up automatically in the form under COD tab on PayU payment page
41)	offer_key	This parameter is useful when the merchant wants to give the customer a discount offer on certain transactions based upon a pre-defined combination This combination can be based upon payment options/bins etc. For each new offer created, a unique **offer_key** is generated. At the time of a transaction, this offer_key needs to be posted by the merchant.
42)	partner_hold_time	This parameter is useful when merchants wants to provide hold time of the product in case of Cardless EMI option. Hold time defines the time until thetime for which merchant can hold the current basket until the merchant receives the final success/failure status from PayU. Default partner_hold_time for all transactions can be defined for the merchant by reaching out to integration team at payu Otherwise, it will be considered 15 days. After transaction initiation, transaction for Cardless EMI will expire after partner_hold_time value and will be marked as failed. This value should be in minutes. E.g if partner hold time is 3 days, then value will be 4320(3*24*60)
43)	Items	Array of items in the basket Array [Uuid – string - Identifier of the item Name – string - Item name[Required] Unit_price – Decimal[decimal(18,2)] – Price in rupees[Required] Sku – string - Stock keeping unit (article unique identifier) Category – string - Item Category Manufacturer – string - Item manufacturer Quantity – Integer[int64] – Quantity of itemp[Required] Img – string – Link to item avatar on Picture] "items" as a json of array of items (a json string). As an example, items = [{"uuid"="2273", "name"="Sony Xperia XZ1 Dual (Black)", "unit_price"="42990", "manufacturer"="Sony", "quantity"="1", "img"="https://www.payu.com/uploads/sony-xperia-xz1-black-1-12753.jpg"}]

44)	Birthday	string <date> Customer birthday in format YYYY-MM-DD e.g. – 1990-01-17
45)	Gender	String e.g – MALE, FEMALE
46)	Ipurl	In progress URL - This parameter must contain the URL on which PayU will redirect the customer if the transaction is in progress and needs some work from the backend. The response handling can then be done by the merchant after redirection to this URL. This is required for Cardless EMI option
47)	pre_authorize	This parameter needs to be sent in the request only if the transaction is intended on auth-capture model. This means the transaction amount would not actually debit, but it would be blocked. Its value should be 1. Please ignore this flag if the transaction is not on auth-capture model. Auth-capture model only works on credit cards (transactions will fail with debit cards for auth-capture model)
48)	transactionContext	This is a "PhonePe Switch" specific parameter, Its value will be provided by PhonePe to merchant and merchant post this parameter in the transaction request to PayU. Other parameter that needs to be passed with it are "pg": CASH and "bankcode": PPINAPP.

Table 1: Post Parameters from Merchant to PayU

For your reference, please find sample code below which shows the basic set of parameters being posted. Please execute this piece of code in browser to observe the POST request being re-directed to PayU page and then you can form the complete transaction request in your code base (with the mandatory and optional parameters)

```
<html>
<head>
</head>
<body>
<form action='https://test.payu.in/_payment' method='post'>
<input type="hidden" name="firstname" value="Vikas Kumar" />
<input type="hidden" name="lastname" value="" />
<input type="hidden" name="surl" value="https://www.google.com" />
<input type="hidden" name="phone" value="9999999999" />
<input type="hidden" name="key" value="C0Dr8m" />
<input type="hidden" name="hash" value =
"c2522a8d561e7c52f7d6b2d46c96b924afac8554313af4b80edef3e237e179bd6e2020e8c548060306d9fa2cf5c75
c35205bcc4b09bcf5b9a9bececc8de2952d0" />
<input type="hidden" name="curl" value="http://www.google.com" />
<input type="hidden" name="furl" value="https:/www.yahoo.in" />
<input type="hidden" name="txnid" value="PLS-10061-3" />
<input type="hidden" name="productinfo" value="SAU Admission 2014" />
<input type="hidden" name="amount" value="600.000" />
<input type="hidden" name="email" value="vikaskumarsre@gmail.com" />
<input type= "submit" value="submit">
</form>
</body></html>
```

For seamless mode, 8 extra parameters are required in the transaction Post Request from your end – along with the parameters mentioned in the above table. These are mentioned below:

S No	Variable	Description
1)	pg (**Mandatory**)	This parameter is the same as the one mentioned in the POST Parameters mentioned above. It must be set as the payment category. Please set its value to '**NB'** for Net Banking , '**CC'** for Credit Card , '**DC'** for Debit Card , '**CASH'** for Cash Card and '**EMI'** for EMI, 'CLEMI' for Cardless EMI
2)	bankcode (**Mandatory**)	Each payment option is identified with a unique bank code at PayU. You would need to post this parameter with the corresponding payment option's bankcode value in it. For example, for ICICI Net Banking, the value of bankcode parameter value should be ICIB. For detailed list of bank codes, please contact PayU team
3)	ccnum (**Mandatory**)	This parameter must contain the card (credit/debit) number entered by the customer for the transaction.
4)	ccname (**Mandatory**)	This parameter must contain the name on card – as entered by the customerfor the transaction.
5)	ccvv (**Mandatory**)	This parameter must contain the cvv number of the card – as entered by the customer for the transaction.
6)	ccexpmon (**Mandatory**)	This parameter must contain the card's expiry month - as entered by the customer for the transaction. Please make sure that this is always in 2 digits. For months 1-9, this parameter must be appended with 0 – like 01, 02…09 For months 10-12, this parameter must not be appended – It should be 10, 11 and 12 respectively.
7)	ccexpyr (**Mandatory**)	The customer must contain the card's expiry year – as entered by the customer for the transaction. It must be of 4 digits. For example - 2017, 2029 etc.
8)	Consent_shared (Mandatory)	This is applicable for Cardless EMI transactions only. Values can be 0 or 1 based on whether the merchant has taken customer's consent to share data or not.

Table 2: Additional Parameters for Seamless Mode

Additional Charges – Convenience Fee Model (To be used only if recommended by Account Manager at PayU)

There are 2 different methods to implement Additional Charges on PayU.

Method 1: Enabled from backend at PayU

The merchant would be posting the **transaction amount** of the product in the transaction request.

1) Once the customer lands on PayU payment page and clicks on '**Pay Now**' option, the **additional amount** would be added to the amount of the product by PayU (based upon the TDR values) and the **total amount** would be passed on to the bank's page while re-directing.

2) After PayU receives the status of transaction from the bank, it sends the response of back to the merchant. In this response, the **amount** and **additional amount** can be differentiated with the below parameters.

   - Original Transaction Amount - **amount**
   - Additional Amount - **additionalCharges**

3) Once you receive the response from PayU, you need to check for reverse hash. If you are verifying the reverse hash at your end (which is strictly recommended to avoid any tamper cases), its formula will also change in case additionalCharges value issent. Here, if the additionalCharges parameter is posted in the transaction response, then hash formula is:
   sha512**(additionalCharges|SALT|status||||||udf5|udf4|udf3|udf2|udf1|email|firstname|productinfo|amount|txnid|key)**

4) If additionalCharges parameter is not posted in the transaction response, then hash formula is the generic reverse hash formula:
sha512(**SALT|status||||||udf5|udf4|udf3|udf2|udf1|email|firstname|productinfo|amount|txnid|key)**

Method 2: Merchant Calculates and Posts Additional Charges to PayU

1) The merchant would be posting both the transaction amount and additional charges in the transaction request. The parameters used for these are **amount** and **additional_charges** respectively. The way to pass the additional_charges parameter is as below:

<bankcode1> :< additional charge value>, < bankcode2> :< additional charge value>

Example: **CC:12,AMEX:19,SBIB:98,DINR:2,DC:25,NB:55**

2) In this method of applying additional charges, hash sequence would be affected for both Pre-Transaction and Post-Transaction.

Pre-Transaction hash sequence:

Merchant needs to form the below hash sequence before posting the transaction to PayU:

sha512**(key|txnid|amount|productinfo|firstname|email|udf1|udf2|udf3|udf4|udf5||||||SALT|additional_charges)**

Where additional_charges value would be same as the value posted in transaction request. For example, **CC:12,AMEX:19,SBIB:98,DINR:2,DC:25,NB:55**

3) Now, once the transaction request hits PayU server and re-direction happens, the customer lands upon PayU payment page. Here, depending on the payment option selection by the customer, the additional charge value would be added to transaction amount. For example, for the above example, if the customer selects Credit Card, Rs 12 would be added to the transaction amount. If the customer selects AMEX option, Rs 19 would be added to the transaction amount. For SBI Net Banking, Rs 98 would be added to the transaction amount and so on. Please note that the additional charges would be added only once the customer clicks on 'Pay Now' option.

4) When PayU receives the response from Bank, a POST Response is sent to the merchant. Here also, the hash sequence needs to be changed.

Post-Transaction hash sequence:

Merchant needs to form the below hash sequence and verify it with the hash sent by PayU in the Post Response:

sha512**(additionalCharges|SALT|status||||||udf5|udf4|udf3|udf2|udf1|email|firstname|productinfo|amount|txnid|key)**

Where, **additionalCharges** value must be same as the value Posted from PayU to the merchant in the response.

5) This hash value must be compared with the hash value posted by PayU to the merchant. If both match, then only the order should be processed. If they don't match, then the transaction has been tampered with by the user and hence should not be processed further.

Important Things to remember: Characters allowed for parameters

- For parameters address1, address2, city, state, country, product info, email, and phone following characters are allowed:
- Characters: A to Z, a to z, 0 to 9
- -(Minus)
- _ (Underscore)
- @ (At the Rate)
- / (Slash)
- (Space)
- . (Dot)

If the merchant sends any other special characters then they will be automatically removed. The address parameter will consider only first 100 characters.

Formula for hash (checksum) before transaction

This has already been covered in the description of **hash** in the table containing the POST Parameters above.

Formula for hash (checksum) after transaction

This time the variables are in reverse order and status variable is added between salt and udf1.

sha512(SALT|status||||||udf5|udf4|udf3|udf2|udf1|email|firstname|productinfo|amount|txnid|key)

Please Note:

It is absolutely mandatory that the hash (or checksum) is computed again after you receive response from PayU and compare it with request and post back parameters. This will protect you from any tampering by the user and help in ensuring a safe and secure transaction experience. It is also a mandate that you secure your integration with PayU by implementing Verify webservice and Webhook/callback as a secondary confirmation of transaction response. Detailed integration process of Verify webservice and webhook and be found further in this document.

Please note that PayU will not be responsible for any security breaches (including any data breaches) that may occur due to non-implementation of the aforesaid security features at your end or any loss or damage arising therefrom, to you or to any third party.

