

# **HOSTED**

## **INTEGRATION GUIDE**

Version: 9.13

1	Hosted Form Integration.....	3
1.1	About This Guide.....	3
1.2	Pay Global Integration Disclaimer.....	3
1.3	New Customers Testing.....	3
1.4	Pre-Requisites .....	4
1.5	3D Secure.....	5
1.6	Test Cards.....	5
2	Gateway Request .....	6
2.1	General Fields .....	6
2.2	Redirection and Verification Fields .....	8
2.3	Customer Details Fields.....	8
2.4	American Express and Diners Card Fields.....	9
2.5	Merchant Data Field .....	10
3	Gateway Response.....	11
3.1	Response Fields.....	11
3.2	3D Secure Fields.....	13
<b>A-1</b>	<b>Response Codes .....</b>	<b>15</b>
<b>A-2</b>	<b>Types of card.....</b>	<b>22</b>
<b>A-3</b>	<b>AVS / CV2 Check Response .....</b>	<b>23</b>
<b>A-4</b>	<b>3D Secure Enrolment/Authentication Codes .....</b>	<b>25</b>
<b>A-5</b>	<b>Example Code.....</b>	<b>26</b>
<b>A-6</b>	<b>Test Cards .....</b>	<b>27</b>
<b>A-7</b>	<b>3D Secure Test Cards .....</b>	<b>30</b>
<b>A-8</b>	<b>Signing Your Request.....</b>	<b>31</b>

## **1 Hosted Form Integration**

### **1.1 About This Guide**

The Pay Global Hosted Form Integration method requires the merchant (or the merchant's web developer) to have knowledge of server side scripting languages (e.g. PHP, ASP etc.), although less so than the Direct method. Unlike the Direct method, the merchant's website does not need to have a SSL Certificate, and PCI compliance becomes more straightforward.

If you wish to process card details on your own website, or style the payment pages of your website, you either need to use the Direct integration method or request a Custom Hosted Form for your business.

### **1.2 Pay Global Integration Disclaimer**

Pay Global provides all integration documentation necessary for enabling merchant clients to process payments via our Payment Gateway. Whilst every effort has been made to ensure these guides are accurate and complete, we expect Merchants undertaking any integration to test all their technical work fully and satisfy their own standards. Pay Global is not responsible or liable for any Merchant or Third Party integration.

### **1.3 New Customers Testing**

New customers who have not yet received their live Merchant ID can still perform an integration for testing purposes. Simply enter one of the below Test Merchant IDs and then use the Pay Global test cards to run a test transaction.

Standard Visa and MasterCard Testing use **101661**  
3D Secure Testing use **101662**

This guide provides the information required to integrate with Pay Global, and gives a very basic example of code for doing so. It is expected that the Merchant, or the Merchant's developers, have some experience in server side scripting with languages such as PHP or ASP, or that an off-the-shelf software package is being used that has in-built Pay Global integration support.

If you do require programming assistance, please contact Pay Global on 0203 504 2443 or via email to [support@payglobal.org](mailto:support@payglobal.org).

## **1.4 Pre-Requisites**

You will need the following information to integrate with Pay Global Hosted Forms.

<b>Pay Global Merchant ID</b>	<p>Your Merchant ID enables you to access and communicate with the payment gateway. Please note that these details will differ to the login details supplied to access the Merchant Management System. You should have received these details when your account was set up.</p> <p>You may also use test account IDs (listed above) and swap these for your live account details when you receive them.</p>
<b>Integration URL</b>	<a href="https://gateway.payglobal.org/paymentform/">https://gateway.payglobal.org/paymentform/</a>

## **1.5 3D Secure**

If your merchant account is enrolled with 3D Secure, the hosted form method will automatically attempt to perform 3D Secure transactions. If the customer's card is not participating in 3D Secure then the transaction will be processed as normal, otherwise it will take the customer through the 3D Secure authentication process.

You can choose how to deal with 3D Secure transactions that fail authentication – either declining the transaction or continuing without 3D Secure protection. These preferences are set in the Merchant Management System.

## **1.6 Test Cards**

For the latest copy of the test cards, for both 3D Secure and non 3D Secure transactions, please see Appendix A-6 & A-7 below.

## 2 Gateway Request

Your website will need to send the request details to the integration URL via an HTTP POST request. The details should be URL encoded Name=Value fields separated by ‘&’ characters (refer to RFC 1738 and the application/x-www-form-urlencoded media type).