Hash (Checksum) Algorithm Example codes

The Checksum algorithm used is SHA512 which is globally well known algorithm. To need help with implementation, feel free to call us, mail us or use Google to find the desired function library for your implementation. Some example codes are also mentioned below:

For PHP

Example code:

```
$output = hash ("sha512", $text);
```

For .NET

Link: http://msdn.microsoft.com/en- us/library/system.security.cryptography.sha512.aspx

Example code:

```
byte[] data = new byte[DATA_SIZE];
        byte[] result;
        SHA512 shaM = new SHA512Managed();
        result = shaM.ComputeHash(data);
```

For JSP

Example code:

```
import java.io.FileInputStream;
        import java.security.MessageDigest;
public class SHACheckSumExample
{
        public static void main(String[] args)throws Exception
                {
                        MessageDigest md = MessageDigest.getInstance("SHA-512");
                                FileInputStream fis = new
FileInputStream("c:\\loging.log");                      byte[] dataBytes = new
byte[1024];                                             int nread = 0;
                                                        while ((nread =
fis.read(dataBytes)) != -1)                                     {

md.update(dataBytes, 0, nread);                                                 };

byte[] mdbytes = md.digest();
//convert the byte to hex format method
StringBuffer sb = new StringBuffer();
        for (int i = 0; i < mdbytes.length; i++)
                {
                        sb.append(Integer.toString((mdbytes[i] & 0xff) + 0x100,
                                16).substring(1));
                        }
                        System.out.println("Hex format : " + sb.toString());
                        //convert the byte to hex format method 2
                        StringBuffer hexString = new StringBuffer();
                                for (int i=0;i<mdbytes.length;i++)
                                hexString.append(Integer.toHexString(0xFF               &
mdbytes[i]));                           }
                                System.out.println("Hex       format       :       "       +
hexString.toString());                          }
```

Response Parameters posted by PayU to Merchant in redirection

Sr.No	Variable Name	Description

<table>
<tr><td>1</td><td>mihpayid</td><td>It is a unique reference number created for each transaction at PayU's end. For every new transaction request that hits PayU's server (coming from any of our merchants), a unique reference ID is created and it is known as mihpayid (or PayU ID)</td></tr>
<tr><td>2</td><td>mode</td><td>This parameter describes the payment category by which the transaction was completed/attempted by the customer. The values are mentioned below:
<table>
<tr><th>Category used by Customer</th><th>Value of Mode Parameter</th></tr>
<tr><td>Credit Card</td><td>CC</td></tr>
<tr><td>Debit Card</td><td>DC</td></tr>
<tr><td>NetBanking</td><td>NB</td></tr>
<tr><td>Cash Card</td><td>CASH</td></tr>
<tr><td>EMI</td><td>EMI</td></tr>
<tr><td>IVR</td><td>IVR</td></tr>
<tr><td>Cash On Delivery</td><td>COD</td></tr>
<tr><td>Cardless EMI</td><td>CLEMI</td></tr>
</table></td></tr>
<tr><td>3</td><td>status</td><td>This parameter gives the status of the transaction. Hence, the value of this parameter depends on whether the transaction was successful or not. You must map the order status using this parameter only. The values are as below:

If the transaction is successful, the value of 'status' parameter would be 'success'.

The value of 'status' as 'failure' or 'pending' must be treated as a failed transaction only.</td></tr>
<tr><td>4</td><td>key</td><td>This parameter would contain the merchant key for the merchant's account at PayU. It would be the same as the key used while the transaction request is being posted from merchant's end to PayU.</td></tr>
<tr><td>5</td><td>txnid</td><td>This parameter would contain the transaction ID value posted by the merchant during the transaction request.</td></tr>
<tr><td>6</td><td>amount</td><td>This parameter would contain the original amount which was sent in the transaction request by the merchant.</td></tr>
<tr><td>7</td><td>discount</td><td>This parameter would contain the discount given to user - based on the type of offer applied by the merchant.</td></tr>
<tr><td>8</td><td>offer</td><td>This parameter would contain the offer key which was sent in the transaction request by the merchant.</td></tr>
<tr><td>9</td><td>productinfo</td><td>This parameter would contain the same value of productinfo which was sent in the transaction request from merchant's end to PayU</td></tr>
<tr><td>10</td><td>firstname</td><td>This parameter would contain the same value of firstname which was sent in the transaction request from merchant's end to PayU</td></tr>
</table>

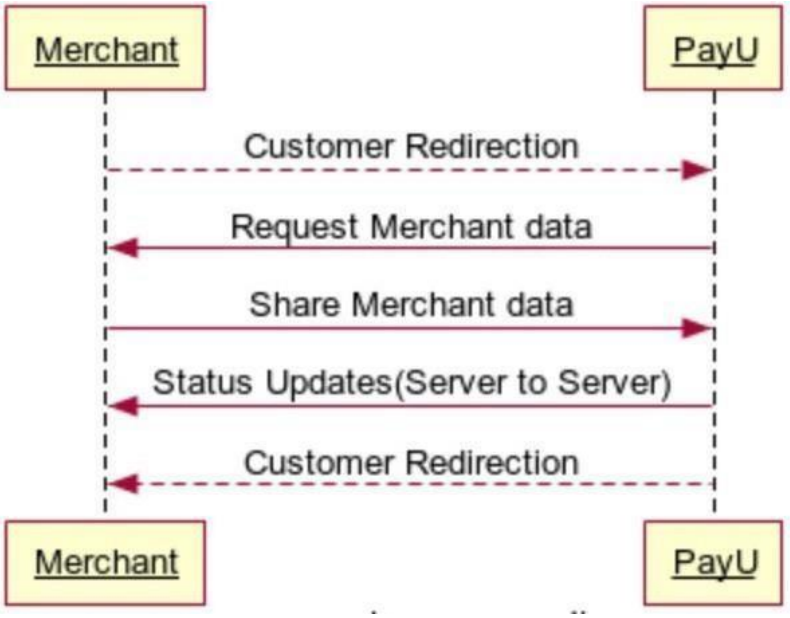
11	lastname	This parameter would contain the same value of **lastname** which was sent in the transaction request from merchant's end to PayU
12	address1	This parameter would contain the same value of **address1** which was sent in the transaction request from merchant's end to PayU
13	address2	This parameter would contain the same value of **address2** which was sent in the transaction request from merchant's end to PayU
14	city	This parameter would contain the same value of **city** which was sent in the transaction request from merchant's end to PayU
15	state	This parameter would contain the same value of **state** which was sent in the transaction request from merchant's end to PayU
16	country	This parameter would contain the same value of **country** which was sent in the transaction request from merchant's end to PayU
17	zipcode	This parameter would contain the same value of **zipcode** which was sent in the transaction request from merchant's end to PayU
18	email	This parameter would contain the same value of **email** which was sent in the transaction request from merchant's end to PayU
19	phone	This parameter would contain the same value of **phone** which was sent in the transaction request from merchant's end to PayU
20	udf1	This parameter would contain the same value of **udf1** which was sent in the transaction request from merchant's end to PayU
21	udf2	This parameter would contain the same value of **udf2** which was sent in the transaction request from merchant's end to PayU
22	udf3	This parameter would contain the same value of **udf3** which was sent in the transaction request from merchant's end to PayU
23	udf4	This parameter would contain the same value of **udf4** which was sent in the transaction request from merchant's end to PayU
24	udf5	This parameter would contain the same value of **udf5** which was sent in the transaction request from merchant's end to PayU

25	hash	This parameter is absolutely crucial and is similar to the hash parameter used in the transaction request send by the merchant to PayU. PayU calculates the hash using a string of other parameters and returns to the merchant. The merchant must verify the hash and then only mark a transaction as success/failure. This is to make sure that the transaction hasn't been tampered with. The calculation is as below: **sha512(SALT|status|||||udf5|udf4|udf3|udf2|udf1|email|firstname|productinfo|amount|txnid|key)** The handling of udf1 – udf5 parameters remains similar to the hash calculation when the merchant sends it in the transaction request to PayU. If any of the udf (udf1-udf5) was posted in the transaction request it must be taken in hash calculation also. If none of the udf parameters were posted in the transaction request, they should be left empty in the hash calculation too.
26	error	For the failed transactions, this parameter provides the reason of failure. Please note that the reason of failure depends upon the error codes provided by different banks and hence the detailing of error reason may differ from one transaction to another. The merchant can use this parameter to retrieve the reason of failure for a particular transaction.
27	bankcode	This parameter would contain the code indicating the payment option used for the transaction. For example, in Debit Card mode, there are different options like Visa Debit Card, Mastercard, Maestro etc. For each option, a unique bankcode exists. It would be returned in this bankcode parameter. For example, Visa Debit Card – **VISA,** Master Debit Card – **MAST.**
28	PG_TYPE	This parameter gives information on the payment gateway used for the transaction. For example, if SBI PG was used, it would contain the value **SBIPG.** If SBI Netbanking was used for the transaction, the value of PG_TYPE would be **SBINB**. Similarly, it would have a unique value for all different type of payment gateways.
29	bank_ref_num	For each **successful** transaction – this parameter would contain the **bank reference number** generated by the bank.
30	shipping_firstname	This parameter would contain the same value of **shipping_firstname** which was sent in the transaction request from merchant's end to PayU

31	shipping_lastname	This parameter would contain the same value of **shipping_lastname** which was sent in the transaction request from merchant's end to PayU
32	shipping_address1	This parameter would contain the same value of **shipping_address1** which was sent in the transaction request from merchant's end to PayU
33	shipping_address2	This parameter would contain the same value of **shipping_address2** which was sent in the transaction request from merchant's end to PayU
34	shipping_city	This parameter would contain the same value of **shipping_city** which was sent in the transaction request from merchant's end to PayU
35	shipping_state	This parameter would contain the same value of **shipping_state** which was sent in the transaction request from merchant's end to PayU
36	shipping_country	This parameter would contain the same value of **shipping_country** which was sent in the transaction request from merchant's end to PayU
37	shipping_zipcode	This parameter would contain the same value of **shipping_zipcode** which was sent in the transaction request from merchant's end to PayU
38	shipping_phone	This parameter would contain the same value of **shipping_phone** which was sent in the transaction request from merchant's end to PayU
39	unmappedstatus	This parameter contains the status of a transaction as per the interna database of PayU. PayU's system has several intermediate status which are used for tracking various activities internal to the system. Hence, this status contains intermediate states of a transaction also - and hence is known as **unmappedstatus**. For example: dropped/bounced/captured/auth/failed/usercancelled/pending

Table 3: Response parameters from PayU to Merchant

Sequence Diagram for Cardless EMI



Cardless EMI Additional Response(Server to Server)

Since Cardless EMI application is longer than usual bank transactions, it is recommended to receive live updates from PayU for the application.
If Merchant wants to receive server to server live updates from PayU for all Cardless EMI transactions, it can be implemented in following ways:

PayU will also notify merchant server to server as additional response along with above status update for all notifications received. Following values will be posted in notification update to merchant:

- txnid – Transaction Id shared by merchant
- payuid – PayU Id generated at payu's end for this transaction
- payustatus – Transaction status at payu's end
- status – Further details of the payustatus

Sample response:

payuid=700010006174603&status=IN_PROGRESS&txnid=5467c0b5ea59b5d45088&payustatus=in progress

Here is the complete list of status and mapping:

STATUS	PURPOSE OF THE STATE	PayU Status

OPEN	Thisstateindicatesthatanapplicationhasbeen created by PayU in the system.	In Progress
IN_PROGRESS	Right after OPEN, the state of the application moves into in this state. This state is different from the state of the application in the PLC.	In Progress
TIMED_OUT	This state indicates that the application timed out on the LC. The timeout duration would be default be equal to 48 hours.	Failed
CANCELLED	This state indicates that the application has been cancelled. Reason_code would capture the reason of cancellation.	Failed
UNDERWRITING	This state indicates that the application is currently submitted and being scored by underwriting.	In Progress
UNDERWRITING_PENDING	This state indicates that the application has moved into review because of - 1. An underwriting error 2. Timeout on underwriting side 3. Timeout on the LAS side 4. Non-availability of certain services.	In Progress
UNDERWRITING_ACCEPTED	This state indicates that the customer has been accepted by Underwriting. If there is a difference payment required, it would already be added as part of ATP conditions.	In Progress

OFFER_ACCEPTED	The state indicates that the customer has clicked on one of the offers and moved forward in the lead cycle process to the eKYC step	In Progress
REJECTED	This state indicates that the customer has been rejected by Underwriting. The reason ofrejections would be specified in the reason_codes attached to the state change.	Failed
APPROVED_IN_PRINCIPLE	This state indicates that the customer has signed the contract and finishedthe LC. If no ATP conditions, AIP would be followed directlybyAPPROVAL_TO_PAYOUT otherwise would stay as APPROVAL_IN_PRINCIPLE.	In Progress
IN_PROGRESS_POST_LEAD_CYCLE	This state indicates that thecustomer has initiated the PLC (reached the landing page for PLC).	In Progress
APPROVED_TO_PAYOUT	This state can be reached in two ways - 1. There were no ATP Conditions. In this case, ATP is followed directly by AIP. 2. The Service Center Agent approves the application and application moves from IN_PROGRESS_POST_LEAD_CYCLE to this state.	Captured
TIMED_OUT_POST_LEAD_CYCLE	This state indicates that the Partner Hold Time is reached but application did not get to the ATP state. This would make the application expired and inactive.	Failed

CANCELLED_POST_LEAD_CYCLE	This state indicates that the application was cancelled by the Service Center.	Failed
REJECTED_POST_LEAD_CYCLE	This state indicates that the application was marked rejected by the Service Center.	Failed
FRAUD_SUSPECTED_POST_LEAD_CYCLE	This state indicates that the application has been marked as a suspected fraud application.	In Progress
PAYOUT_STARTED	This state is reached after the ATP state. Loan Application System takes the necessary actions inside Mambu and changes to this state. The loan account is made Active in Mambu and the interest starts getting accrued. Based on this state notification, PayU asks the merchant to ship the products and initiates the transfer of loan amount to the merchant.	Captured
PAYOUT_COMPLETED	This state indicates that the merchant has been successfully paid out. This state is reached once the Loan Application System reads the MT files, confirms the transfer of payment to the merchant.	Captured
PAYOUT_ERROR	This state indicates the the status PAYOUT_STARTED has not moved into PAYOUT_COMPLETED after a certain amount of time (X days).	Captured

	From this state, the system should move into PAYOUT_COMPLETED, PAYOUT_STARTED or PAYOUT_CANCELLED.	
PAYOUT_CANCELLED	This state indicates that the payout was not processedbecause PayU / merchant refused to process this particular payout. The agent andthe reason code would show upin the respective fields.	Captured

Whitelisting Required
Whitelisting is required at both merchant's and PayU's end to establish this connection.

a) Merchant needs to whitelist below IP address at their firewall side:

For production-

180.179.174.1

180.179.174.2

For integration

180.179.100.1

b) PayU needs to whitelist merchant server side IP Address–which merchant would be providing to PayU. It will be two IP addresses: one for Option 1 and another for Option 2. Both IP addresses could be same also as per merchant's convenience.

URL to be shared for this response should be less than 512 characters.

Data Sharing between PayU and Merchant for Cardless EMI

For Cardless EMI option, PayU will need further information about the customer from merchant. Merchant will share a trigger point with PayU at the time of onboarding to share this data at the time of transaction. Also, inform PayU so that merchant data sharing at PayU's end can be enabled.

1. PayU hits the merchant's trigger point with following inputs whenever data is needed:
    a. Txn ID – Transaction Id received from merchant
    b. PayU ID – PayU's transaction id
    c. PayU Status – Status in payu's system
    d. Status – "DATA_REQUEST" hardcoded

Sample Value:
payuid=700010006174603&status=DATA_REQUEST&txnid=5467c0b5ea59b5d45088&payustatus=in progress

2. In response, merchant will share data with PayU using ‘ Post Customer Transaction History Data’ under SELLERSERVICE at this link: https://developer.payubiz.in/v2/documentation/index.html
3. For authentication, please refer to the section ‘AUTHENTICATION’. Same key andsalt will be used.

Sample data


```
{
  "account_id":"iwcdiu",
  "payment_id":"iib8y",
  "reference_id":"WEBIN/100819507/1",
  "data":{
    "first_name": "David",
      "last_name": "Smith",
      "email": "david@gmail.com",
      "phone": "+919332456789",
      "transaction" :[ {
       "delivery_details":{
       "address": "43, ABC Apartments, Xyz Street",
       "city": "New Delhi",
       "zip": 110024,
       "state": "Delhi"
       },
      "billing_details":{
       "address": "House No. 214, Pqr Street",
       "city": "Delhi",
       "zip": 110203,
       "state": "Delhi"
      },
       "basket": [ {
            "name": "Bass Speaker",
            "code": "SBS12",
            "description": "Bose Bass Speaker as part of 5.1 or 7.1 Surround Sound",
            "quantity": 1,
            "price": "",
            "added_on": "2017-11-01T15:00:00+05:30",
            "removed_on": ""
        },
        {
            "name": "Wireless Speaker Module",
            "code": "WS003",
            "description": "Boat Wireless Speaker",
```

```
            "quantity": 1,
            "price": 1300,
            "added_on": "2017-11-01T15:04:30+05:30",
            "removed_on": "2017-11-01T15:05:00+05:30"
        }
       ],
       "purchase":{
            "added_on": "2017-11-01T15:10:00+05:30",
            "number_of_items": 1,
            "total_cost": 33500,
            "tax": 6600,
            "shipping_cost": "",
            "payment_method": "Credit Card",
            "reverse_amount": 33000,
            "number_of_items_returned": 1,
            "total_cost_returned": 33500
         },
       "visit": [{
          "begin_timestamp": "1509548400",
          "end_timestamp": "1509552000",
          "url": "http://www.amazon.in/"
         }],
       "device": [{
          "device_fingerprint": "string",
          "user_agent": "string"
       }]
  }]
  }
}
```


Enabling HDFC Debit Card, Bajaj Finserv, Axis Debit Card and Zest Money EMIs

For all these EMIs, **merchant will have to display a button for each EMI option on their payment page** and then enforce, by passing the different combination of values in "enforce_paymethod" as per the table given below, the one chosen by the customer while sending the transaction request by PayU. No additional information needs to be posted in the transaction request.

In this phase, merchant who are using PayU checkout page for collecting payment option related information for rest of their payment options will not be able to avail these EMI options without any changes. If any such merchant wants to avail any of these EMI options then they will have to display different buttons for different EMI options on their page and use the enforce parameter method, as given above.

EMI Option	**Value of enforce_paymethod**	**Eligibility Amount range**
HDFC Debit Card	HDFCD06|HDFCD09|HDFCD12|HDFCD18	5,00,000>=Transaction amount>=5,000

EMI		
Bajaj Finserv EMI	BAJFIN03|BAJFIN03|BAJFIN06|BAJFIN09|BAJFIN12	Transaction amount>=4,499
Zest Money EMI	ZESTMON	3,00,000>=Transaction amount>=1,000
Axis Debit Card EMI	AXISD03|AXISD06|AXISD09|AXISD12|AXISD18|AXISD24	1,00,000>=Transaction amount>=5,000

EMI option specific handling/information-

For Axis Debit Card,

Single item should be there in the cart since partial refunds are not allowed on this EMI option.

For HDFC Debit Card EMI

Merchant will have to call Proof of Delivery API, details given on page number 73, as soon as the services/goods has been delivered to the customer.

The maximum time allowed will be 15 days before we notify your team of transactions where we haven't received proof of delivery and it might lead to EMI option deactivation.

For Bajaj Finserv EMI

Merchant will have to call Proof of Delivery API, , details given on page number 73, as soon as the services/goods has been delivered to the customer.

The maximum time allowed will be 15 days before we notify your team of transactions where we haven't received proof of delivery and it might lead to EMI option deactivation.

Also, since decimal values are not supported in Bajaj Finserv system, we round up/down the amount depending whether it is sale request or refund request.

This will be by default No Cost EMI from customer standpoint so the net amount customer will be charged by Bajaj Finserv will be amount sent by bank only.

For Zest Money EMI

Merchants will not be able to enforce specific tenures since tenures are known once customer has been authenticated.

It is recommended that merchant passes the customer mobile number in "phone" parameter while sending the transaction request to PayU so that the customer doesn't have to enter the

mobile number on PayU checkout page, customer will have the option to edit the mobile number in case she wishes to change the mobile number.

Shopping Cart Integration Kits

Shopping Cart Kits currently available with PayU are:

- Interspire
- Opencart
- Jhoomla Virtue Mart
- Magento
- Prestashop
- Tomatocart
- Zencart
- CS-Cart
- OSCommerce
- Wordpress ecommerce
- WordPress Woo-commerce
- Wordpress - Paid Membership Pro
- Drupal Ubercart
- X-Cart

Platform based Integration kits

PayU Integration Kits are available in the following environments:

- PHP
- JSP
- .NET
- ROR

NOTE: *Kindly contact your account manager in case you are using some other shopping cart and want us to develop a kit for the same.*

NOTE: In case of any integration queries, please drop a mail at tech@payu.in

SECTION II: WEB SERVICES – APIs

PayU has made many web-services for you. Each web-service has a specific function and hence can be used to automate different features. The basic format and execution of all web- services remains the same. Each web-service is a server-to-server call from your server to PayU's server. Web services can be accessed by making a **server to server call** on the below mentioned PayU URLs:

URL to be used:

For Production Server:

https://info.payu.in/merchant/postservice.php?form=1
(form=1 shall return output in array form)

https://info.payu.in/merchant/postservice.php?form=2
(form=2 shall return output in json form)

For Test Server:

https://test.payu.in/merchant/postservice.php?form=1
(form=1 shall returns output in array form)

https://test.payu.in/merchant/postservice.php?form=2
(form=2 shall return output in json form)

Web Service Request Format:

The input request format for executing a web-service is as follows:

Mandatory Input Parameters

Parameter	Description	Sample Value
key	Merchant key provided by PayU. Please refer to the first entry in the Post Parameters table for detailed description of this parameter	Ibibo
command	This parameter must have **name of the web-service.** The names and definitions of all web-services will be covered later in detail	verify_payment
hash	This parameter **must** contain the hash value to be calculated a your end. The string used for calculating the hash is mentioned below: **sha512(key|command|var1|salt)** sha512 is the encryption method used here.	ajh84ba8abvav
var1, var2, var3 ... up to var15	These are the variable parameters, whose values depend on the particular web-service. The definition of these parameters will be covered in the (Read command explanations mentionedlater for this)	Abc

Web Service Response Format

Web Service API responds back in PHP serialized string by default.

Parameter	Description	Sample Value
status	Status of web service call	0 if web service call failed 1 if web service call succeeded
msg	Reason String	Parameter missing or token is empty or amount is empty or transaction not exists
transaction_details	May or may not be returned depending on the web service being called	mihpayid,request_id, bank_ref_num etc
request_id	PayU Request ID for a request in a Transaction. eg. A transaction can have a refund request.	7800456
bank_ref_num	Bank Reference Number. If bank provides after a successful action.	204519474956

LIST OF APIs AND THEIR DESCRIPTION

1) verify_payment

This web-service is used to reconcile the transaction with PayU. When we **post back the final response** to you (merchant), we provide a list of parameters (including the status of the transaction – For example, **success, failed** etc). On a few occasions, the transaction response is initiated from our end, but it doesn't reach you due to network issues or user activity (like refreshing the browser etc).