For example, you might create an HTML form to collect the customer information (without card details), then use hidden fields to post the other options.

*Please note that the field names are cAsE sEnSiTiVe.*

### 2.1 General Fields

Field Name	Mandatory?	Description
<b>merchantID</b>	Yes	Your Pay Global Merchant user ID, or “101661” if you are just testing.
<b>merchantPwd</b>	No *	The password you have configured for the merchantID. This is set within the MMS  <small>* Using this field may result in your password being visible in plain text within the source code.</small>
<b>signature</b>	Yes	The hash used to sign the transaction request.
<b>amount</b>	Yes	The amount of the transaction in minor currency. For the UK, this is pence, so £10.99 should be sent as 1099.  <b>Numeric values only – no decimal points or currency symbols.</b>
<b>action</b>	Yes	The transaction action.  Possible values are:  <b>PREAUTH</b>  This will reserve an amount from the customer’s card but not collect them. For a period of up to 5 days (depending on the card issuing bank) after the transaction is placed, you can place a subsequent transaction with an action of SALE and the xref value returned from the first transaction in order to collect the previously reserved funds – This subsequent transaction is usually preformed using a direct integration.  If the period of time between the first and second transactions is greater than the card issuing bank

		<p>reserves the funds for, then new, unreserved funds will be taken from the cardholders account.</p> <p><b>SALE</b></p> <p>This will collect an amount from the customer's card.</p>
<b>type</b>	Yes	<p>The type of transaction.</p> <p>Possible values are:</p> <p><b>1</b> - Cardholder Not Present: Ecommerce.  <b>2</b> - Cardholder Not Present: Mail Order.  <b>3</b> - Point of Sale: Card Keyed.  <b>4</b> - Point of Sale: Card Swiped.  <b>5</b> - Point of Sale: Card Chip &amp; Pin.</p>
<b>countryCode</b>	Yes	ISO standard country code for the merchant's location.
<b>currencyCode</b>	Yes	ISO standard currency code for this transaction. You may only use currencies that are enabled for your merchant account.
<b>transactionUnique</b>	No	A unique identifier for this transaction. This should be set by your website or shopping cart. This is an added security feature to combat transaction spoofing.
<b>orderRef</b>	No	This text field allows you to describe the order or provide an invoice number/reference number for the merchant's records.

## 2.2 Redirection and Verification Fields

The Hosted Form, after completion, will redirect the customer to the **redirectURL**, which will be called with POST data attached. Since this POST could conceivably be forged by a malicious user, it is a good idea to also supply a **callbackURL**. If supplied, the Hosted Form will POST the same transaction result data to the Callback URL in the background. This background page should be used to update your database.

Field Name	Mandatory?	Description
<b>redirectURL</b>	Yes	The URL to which the customer will be redirected and the transaction result will be POSTed.
<b>callbackURL</b>	No (Recommended)	A non-public URL which will receive a copy of the transaction result by POST.

## 2.3 Customer Details Fields

Customer details are optional by default, however if the merchant has chosen to require AVS checking in their preferences, then **customerAddress** and **customerPostCode** become mandatory. All data is stored and accessible within the administration panel.

Field Name	Mandatory?	Description
<b>customerName</b>	No	The customer or cardholder's name.
<b>customerAddress</b>	Yes, if AVS enabled	The customer or cardholder's address. For AVS checking this must be the registered billing address of the card.
<b>customerPostCode</b>	Yes, if AVS enabled	The customer or cardholder's post code. For AVS checking this must be the registered billing post code of the card.
<b>customerEmail</b>	No	The customer's email address.
<b>customerPhone</b>	No	The customer's telephone number.



## 2.4 American Express and Diners Card Fields

American Express or Diners Card cards require additional information about the customer's purchase to be posted to the hosted form. Only one order line needs to be entered. For other card types all items are optional and will be stored for reference purpose only.

Field Name	Mandatory?	Description
item1Description	Yes <sup>†</sup>	A short text description of the item.
item1Quantity	Yes <sup>†</sup>	The quantity of the item purchased.
item1GrossValue	Yes <sup>†</sup>	The gross, or tax inclusive, value of this order line.
item2Description	No	A short text description of the item.
item2Quantity	No	The quantity of the item purchased.
item2GrossValue	No	The gross, or tax inclusive, value of this order line.
item3Description	No	A short text description of the item.
item3Quantity	No	The quantity of the item purchased.
item3GrossValue	No	The gross, or tax inclusive, value of this order line.
item4Description	No	A short text description of the item.
item4Quantity	No	The quantity of the item purchased.
item4GrossValue	No	The gross, or tax inclusive, value of this order line.
item5Description	No	A short text description of the item.
item5Quantity	No	The quantity of the item purchased.
item5GrossValue	No	The gross, or tax inclusive, value of this order line.