This API is helpful to tackle such cases - where you can execute it to get the status of the transaction. Since you already have the **txnID (Order ID generated at your end)** value for such cases, you simply need to execute the verify_payment API with the necessary input parameters. The output would return you the transaction status and various other parameters also.

Another usage of this API is to provide an additional layer of verification of the transaction (in addition to checksum). You can verify the status and other parameters received in the post response via this API.

We strongly recommend that this API is used to reconcile with PayU's database once you receive the response. This will protect you from any tampering by the user and helpin ensuring safe and secure transaction experience.

The return parameters are MIHPayID, Amount, Discount, Mode and Status of transaction.

Input Variables Description:

Parameter	Description	Sample Value
var1	In this parameter, you can put all the txnid(Your transaction ID/order ID) values in a pipe separated form.	100123|100124|100125|100126

Web Service Responses:

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => 1 out of 1 Transactions Fetched Successfully
    [transaction_details] => Array
        (
            [100123] => Array
                (
                    [mihpayid] => 403993715511385302
                    [request_id] =>
                    [bank_ref_num] => 3465241441650741
                    [amt] => 63050.00
                    [txnid] => 100123
                    [additional_charges] => 0.00
                    [productinfo] => book
                    [firstname] => uday
                    [bankcode] => CC
                    [udf1] =>
                    [udf3] =>
                    [udf4] =>
                    [udf5] =>
                    [field9] => SUCCESS
                    [error_code] => E000
                    [error_Message] => NO ERROR
                    [net_amount_debit] => 63050
                    [disc] => 0.00
                    [mode] => CC
                    [PG_TYPE] => HDFCPG
                    [card_no] => 512345XXXXXX2346
                    [name_on_card] => shop
                    [udf2] =>
                    [addedon] => 2015-03-15 16:44:21
                    [status] => success
                    [unmappedstatus] => captured

                )
        )
)
```

- **If txnID not found**

```
Array
(
    [status] => 0
    [msg] => 0 out of 1 Transactions Fetched Successfully
    [transaction_details] => Array
        (
            [ecc5tashi] => Array
                (
                    [mihpayid] => Not Found
                    [status] => Not Found
                )
        )
)
```

2) check_payment

This API functions similar to verify_payment API mentioned above. The only difference is that the input parameter in this API is the PayUID (MihpayID) generated at PayU's end

whereas the input parameter in verify_payment API is the TxnID (Transaction ID generated at your end). It returns all the parameters for a given transaction.

Input Variables Description:

Parameter	Description	Sample Value
var1	In this parameter, you need to pass the Payu id (mihpayid) of the transaction.	8000123

Web Service Responses:

- **If mihpayid is missing**

```
Array
(
    [status] => 0
    [msg] => Parameter missing
)
```

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => Transaction Fetched Successfully
    [transaction_details] => Array
        (
            [request_id] => 124755210
            [bank_ref_num] => 3465241441650741
            [net_amount] => 63050.00
            [mihpayid] => 403993715511385302
            [amt] => 63050.00
            [disc] => 0.00
            [mode] => CC
            [txnid] => ecc5tashiv
            [amount] => 63050.00
            [amount_paid] => 63050.00
            [discount] => 0.00
            [additional_charges] => 0.00
            [udf1] =>
            [udf2] =>
            [udf3] =>
            [udf4] =>
            [udf5] =>
            [field1] => 507442425118
            [field2] => 999999
            [field3] => 3465241441650741
            [field4] => -1
            [field5] =>
            [field6] =>
            [field7] =>
            [field8] =>
            [field9] => SUCCESS
            [status] => success
            [net_amount_debit] => 63050
            [unmappedstatus] => captured
            [firstname] => uday
            [bankcode] => CC
```

```
            [productinfo] => book
            [name_on_card] => shop
            [card_no] => 512345XXXXXX2346
            [PG_TYPE] => HDFCPG
        )
)
```

3) cancel_refund_transaction

This command can be used for 2 different purposes:

- To cancel a transaction which is in '**auth'** state at the moment
- To refund a transaction which is in '**captured'** state at the moment

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu ID (mihpayid) of transaction	8000123
var2	This parameter should contain the Token ID (unique token from merchant) for the refund request. Token ID has to be generated at your end for each new refund request. It is an identifier for each new refund request which can be used for tracking it. It must be unique for every new refund request generated – otherwise the refund request would not be generated successfully. Token ID length should not be greater than **23** characters	7800456
var3	**For captured transaction:** This parameter should contain the amount which needs to be refunded. Please note that both partial and full refunds are allowed. Hence, for partial refund, this var3 value would be less than the amount with which the transaction was made. For full refund, var3 value would be equal to the amount with which the transaction was made. **For pre-auth transaction:** If the transaction is in pre-auth state currently, then only a **full cancellation** is allowed. The amount must be same as the auth amount. Partial amount would not be allowed.	500

Web Service Responses:

- **if token is missing**

```
Array
(
    [status] => 0
    [msg] => token is empty
)
```

- **if amount is missing**

```
Array
```

```
(
    [status] => 0
    [msg] => amount is empty
)
```

- **if transaction isn't found**

```
Array
(
    [status] => 0
    [msg] => transaction not exists
)
```

- **on successful processing at our end**

```
Array
(
    [status] => 1
    [msg] => Cancel Request Queued
    [txn_update_id] => Request ID
    [bank_ref_num] => Bank Reference Number
    [mihpayid] => PayU Transaction id
)
```

- **on successful processing on our end for captured transactions**

```
Array
(
    [status] => 1
    [msg] => Refund Request Queued
    [request_id] => Request ID
    [bank_ref_num] => Bank Reference Number
    [mihpayid] => PayU Transaction id
)
```

- **if failed to refund**

```
Array
(
    [status] => 0
    [msg] => Refund request failed
)
```

- **if capture is done on the same day**

```
Array
(
    [status] => 1
    [msg]=> Capture is done today, please check for refund status tomorrow
    [request_id] => Request ID
    [bank_ref_num] => Bank Reference Number
    [mihpayid] => PayU ID
)
```

- **if invalid token**

```
Array
(
    [status] => 0
    [msg] => token already used or request pending.
)
```

- **on successful processing at PayU end for** auth **transactions**

```
Array
(
    [status] => 1
    [msg] => Cancel Request Queued
    [txn_update_id] => Request ID
    [bank_ref_num] => Bank Reference Number
)
```

- **if failed to cancel a transaction**

```
Array
(
    [status] => 0
    [msg] => Cancel request failed
)
```

4) check_action_status (1ST Usage)

This API is used to check the status of refund/cancel requests. Whenever the cancel_refund_transaction API is executed successfully, a **Request ID** is returned in the output parameters for that particular request. In check_action_status API, you need to input this Request ID to get the current status of the request. The return parameters are MIHPayID, Amount, Discount, Mode and Status of transaction.

Input Variables Description:

Parameter	Description	Sample Value
var1	request_id	7800456

Web Service Responses:

- **if mihpayid is missing**

```
Array
(
    [status] => 0
    [msg] => Parameter missing
)
```

- **if mihpayid isn't found**

```
Array
(
    [status] => 0
    [msg] => 0 out of 1 Transactions Fetched Successfully
    [transaction_details] => Array
```

```
        (
            [1247498364] => No action status found
        )
)
```

- **if successfully fetched**

```
Array
(
    [status] => 1
    [msg] => 1 out of 1 Transactions Fetched Successfully
    [transaction_details] => Array
        (
            [124749836] => Array
                (
                    [124749836] => Array
                        (
                            [mihpayid] => 403993715511370816
                            [bank_ref_num] =>
                            [request_id] => 124749836
                            [amt] => 10.00
                            [mode] => DC
                            [action] => refund
                            [token] => recon_40399371551137081
                            [status] => failure
                            [bank_arn] =>
                            [settlement_id] =>
                            [amount_settled] => -10.00
                            [UTR_no] =>
                            [value_date] =>
                        )
                )
        )
)
```

5) check_action_status (2nd Usage)

This command has a second usage also. For a particular PayUID, it returns the status of all requests (capture/refund/cancel).

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu ID (mihpayid) of transaction	8000123
var2	String Payuid i.e. **'payuid'**	payuid

- **If successfully fetched**

You will get both 1) Transaction success information and 2) Refund information as well

```
Array
(
    [status] => 1
    [msg] => 1 out of 1 Transactions Fetched Successfully
```

```
    [transaction_details] => Array
        (
            [403993715510993714] => Array
                (
                    [124508550] => Array
                        (
                            [mihpayid] => 403993715510993714
                            [bank_ref_num] => 114952
                            [request_id] => 124508550
                            [amt] => 1.00
                            [mode] => CC
                            [action] => auth
                            [token]  =>
                            [status] => SUCCESS
                            [bank_arn] =>
                            [settlement_id] =>
                            [amount_settled] => 1.00
                            [UTR_no]  =>
                            [value_date] =>
                        )

                    [124508552] => Array
                        (
                            [mihpayid] => 403993715510993714
                            [bank_ref_num] =>
                            [request_id] => 124508552
                            [amt] => 1.00
                            [mode] => CC
                            [action] => capture
                            [token] => 1422619587
                            [status] => failure
                            [bank_arn] =>
                            [settlement_id] =>
                            [amount_settled] => 1.00
                            [UTR_no]  =>
                            [value_date] =>
                        )

                    [124538030] => Array
                        (
                            [mihpayid] => 403993715510993714
                            [bank_ref_num] =>
                            [request_id] => 124538030
                            [amt] => 1.00
                            [mode] => CC
                            [action] => capture
                            [token] => 1422619587
                            [status] => requested
                            [bank_arn] =>
                            [settlement_id] =>
                            [amount_settled] => 1.00
                            [UTR_no]  =>
                            [value_date] =>
                        )
                )
        )
)
```

6) getAllRefundsFromTxnIds

This command is used to retrieve status of all the refund requests fired for a particular Transaction ID. The output of this API provides the request ID, the PG used, the status of refund request and creation of refund date information.

Input Variables Description:

Parameter	Description	Sample Value
var1	In this parameter, you need to pass the Transaction ID (txnid) of the transaction.	8000123

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => Refunds fetched successfully.
    [Refund Details] => Array
        (
            [8000123] => Array
                (
                    [0] => Array
                        (
                            [PayuID] => 8000123
                            [RequestID] => 124748442
                            [RefundToken] => 2348596079
                            [PaymentGateway] => HDFCPG
                            [Amount] => 10.00
                            [Status] => failure
                            [RefundCreationDate] => 2015-03-13 19:01:55
                        )

                    [1] => Array
                        (
                            [PayuID] => 8000123
                            [RequestID] => 124748448
                            [RefundToken] => 2488596981
                            [PaymentGateway] => HDFCPG
                            [Amount] => 10.00
                            [Status] => success
                            [RefundCreationDate] => 2015-03-13 19:02:28
                        )

                    [2] => Array
                        (
                            [PayuID] => 8000123
                            [RequestID] => 124749836
                            [RefundToken] => 2423456782
                            [PaymentGateway] => HDFCPG
                            [Amount] => 14.00
                            [Status] => success
                            [RefundCreationDate] => 2015-03-14 01:13:25
                        )

                )

        )

)
```

- **If no refunds found**

```
Array
(
    [status] => 1
    [msg] => No Refunds Found for the transaction.
)
```

7) capture_transaction

This command is used to update the status of a transaction which is in auth (authorized) state at the moment. Please note that this API is applicable only for transactions in pre-auth status. Once the API is success, the transaction would be captured and settled to merchant.

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu ID (mihpayid) of transaction	8000123
var2	token ID(unique token from merchant)	7800456
var3	Amount to be captured. It can be a equal to or less than or more than auth amount to certain limit than the amount used in pre-auth transaction	50

Web Service Responses:

- **If token is missing**

```
Array
(
    [status] => 0
    [msg] => token is empty
)
```

- **If transaction isn't found**

```
Array
(
    [status] => 0
    [msg] => transaction not exists
)
```

- **On successful processing at our end**

```
Array
(
    [status] => 1
    [msg] => Capture Request Queued
    [request_id] => Request ID
    [bank_ref_num] => Bank Reference Number
)
```

- **If invalid token**

```
Array
(
    [status] => 0
    [msg] => token already used or request pending.
)
```

- **If failed to refund**

```
Array
(
    [status] => 0
    [msg] => Capture request failed
)
```

7) update_requests

This command is used to update a requested refund, cancel, or capture transaction. The return parameters are status and msg. For example, in case of COD transaction, if a refund is initiated its status goes to **'requested'** state. Once the refund is done, then its status can be changed to **'refund'** by calling this API.

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu id (mihpayid) of transaction	8000123
var2	Request ID (unique id given to merchant) provided when cancel_transaction or refund_transaction or capture_transaction was called)	7800456
var3	Bank Ref Id for the requested transaction	Abc123
var4	Amount of the requested transaction	5000
var5	Action (cancel/capture/refund)	Refund
var6	New Status to be set	Success/failure

Web Service Responses:

- **If bank_ref_no is missing**

```
Array
(
    [status] => 0
    [msg] => bank_ref_no is empty
)
```

- **If amount is missing**

```
Array
(
    [status] => 0
    [msg] => amount is empty
)
```

- **If transaction isn't found**

```
Array
(
    [status] => 0
    [msg] => transaction not exists
)
```

- **If action is not valid**

```
Array
(
    [status] => 0
    [msg] => action is not valid
)
```

- **If status is not correct**

```
Array
(
    [status] => 0
    [msg] => status is not correct
)
```

- **On success**

```
Array
(
    [status] => 1
    [msg] => Status updated to success.
)
```

- **On failure**

```
Array
(
    [status] => 0
    [msg] => Status could not be updated. Please verify the parameters.
)
```

8) cod_verify

This command is used to **verify** a COD request. When a transaction is successful through PayU, it is marked as **'in progress'** at that moment. The reason is that the money hasn't been received yet and hence we mark it in this intermediary state. Once you verify the transaction with the customer, you can execute this API to update the status in PayU Database from '**in progress**' to '**pending**'. The return parameters are status, message and transaction ID.

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu ID (mihpayid) of transaction	8000123
var2	Token ID(unique token from merchant)	7800456

var3	Amount	500

Web Service Responses:

- **If token is missing**

```
Array
(
    [status] => 0
    [msg] => token is empty
)
```

- **If amount is missing**

```
Array
(
    [status] => 0
    [msg] => amount is empty
)
```

- **If amount is invalid**

```
Array
(
    [status] => 0
    [msg] => Invalid amount
)
```

- **If transaction isn't found**

```
Array
(
    [status] => 0
    [msg] => transaction not exists
)
```

- **On successful processing at PayU end**

```
Array
(
    [status] => 1
    [msg] => Queued
    [transaction_id] => $mihpayid
)
```

- **If failed to verify a request**

```
Array
(
    [status] => 0
    [msg] => Failed
    [error_code] => $verifyReturn['status']
)
```

9) cod_cancel

This command is used to **cancel** a cod request. When a COD transaction is successful at PayU's end in real time, its status is marked as '**in progress'** at that moment. This API can beexecuted to change the transaction status from '**in progress'** to '**cancelled'** in the PayU database. It is suggested to execute this API only when you are sure you want to cancel the transaction. Updating this way in PayU Database would help you in tracking such orders for future purpose – through the merchant panel provided to you. The return parameters arestatus message and transaction ID.

Additional Variables Description:

Parameter	Description	Sample Value
var1	Payu ID (mihpayid) of transaction	8000123
var2	Token ID(unique token from merchant)	7800456
var3	Amount	500

Web Service Responses:

- **If token is missing**

```
Array
(
    [status] => 0
    [msg] => token is empty
)
```

- **If amount is missing**

```
Array
(
    [status] => 0
    [msg => amount is empty
)
```

- **If amount is invalid**

```
Array
(
    [status] => 0
    [msg] => Invalid amount
)
```

- **If transaction isn't found**

```
Array
(
    [status] => 0
    [msg] => transaction not exists
)
```

- **On successful processing at PayU end**

```
Array
(
    [status] => 1
    [msg] => Queued
    [transaction_id] => $mihpayid
)
```

- **If failed to cancel a request**

```
Array
(
    [status] => 0
    [msg] => Failed
    [error_code] => $cancelReturn['status']
)
```

10) cod_settled

This command is used to **settle** a COD request. cod_settled API should be executed on a transaction only when cod_verify has already been executed. cod_settled updates the transaction status from 'pending' to 'captured'. It is suggested, that you execute this API only when you are sure that money has been successfully received from the customer at your end. Doing it this way would ensure you can track such orders in the future through the merchant panel provided to you. The return parameters are status message and Transaction ID.

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu id (mihpayid) of transaction	8000123
var2	token ID(unique token from merchant)	7800456
var3	amount	500

Web Service Responses:

- **If token is missing**

```
Array
(
    [status] => 0
    [msg] => token is empty
)
```

- **If amount is missing**

```
Array
(
    [status] => 0
    [msg] => amount is empty
)
```

- **If amount is invalid**

```
Array
```

```
(
    [status] => 0
    [msg] => Invalid amount
)
```

- **If transaction isn't found**

```
Array
(
    [status] => 0
    [msg] => transaction not exists
)
```

- **On successful processing at PayU end**

```
Array
(
    [status] => 1
    [msg] => Queued
    [transaction_id] => $mihpayid
)
```

- **If failed to settled a request**

```
Array
(
    [status] => 0

    [msg] => Failed
    [error_code] => $settledReturn['status']
)
```

11) get_TDR

This command is used to get the TDR value of a transaction with PayU. It is a simple API for which you need to provide the PayU ID of the transaction as input and the TDR value is returned in the output.

Input Variables Description:

Parameter	Description	Sample Value
var1	Payu id (mihpayid) of transaction	8000123

Web Service Responses

- **If mihpayid is not found**

```
Array
(
    [status] => 0
    [msg] => Invalid PayU ID
)
```

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => Transaction Fetched Successfully
    [TDR_details] => Array
        (
            [TDR] => <Value>
        )
)
```

12) udf_update

This command is used to update the UDF1-UDF5 values of a transaction. UDFs are the user-defined fields which are posted from the merchant to PayU. This API is specifically used to update the values in these fields in PayU Database. The return parameters are the **updated UDF** values of transaction.

Input Variables Description:

Parameter	Description	Sample Value
var1	transaction ID(txnid)	7cf3f43146da5a319ccc
var2	udf1 of transaction	8000123
var3	udf2 of transaction	4334343
var4	udf3 of transaction	434343
var5	udf4 of transaction	Abcd123
var6	udf5 of transaction	Efgh1234

Web Service Responses

- **If transaction ID is empty**

```
Array
(
    [status] => 0
    [msg] => Parameter missing
)
```

- **If transaction ID is invalid**

```
Array
(
    [status] => 0
    [msg] => Invalid TXN ID
)
```

- **If successfully updated**

```
Array
```

```
(
    [status] => UDF values updated
    [transaction_id] => 7cf3f43146da5a319ccc
    [udf1] => 8000123
    [udf2] => 4334343
    [udf3] => 434343
    [udf4] => Abcd123
    [udf5] => Efgh1234
)
```

13) create_invoice

This API is provided to the merchant to create an email invoice for a customer and gives the merchant an option of sending the email invoice immediately to the customer or it can be automated to be sent later.

Input Variables Description:

Parameter	Sample Value
var1	{"**amount**":"10","**txnid**":"abaac3332","**productinfo**":"jnvjrenv","**firstname**":"test","**email**":"test@test.com","**phone**":"1234567890","**address1**":"testaddress","**city**":"test","**state**":"test","**country**":"test","**zipcode**":"122002","**template_id**":"14","**validation_period**":6,"**send_email_now**":"1"}

Here, the input var1 parameter has to be generated in the json string format mentioned in the sample value string above. This string shows each parameter and its corresponding value separated by the delimiter colon (:). The parameters are also separated by the comma delimiter (,)

Following is the description of the parameters in the above mentioned string:

Parameter	Description
amount **(Mandatory)**	Payment Amount
txnid **(Mandatory)**	Merchant generated transaction number which is used to track a particular order. (Must be unique every time if already successful, otherwise you get an error of duplicate transaction)
productinfo **(Mandatory)**	Product Description
firstname **(Mandatory)**	Self-Explanatory (only alphabets a-z are allowed)
email **(Mandatory)**	Self-explanatory
phone **(Mandatory)**	Self-explanatory (Numeric Value only)
address1	Self-Explanatory (Length of Address1 must not be more than 100 characters and the allowed characters are only) A TO Z, a to z, 0 to 9, @, - (Minus), _ (Underscore), / (Backslash), (Space), (Dot)
city	Self-explanatory (allowed characters are same as in address1)
state	Self-explanatory (allowed characters are same as in address1)
Country	Self-explanatory (allowed characters are same as in address1)
Zipcode	Self-explanatory (numeric value only)

template_id	Template ID to be provided in case of more than one email invoice templates. Merchant can decide which template to use and provide that particular template ID in this parameter
validation_period	Number of days for which the email invoice usage is valid (If this field is left empty, then default value will be taken as 7 days)
send_email_now	1 - If the merchant wants to automatically send the email invoice request to the customer at the time of creation of email invoice itself 0 - If the merchant doesn't want to send the email invoice request to the customer at the creation time itself. In this case, the email would be sent later automatically

Web Service Responses

- **If successfully executed**

```
Array
(
    [Transaction Id] => abaac3332
    [Email Id] => test@test.com
    [Phone] => 1234567890
    [Status] => Success
    [URL] =>
https://test.payu.in/processInvoice?invoiceId=9eec02ac9e2efc335bdda2d748612
1ce03de24c2fa7d32d17462ad5a6a9058db
)
```

- **If duplicate transaction id is used**

```
Invoice for this transaction ID already exists.
```

- **If invalid parameter is sent***

```
Invalid <parameter>
```

Note: Here <parameter> value displayed would be the incorrect parameter provided*

14) expire_invoice

This API is used to expire an invoice link corresponding to the txnID. In a few cases – an invoice might be sent to an incorrect email ID by the merchant. In such scenario, merchant might want to discard the invoice by expiring it. This API can be useful in such scenario.

- **If invoice is successfully expired, and the transaction isn't already in progress**

```
Array
(
    [status] => 1
    [msg] => Invoice expired
)
```

- **If invoice is successfully expired, but the transaction is already in progress**

```
Array
(
    [status] => 1
```

```
    [msg] => Invoice expired, Transaction is already in progress
)
```

- **If invoice doesn't exist for txnID**

```
Array
(
    [status] => 0
    [msg] => Invoice does not exist for this txnid
)
```

15) check_offer_status (1st Usage)

This API is used to check the status of an offer for a particular merchant when all the details are passed. The return parameters are status, msg, discount/error_code, category, offer_key, offer_type(instant/ cashback) , offer_availed_count, offer_remaining_count.

Input Variables Description:

Parameter	Description	Sample Value
var1	Offer Key(mandatory)	offer@123
var2	Amount	100
var3	Category	CC
var4	Bank Code	CC
var5	Card Number(mandatory)	5432112345678901
var6	Name on Card	Nitesh
var7	Phone Number	91234567890
var8	Email Id	abc@xyz.com

Error Codes:

- 'INVALID_OFFER'=>'E001',
- 'INVALID_PAYMENT_METHOD'=>'E002'

In the Output:

- Parameter 'status' = 1, means offer is valid
- Parameter 'status' = 0, means offer is invalid.

Web Service Responses:

Note: In the response, category will be the passed Category.

- **If the offer is a valid offer**

```
Array
(
    [status] => 1
    [msg] => Valid offer
    [discount] => 15
    [category] => creditcard
    [offer_key] => testoffer12312@5788
```

```
    [offer_type] => instant
    [offer_availed_count] => 5
    [offer_remaining_count] => 3
)
```

- **If the offer is expired**

```
Array
(
    [status] => 0
    [msg] => Offer expired.
    [error_code] => E001
    [category] => creditcard
    [offer_key] => newoffer1@5686
    [offer_type] => instant
    [offer_availed_count] => Unknown
    [offer_remaining_count] => Unknown
)
```

- **If the card limit is exhausted**

```
Array
(
    [status] => 0
    [msg] => Offer Exhausted
    [error_code] => E001
    [category] => creditcard
    [offer_key] => newoffer1@568
    [offer_type] => Unknown
    [offer_availed_count] => Unknown
    [offer_remaining_count => Unknown
)
```

- **If offerKey is invalid**

```
Array
(
    [status] => 0
    [msg] => Invalid offer Key
    [error_code] => E001
    [offer_key] => newoffer1@568
    [offer_type] => Unknown
    [offer_availed_count] => Unknown
    [offer_remaining_count] => Unknown
)
```

16) check_offer_status (2nd Usage)

This API is used to check the status of an offer when only the parameters Offer Key and card number are passed as input. This API can be used to check the offer status when offer is created using bin only. In this case we can depict that the offer has been created for which category (like CC/DC/NB/EMI). Hence, for using this API, you need to pass the Offer Key and Card Number in var1 and var5 field as inputs and leave the rest field empty.
The return parameters are status, msg, error_code (In case of error), category, offer_key, offer_type (instant/cashback), offer_availed_count, ‘offer_remaining_count'.

Input Variables Description:

Parameter	Description	Sample Value
var1	Offer Key(mandatory)	offer@123
var2	Empty	-
var3	Empty	-
var4	Empty	-
var5	Card Number(mandatory)	5432112345678901

Error Codes:

- 'INVALID_OFFER'=>'E001',
- 'INVALID_PAYMENT_METHOD'=>'E002'

Output:

- Parameter 'Status' = 1, means offer is valid
- Parameter 'Status' = 0, means offer is invalid

Web Service Responses:

- **If the offer is a valid offer for the given card number(bin)**

```
Array
(
    [status] => 1
    [msg] => Valid offer
    [category] => creditcard
    [offer_key] => abc@123
    [offer_type] => instant
    [offer_availed_count] => 5
    [offer_remaining_count => 1
)
```

- **If the offer is expired**

```
Array
(
    [status] =>0
    [msg] => Offer Expired
    [error_code] => E001
    [category] => Unknown
    [offer_key] => offerKey
    [offer_type] => Unknown
    [offer_availed_count] => Unknown
    [offer_remaining_count] => Unknown
)
```

- **If the card limit is exhausted**

```
Array

(
    [status] => 0
    [msg] => Offer Exhausted
    [error_code] => E001
```

```
    [category] => Unknown
    [offer_key] => offerKey
    [offer_type] => Unknown
    [offer_availed_count]  => Unknown
    [offer_remaining_count] => Unknown
)
                    )
```

- **If the offer is an invalid offer for the given card number(bin)**

```
Array
(
    [status] => 0
    [msg] => Invalid offer
    [error_code] => E001/E002
    [offer_key] => abc@123
    [offer_type] => Unknown
    [offer_availed_count] => Unknown
    [offer_remaining_count]  => Unknown
)
```

17) getNetbankingStatus

This API is used to help you in handling the NetBanking Downtime. A few times, one or more Net Banking options may be facing downtime due to issues observed at Bank's end. This API is used to tell the status of one or all the net banking options. The status can be either up or down. If you want to know the status of a specific Net Banking option, the input parameter should contain the corresponding ibibo_code. If you want to know the status of all the Net Banking options, the input parameter should contain the value 'default'.

Input variable description:

Parameter	Description	Sample Value
var1	ibibo_code or "default"	AXIB/"default"

Web Service Responses:

Case a: To get status of one Net Banking Option **(The specific ibibo_code is passed in input)**

Response**:**

```
Array
(
    [AXIB] => array
       (
            [ibibo_code] => AXIB
            [title] => AXIS Bank NetBanking
            [up_status] => 0
       )
)
```

Note:

- up_status = 0 signifies that the particular Bank option is **down** at the moment.
- up_status=1 signifies that the particular Bank Banking option is **up** at the moment.

Case b: To get status of all Net Banking options. (**The value "default" is passed in input)**

Web Service Responses:

```
Array
(
    [AXIB] => array
        (
            [ibibo_code] => AXIB
            [title] => AXIS Bank NetBanking
            [up_status] => 1
        )

    [BOIB] => array
        (
            [ibibo_code] => BOIB
            [title] => Bank of India
            [up_status] => 1
        )

    [BOMB] => array
        (
            [ibibo_code] => BOMB
            [title] => Bank of Maharashtra
            [up_status] => 1
        )

    [CABB] => array
        (
            [ibibo_code] => CABB
            [title] => Canara Bank
            [up_status] => 1
        )
    .
    .
    .
    . <All the other banks and their status>
```

Note:

- up_status = 0 signifies that the particular Bank option is **down** at the moment.
- up_status= 1 signifies that the particular Bank Banking option is **up** at the moment.

18) getIssuingBankStatus

This API is used to help you in handling the Credit Card/Debit Card Issuing Bank Downtime. It allows you get the present status of an Issuing Bank using the specific Bank Identification Number (BIN). BIN is identified as the first 6 digits of a credit/debit card. You need to provide the bin number as input and the corresponding issuing bank's status would bereturned in the output (whether up or down).

Input variable description:

Parameter	Description	Sample Value
var1	Bank Identification Number(First 6 digits of a card)	512345

Web Service Responses:

```
Array
(
    [issuing_bank] => HDFC
    [up_status] => 1
)
```

Note:

- up_status = 0 signifies that the particular Bank option is **down** at the moment.
- up_status= 1 signifies that the particular Bank Banking option is **up** at the moment.

19) getIssuingBankDownBins

This command is used to retrieve the card bins for all banks which are observing either full downtime or partial downtime at an instant. The information related to full/partial downtime depends on the input parameter values.

Input Variables Description:

Parameter	Description	Sample Value
var1	Bank Name code (To be Provided by PayU) or "default"	Default
var2	1 if you want to extract information about partially down bins as well and 0 if you want information about fully down bins only.	0/1

Web Service Responses:

- **If successfully fetched**

```
Array
(
    [0] => Array
        (
            [issuing_bank] => KOTAK
            [status] => 0
            [title] => KOTAK MAHINDRA BANK LTD
            [bins_arr] => Array
                (
                    [0] => 429393
                    [1] => 416644
                    [2] => 416645
                    [3] => 416643
                    [4] => 416646
                    [5] => 436390
                )
        )

    [1] => Array
        (
            [issuing_bank] => ALLBD
            [status] => 2
            [title] => ALLAHABAD BANK
            [bins_arr] => Array
                (
                    [0] => 430450
                    [1] => 421337
                )
        )
)
```

The values referring to the array can be described below:

- [issuing_bank] => The bank which is down or partially down
- [bins_arr] => The card bins array
- [status] => 0 if the issuing bank is completely down and 2 if it is partially down
- [title] => title of the bank

20) get_Transaction_Details

This API is used to extract the transaction details between two given time periods. The API takes the input as two dates (initial and final), between which the transaction details are needed. The output would consist of the status of the API (success or failed) and all the transaction details in an array format.

Input variable description:

Parameter	Description	Sample Value
var1	Starting Date (From when the transaction details are needed) in yyyy-mm-dd format	2014-01-12
var2	End Date (Till when the transaction details are needed) in yyyy-mm-dd format	2014-01-13

Web Service Responses:

The status variable would be 1 for successful web-service execution and would be 0 in case of unsuccessful web-service execution. Output would be returned in the following array format:

- **For Successful Response, status=1:**

```
Array
(
    [status] => 1
    [msg] => Transaction Fetched Successfully
    [Transaction_details] => Array
      (
            [0] => array
          (
              [id] => 403993715508970248
              [status] => failed
              [key] => C0Dr8m
              [merchantname] => test payu
              [txnid] => e1e8a8f4ace8506043e1
              [firstname] => John
              [lastname] => Moses
              [addedon] => 2014-02-04 01:25:38
              [bank_name] => Visa Debit Cards (All Banks)
              [payment_gateway] => AXIS
              [phone] => 9585475883
              [email] => y.johnmoses@gmail.com
              [amount] => 100.00
              [discount] => 0.00
              [additional_charges] => 0.00
              [productinfo] => CSIIT Conference Registration
              [error_code] => E312
              [bank_ref_no] => 2000112693
```

```
                [ibibo_code] => VISA
                [mode] => DC
                [ip] => 117.206.82.90
                [card_no] => 414367XXXXXX0250
                [cardtype] => international
                [offer_key] =>
                [field2] => 403506432293
                [udf1] =>
                [pg_mid] => TESTIBIBOWEB
                [offer_type] =>
                [failure_reason] =>
                [mer_service_fee] =>
                [mer_service_tax] =>
            )

        [1] => Array
            (
                [id] => 403993715508970268
                [status] => captured
                [key] => C0Dr8m
                [merchantname] => test payu
                [txnid] => 8613914632655135
                [firstname] => Hans Wurst
                [lastname] =>
                [addedon] => 2014-02-04 03:03:06
                [bank_name] => Credit Card
                [payment_gateway] => HDFC
                [phone] =>
                [email] => f606f938f64b499aa3fd952d6338aa54@example.com
                [amount] => 30.00
                [discount] => 0.00
                [additional_charges] => 0.00
                [productinfo] => 3752946
                [error_code] => E000
                [bank_ref_no] => 1953525040340351
                [ibibo_code] => CC
                [mode] => CC
                [ip] => 217.6.59.133
                [card_no]  => 512345XXXXXX2346
                [cardtype] => domestic
                [offer_key] =>
                [field2] => 999999
                [udf1] =>
                [pg_mid] => 90000970
                [offer_type] =>
                [failure_reason] =>
                [mer_service_fee]  => 0.70
                [mer_service_tax]  => 0.09
            )
        )
)
```

- **For successful web-service execution, but empty response (i.e. No transactions found):**

```
Array
(
    [status] => 1
    [msg] => Transaction Fetched Successfully
    [Transaction_details] => Array
```

```
        (
        )
)
```

- **Failed case:**

  In case of invalid input date format, output would be of the following form:

```
Array
(
    [status] => 0
    [msg] => Invalid Date Entered. Date format should be yyyy-mm-dd
)
```

21) get_transaction_info

This API works exactly the same way as **get_Transaction_Details** API. The only enhancement is that this API can take input as the exact time in terms of minutes and seconds also. Output would be in the same format as get_Transaction_Details API output.

Input variable description:

Parameter	Description	Sample Value
var1	Starting Time (From when the transaction details are needed) in yyyy-mm-dd hh:mm:ss format	2014-01-12 16:00:00
var2	End Time (Till when the transaction details are needed) in yyyy-mm-dd hh:mm:ss format	2014-01-12 16:15:00

Web Service Responses:

The status variable would be 1 for successful web-service execution and would be 0 in case of unsuccessful web-service execution. Output would be returned in the following array format:

a) **For Successful Response, status=1:**

```
Array
(
    [status] => 1
    [msg] => Transaction Fetched Successfully
    [Transaction_details] => Array
      (
            [0] => array
          (
              [id] => 403993715508970248
              [status] => failed
              [key] => C0Dr8m
              [merchantname] => test payu
              [txnid] => e1e8a8f4ace8506043e1
              [firstname] => John
              [lastname] => Moses
              [addedon] => 2014-02-04 01:25:38
              [bank_name] => Visa Debit Cards (All Banks)
              [payment_gateway] => AXIS
              [phone] => 9585475883
              [email] => y.johnmoses@gmail.com
              [amount] => 100.00
```

```
            [discount] => 0.00
            [additional_charges] => 0.00
            [productinfo] => CSIIT Conference Registration
            [error_code] => E312
            [bank_ref_no] => 2000112693
            [ibibo_code] => VISA
            [mode] => DC
            [ip] => 117.206.82.90
            [card_no] => 414367XXXXXX0250
            [cardtype] => international
            [offer_key] =>
            [field2] => 403506432293
            [udf1] =>
            [pg_mid] => TESTIBIBOWEB
            [offer_type] =>
            [failure_reason] =>
            [mer_service_fee] =>
            [mer_service_tax] =>
        )

    [1] => Array
        (
            [id] => 403993715508970268
            [status] => captured
            [key] => C0Dr8m
            [merchantname] => test payu
            [txnid] => 8613914632655135
            [firstname] => Hans Wurst
            [lastname] =>
            [addedon] => 2014-02-04 03:03:06
            [bank_name] => Credit Card
            [payment_gateway] => HDFC
            [phone] =>
            [email] => f606f938f64b499aa3fd952d6338aa54@example.com
            [amount] => 30.00
            [discount] => 0.00
            [additional_charges] => 0.00
            [productinfo] => 3752946
            [error_code] => E000
            [bank_ref_no] => 1953525040340351
            [ibibo_code] => CC
            [mode] => CC
            [ip] => 217.6.59.133
            [card_no]  => 512345XXXXXX2346
            [cardtype] => domestic
            [offer_key] =>
            [field2] => 999999
            [udf1] =>
            [pg_mid] => 90000970
            [offer_type] =>
            [failure_reason] =>
            [mer_service_fee]  => 0.70
            [mer_service_tax]  => 0.09
        )

    [2] => Array
        (
            [id] => 403993715508970270
            [status] => captured
            [key] => C0Dr8m
            [merchantname] => test payu
```

```
                    [txnid] => 8813914632908201
                    [firstname] => Hans Wurst
                    [lastname] =>
                    [addedon] => 2014-02-04 03:03:30
                    [bank_name] => Credit Card
                    [payment_gateway] => HDFC
                    [phone] =>
                    [email] => 89163cd22823449d89e6d5cd2346fea3@example.com
                    [amount] => 30.00
                    [discount] => 0.00
                    [additional_charges] => 0.00
                    [productinfo] => P172
                    [error_code] => E000
                    [bank_ref_no] => 261662040340351
                    [ibibo_code] => CC
                    [mode] => CC
                    [ip] => 217.6.59.133
                    [card_no] => 512345XXXXXX2346
                    [cardtype] => domestic
                    [offer_key] =>
                    [field2] => 999999
                    [udf1] =>
                    [pg_mid] => 90000970
                    [offer_type] =>
                    [failure_reason] =>
                    [mer_service_fee] => 0.70
                    [mer_service_tax] => 0.09

                )
            )
        )
```

b) For successful web-service execution, but empty response (i.e. No transactions found):

```
Array
(
    [status] => 1
    [msg] => Transaction Fetched Successfully
    [Transaction_details] => Array
       (
       )
)
```

c) Failed case:

In case of invalid input date format, output would be of the following form:

```
Array
(
    [status] => 0
    [msg] => Invalid Date Entered. Date format should be yyyy-mm-dd
hh:mm:ss
)
```

22) check_isDomestic

This API is used to detect whether a particular bin number is international or domestic. It is also useful to determine the card's issuing bank, the card type brand – i.e, Visa, Master etc

and also the Card Category – i.e. Credit/Debit etc. Bin number is the first 6 digits of a Credit/Debit card.

Input Variables description:

Parameter	Description	Sample Value
var1	Card Number/Bin(First 6 digits of a card)	512345

Web Service Responses:

Case a: If the card is domestic

```
Array
(
    [isDomestic] => Y
    [issuingBank] => HDFC
    [cardType] => MAST
    [cardCategory] => CC
)
```

Case b: If the card is international

```
Array
(
    [isDomestic] => N
    [issuingBank] => UNKNOWN
    [cardType] => UNKNOWN
    [cardCategory] => CC
)
```

Here in the output,

- isDomestic = Y signifies that the particular bin is domestic.
- isDomestic = N signifies that the particular bin is International.
- cardType = <value> which can be['MAST','VISA','MAES','AMEX', 'DINR','Unknown']
- [issuingBank] = The issuing bank of the card used for transaction
- [cardCategory] = CC signifies that the particular bin is a Credit Card Bin
- [cardCategory] = DC signifies that the particular bin is a Debit Card Bin

Note: This API would give the output based upon PayU's bin list which may not be completely exhaustive.

23) get_settlement_details

This command is used to retrieve Settlement Details for the merchant. The input is the date for which Settlement Details are required.

Input Variables Description:

Parameter	Description	Sample Value
var1	Date for which Settlement Data is required - in YYYY-MM-DD format	2015-08-01

Web Service Responses

- **If date format is incorrect**

```
Array
(
    [status] => 0
    [msg] => Please check date format it should be YYYY-MM-DD
)
```

- **If no data found for the particular date**

```
Array
(
    [status] => 1
    [msg] => 0 transactions settled on 2015-05-01
    [Txn_details] => Array
        (
        )
)
```

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => 6565 transactions settled on 2015-08-01
    [Txn_details] => Array
        (
            [0] => Array
                (
                    [payuid] => 204131224
                    [txnid] => GOFLCF519911416076450
                    [txndate] => 2014-11-16 00:08:40
                    [mode] => DC
                    [amount] => 2580.00
                    [requestid] => 262698935
                    [requestdate] => 2015-08-01 17:43:25
                    [requestaction] => capture
                    [requestamount] => 186.00
                    [mer_utr] => CITIH15213701843
                    [mer_service_fee]  => 0.00000
                    [mer_service_tax]  => 0.00000
                    [mer_net_amount] => 186.00000
                    [bank_name] => VISA
                    [issuing_bank] => BOB
                )

            [1] => Array
                (
                    [payuid] => 206974239
                    [txnid] => GOFLIae1e11416407957
                    [txndate] => 2014-11-19 20:09:29
                    [mode] => CC
                    [amount]  => 33972.00
                    [requestid] => 262698908
                    [requestdate] => 2015-08-01 12:45:03
                    [requestaction] => refund
                    [requestamount] => 4094.00
                    [mer_utr] => CITIH15213701843
                    [mer_service_fee]  => 0.00000
                    [mer_service_tax]  => 0.00000
```

```
                    [mer_net_amount] => -4094.00000
                    [bank_name] => CC
                    [issuing_bank] => CANA
                )
        )
)
```

24) get_merchant_ibibo_codes

This command is used to retrieve all the activated payment options for the merchant. In this API, var1 needs to be left empty in the input and var2 needs to be kept as 1.

Input Variables Description:

Parameter	Description	Sample Value
var2	Has to be equal to 1 always	1

Web Service Responses

- **If successfully fetched**

```
Array
(
    [emi] => Array
        (
            [EMIK12] => KOTAK - 12 Months
            [SBI12] => SBI - 12 months
            [EMIHS12] => HSBC - 12 Months
            [EMIA12] => AXIS - 12 Months
        )

    [cashcard] => Array
        (
            [AMON] => Airtel Money
            [ITZC] => ItzCash
        )

    [netbanking] => Array
        (
            [HDFB] => HDFC Bank
            [AXIB] => AXIS Bank NetBanking
            [ICIB] => ICICI Netbanking
            [UCOB] => UCO Bank
        )

    [creditcard] => Array
        (
            [AMEX] => AMEX Cards
            [CC] => Credit Card
            [DINR] => Diners
        )

    [debitcard] => Array
        (
            [MAST] => MasterCard Debit Cards (All Banks)
            [MAES] => Other Maestro Cards
```

```
        )
)
```

25) eligibleBinsForEMI

This command is used only when the merchant needs the EMI feature of PayU. In case the merchant is managing card details on its own website, this API can tell the issuing bank of the card bin. It also provides the minimum eligible amount for a particular bank.

Input Variables Description (1st Method):

Parameter	Description	Sample Value
var1	Hardcoded as “bin”	Bin
var2	Card bin number (First 6 digits)	434668

Web Service Responses

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => Details fetched successfully
    [details] => Array
        (
            [isEligible] => 1
            [bank] => KOTAK
            [minAmount] => 500
        )
)
```

- **If not found**

```
Array
(
    [status] => 1
    [msg] => Details fetched successfully
    [details] => Array
        (
            [isEligible] => 0
        )
)
```

Input Variables Description (2nd Method):

Parameter	Description	Sample Value
var1	Hardcoded as “bin”	Bin
var2	Card bin number (First 6 digits)	434668
var3	bankname	KOTAK

- **If successfully fetched**

```
Array
(
    [status] => 1
    [msg] => Details fetched successfully
    [details] => Array
        (
            [isEligible] => 1
            [bank] => KOTAK
            [minAmount] => 500
        )
)
```

- **If var3 (input bank name) doesn't match with the bank name in PayU Database, that means the bin given in input is of a different bank name**

```
Array
(
    [status] => 0
    [msg] => Invalid Bin
)
```

API's 27-30 are related to PayU's Store Card Feature

26) get_user_cards

This API is used to fetch all the cards corresponding to the user. In this API, card number and other sensitive information is not returned.

Input Variables description:

Parameter	Description	Sample Value
var1	user_credentials (In the format- MerchantKey:UserIdentifier)	JQBlG:abc

Web Service Responses:

Case a: Cards are found in the vault.

Response:

```
Array
(
    [status] => 1
    [msg] => Cards fetched Succesfully
    [user_cards] => Array
        (
            [745d72e2fd9b7e88824fef4e7ed7dac1fe624b7] => Array
                (
                    [name_on_card] => {name}
                    [card_name] => nickname but if sent empty then
            (cardType****last 4 digits of card) e.g. mastercard****2346
                    [card_type] => CC(ibibo_code)
                    [card_token] => 745d72e2fd9b7e88824fef4e7ed7dac1fe624b7
                    [is_expired] => 1(1 when card is expired , 0 when not)
                    [card_mode] => CC(card Category)
                    [card_no] => 412345xxxxxx2356(masked Card Number)
                    [card_brand] => VISA
                    [card_bin] => 412345
                    [expiry_year] => 2017
                    [expiry_month] => 10
                )
        )
```

```
)
```

Case b: No cards are found for the user

```
Array
(
    [status] => 0
    [msg] => Card not found.
)
```

27) save_user_card

This API is used for saving a card to the vault. On successful storing of the card, it returns the cardToken.

Input Variables description:

Parameter	Description	Sample Value
var1	user_credentials - merchantKey:userId	JQBlG:abc
var2	cardName(nickname of the card)	My_card
var3	cardMode	CC
var4	cardType	AMEX
var5	nameOnCard	Nitesh Jindal
var6	cardNo	5123456789012345
var7	cardExpMon	9
var8	cardExpYr	2014

Case a: When card is stored successfully

Web Service Responses:

```
Array
(
    [status] => 1
    [msg] => Card Stored Successfully.
    [cardToken] => 745d72e2fd9b7e88824fef4e7ed7dac1fe624b7
)
```

Case b: Any of the field is invalid

If card Number is invalid:

Web Service Response:

```
Array
(
    [status] => 0
    [msg] => CardNumber is invalid
)
```

28) edit_user_card

This API is used to edit the details of an existing stored card in the vault. In this case, along with all the parameters that are required to save to the card, cardToken of the card to edit is also required to be passed. On successfully editing the card, it returns the cardToken of the card.

Input Variables description:

Parameter	Description	Sample Value
var1	User Credentials - MerchantKey:UserId MerchantName:UserId	JQBlG:abc
var2	cardToken(card token of the card to edit)	745d72e2fd9b7e88824fef4e7ed7dac1f
var3	cardName(nickname of the card)	My_card
var4	cardMode	CC
var5	cardType	AMEX
var6	nameOnCard	Nitesh Jindal
var7	cardNo	5123456789012345
var8	cardExpMon	9
var9	cardExpYr	2014

Case a: On successful editing of card

Web Service Response:

```
Array
(
    [status] => 1
    [msg] => {cardName} Edited Successfully.
    [cardToken] => 745d72e2fd9b7e88824fef4e7ed7dac1fe624b74
)
```

Case b: If the wrong card token is given to edit

Web Service Response:

```
Array
(
    [status] => 0
    [msg] => Card not found to edit
)
```

29) delete_user_card

This API is used to delete a card.

Input Variables description:

Parameter	Description	Sample Value
var1	user_credentials - merchantKey:userId	JQBlG:abc

	MerchantName:UserId	
var2	cardToken (cardtoken of the card to delete)	745d72e2fd9b7e88824fef4e7ed

Web Service Responses:

Case a: On successful deletion of card

```
Array
(
    [status] => 1
    [msg] => {cardName} deleted successfully
)
```

Case b: on failure of deletion

```
Array
(
    [status] => 0
    [msg] => error reason
)
```

30) clemi_pincode_check

This API is used to check the eligibility of given pincode for a PayU Monedo Loan Application. The pincode to be checked is given as input and its eligibility is accordingly returned in the response. The response parameters are eligibilitystatus [status] and an accompanying message [msg].
The status is returned as '1' in case of eligible pincode, '-1' in case of ineligible (but valid) pincode and '0' in case of any errors.

Input Variables Description:

Web Service Responses:

- **if pincode is invalid**

```
Array
(
    [status] => 0
    [msg] => Pincode is invalid
)
```

- **if pincode is not eligible**

```
Array
(
    [status] => -1
    [msg] => Pincode is not eligible
)
```

- **if pincode is eligible**

```
Array
(
    [status] => 1
    [msg] => Pincode is eligible
)
```

- **if service is unavailable due to internal network or processing error**

```
Array
(
    [status] => 0
    [msg] => Internal Service Error
)
```

31) proofOfDeliveryInformation

This API is used to share the proof of delivery of goods/services to the customer. This is required for Bajaj Finserv & HDFC Debit Card EMI options. The pincode to be checked is given as input and its eligibility is accordingly returned in the response. The response parameters are eligibility status [status] and anaccompanying message [msg].
The status is returned as '1' in case of the information has been successfully captured in our system, in all other cases, status as '0' or timeout this API needs to be called again.

Input Variables Description:

Parameter	Description	Comments
var1	PayUID- Will be returned in the response of the transaction	
var2	AWBno- Tracking number of the shipment in case of goods delivery, "NA" in case of services	
var3	CourierName- Name of the delivery partner in case of goods delivery & name of the merchant in case of services	
var4	DeliveryAddress- Deliveryaddress in case of goods delivery & customer address in case of services	
var5	DeliveryDateTime- Date & time when shipment was handed over to the customer in case of goods & dateand time when service was given to the customer in case of services	Date in YYYY-MM-DDTHH:MM:SS format, for ex. 2006-01-02T15:04:05
var6	Invoicedate- Self explanatory	Date in DDMMYYYY format
var7	InvoiceNumber- Self explanatory	
var8	InvoiceAmount- Self explanatory	
var9	Manufacturer- Manufacturer of the equipment in case of goods & that party, not the marketplaces, who is giving services in case of services	
var10	OrderNo- Self explanatory	
var11	ProductCategory- Table given below for different kinds of categories	
var12	Productdescription- Details of product purchased/services	

	availed by the customer, like Model Name in case of the goods & details of services of the services	
var13	ReceiversName- Name of the person to whom product was delivered in case of goods and customer name in case of services	
var14	SerialNumber- Serial number of the product, like IMEI in case of mobiles & Policy Number in case of insurance	
var15	SellerName- Self explanatory, this will not be name of the marketplace in case of marketplace models	

ProductCategory	Description
Consumer Durable	White goods example: mobile phone, refrigerator, Air conditioner, television etc
Lifestyle	Lifestyle products example: premium Furniture, high-end Watches, Cameras, Fitness equipment, etc.
Life care	Life care finance example: Dental surgeries, Cosmetic Surgeries, Medical Treatments like Laparoscopic, Weight loss surgeries, IVF, Eye care, Stem cells, Hair transplants, etc.
Apparels	Apparels – Branded Clothes and Accessories example: Foot-ware, Eyewear, Handbags, Leather accessories
Travel	Travel & Holidays - Domestic & International Travel financing
Art and Antiques	Art and Antiques such as Paintings by renowned artist sold through listed art galleries

Web Service Responses:

- **When the information has successfully been captured in our system**

```
Array
{
     "status": 1,
     "msg": "INVOICE ADDED SUCCESSFULLY."
 }
```

- **In case of failure**

```
Array
 {
   "status": 0,
   "msg": "Some error occured"
   "description":""
}
```

PayU Webhooks

Document Purpose

Webhooks are user-defined HTTP callbacks or messages, operating at the server to server (S2S) communication levels. Certain instances or events trigger them. The following document attempts a complete overview of how PayU uses the technology to develop a secure and accountable architecture for the payment workflows between the merchant's servers and its own.

What Are PayU Webhooks?

PayU provides for both non-seamless and seamless integration with the merchant's system. These payment workflows are triggered through a browser call and operate at the browser level itself. It involves switching the user between the merchant, PayU and the bank's website environments and redirecting them to the success or failure URLs on a case to case basis. In this browser redirection approach, it may be technically challenging for the merchant to ascertain the integrity of responses everytime, affecting end-user experience.

Webhook is a server to server callback. Once this feature is activated for merchants, PayU would send an S2S response, in addition to Browser redirection, to the merchant. It is recommended for the merchant to process the transaction order status - based upon S2S response and not via the Browser Redirection response to ensure optimum translation outcomes.

Why PayU Uses Webhooks?

The S2S callback is a useful and recommendable feature for merchants while integrating with PayU. PayU sends the final transaction response to the merchant via browser redirection. However, due to network issues or other technical lags, this browser redirection may not be successful and the transaction may get dropped (between PayU and Merchant). In such events, the merchant will not be able to complete the processing of the order at their end. For such cases, this callback feature can be used effectively.

How Can The Merchant Use Webhooks?

Step 1: The merchants need to create a server URL (Ex: www.test.payu.in/success/response) from their business server landscape and share it with PayU, along with its server IP address. It is the URL at which the transaction response from PayU will hit.

Step2: PayU will configure the merchant's server URL at its backend, mapping it against the MID and key of that particular merchant.

Step3: To establish the connection, PayU will Whitelist the merchant's server IP address in its systems. Similarly, the merchant also needs to whitelist the following IP address at their firewall side to receive a response from the PayUBiz servers:

- 180.179.174.1
- 180.179.174.2
- 180.179.165.250
- 3.7.89.8
- 3.7.89.9
- 3.7.89.1052.140.8.88
- 52.140.8.89
- 180.179.174.1
- 180.179.174.23.7.89.1
- 3.7.89.2
- 52.140.8.64
- 52.140.8.65
- 52.140.8.66

Step 4: PayU will send an S2S response to the merchant's server URL. The response will always be sent as the key-value pair separated by '&' character or HashMap formats, and the merchant's server URL should be capable of handling the following content types:

- FormData
- application/x-www-form-urlencoded

So while creating the server URL, the merchant needs to ensure that it can accept the data in the above content formats.

Below is a sample response from PayU to the merchant:

unmappedstatus=success&phone=9999999999&txnid=FCDA1R100870163781&hash=84e335094bbcb2d daa0f9a488eb338e143b273765d89c9dfa502402562d0b6f3c7935e28194ca92f7380be7c84c3695415b10 6dcf52cb016a15fcf6adc98d724&status=success&curl=https://www.abc.in/payment/handlepayuresposn e&firstname=NA&card_no=519619XXXXXX5049&furl=https://www.abc.in/payment/handlepayuresposn e&productinfo=2&mode=DC&amount=800.00&field4=6807112311042810&field3=6807112311042810 & field2=838264&field9=SUCCESS&email=NA&mihpayid=175477248&surl=https://www.ABC.in/payment/ handlepayuresposne&card_hash=9e88cb0573d4a826b61d808c0a870ed4a990682459b0ec9e95ea421e8 e47b e8c&field1=42812

The parameters used in generating the above response block are similar to those that the merchant has shared with PayU while triggering the transaction. It includes:

- mihpayid
- mode
- status
- key
- txnid
- amount
- productinfo
- firstname
- lastname
- address1
- address2
- city
- state
- country
- zipcode
- email
- furl
- card_hash
- phone
- udf1,udf2,udf3,udf4,udf5,udf6,udf7,udf8,udf9,udf10
- card_token
- card_no
- field0,field1,field2,field3,field4,field5,field6,field7,field8,field9
- offer
- discount
- offer_availed
- unmappedstatus
- hash
- bank_ref_no
- surl
- curl

In case a parameter has not been consumed, PayU sends it back to the merchant with an empty string.

Step 5: As the PayU response hits the merchant's server URL, it must confirm the receipt with the success status response code: 200 OK.

PayU will attempt three times to get a 200 OK response from the merchant's servers before flagging the transaction as a timeout. Sometimes it may happen due to the wrong configuration of the merchant's server URL. This makes it crucial for the URL to accept and process data in key-value pairs separated by '&' character or HashMap formats and handle the content types mentioned above.