<sup>†</sup>These fields are only mandatory if an American Express or Diners Card is used for payment.

With American Express or Diners Cards you may also provide tax **or** discount information. Once again for other cards types any values provided will be stored for reference purposes only.

Field Name	Mandatory?	Description
<code>taxValue</code>	No	The total amount of tax for this order.
<code>taxDiscountDescription</code>	No	A text field to describe the tax applied (e.g. "VAT at 20%")

*OR*

Field Name	Mandatory?	Description
<code>discountValue</code>	No	The total amount of discount applied to this order.
<code>taxDiscountDescription</code>	No	A text field to describe the discount applied.

## 2.5 Merchant Data Field

The merchant may send arbitrary data with the request by appending extra fields which will be returned in the response unmodified. These extra fields are merely 'echoed' back and not stored by Pay Global.

However the Merchant can put extra information that should be stored into a **merchantData** field. Associative data can be serialised using the notation **merchantData [name]=value**.

Field Name	Mandatory?	Description
<code>merchantData</code>	No	Arbitrary data to be stored along with this transaction.

### 3 Gateway Response

The Pay Global Hosted Form method returns data to the Redirect URL (and Callback URL, if supplied) via an HTTP POST request. The details are sent URL encoded Name=Value fields separated by ‘&’ characters (refer to RFC 1738 and the application/x-www-form-urlencoded media type).

The fields initially sent to the integration URL are returned and in addition the following fields may be returned.

*Please note that the field names are cAsE sEnSiTiVe.*

#### 3.1 Response Fields

Field Name	Returned?	Description
<b>responseCode</b>	Always	A numeric code providing the outcome of the transaction.  Possible values are:  <b>0</b> - Successful / authorised transaction. <b>2</b> - Card referred. <b>4</b> - Card declined – keep card <b>5</b> - Card declined.  Check <b>responseMessage</b> for more detail or any error that occurred.  For a full list of error codes please refer to the table in Appendix A.
<b>responseMessage</b>	Always	The message received from the acquiring bank, or any error message.
<b>signature</b>	Always	The hash used to sign the transaction reply.
<b>xref</b>	Always	The merchant may store the cross reference for repeat transactions and refunds.
<b>transactionUnique</b>	If supplied	The value supplied in the initial request, if any.
<b>amountReceived</b>	On success	The amount of the transaction. This field used in conjunction with <b>transactionUnique</b> can help provide a measure of security.
<b>transactionID</b>	Always	The ID of the transaction on the Pay Global system – can be used to easily reconcile transactions in the administration panel.

<b>orderRef</b>	If supplied	The value supplied in the initial request, if any.
<b>avscv2ResponseCode</b>	Optional	The result of the AVS/CV2 check. Please see Appendix A-4 for a full list of possible responses.
<b>avscv2ResponseMessage</b>	Optional	The message received from the acquiring bank, or any error message with regards to the AVS/CV2 check. Please see Appendix A-4 for a full list of possible responses.
<b>cv2Check</b>	Optional	Textual description of the AVS/CV2 CV2 check as described in Appendix A-4.  Possible values are: <b>'not known'</b> , <b>'not checked'</b> , <b>'matched'</b> , <b>'not matched'</b> , <b>'partially matched'</b>
<b>addressCheck</b>	Optional	Textual description of the AVS/CV2 address check as described in Appendix A-4.  Possible values are: <b>'not known'</b> , <b>'not checked'</b> , <b>'matched'</b> , <b>'not matched'</b> , <b>'partially matched'</b>
<b>postcodeCheck</b>	Optional	Textual description of the AVS/CV2 postcode check as described in Appendix A-4.  Possible values are: <b>'not known'</b> , <b>'not checked'</b> , <b>'matched'</b> , <b>'not matched'</b> , <b>'partially matched'</b>
<b>avscv2AuthEntity</b>	Optional	Textual description of the AVS/CV2 authorizing entity.  Possible values are: <b>'not known'</b> , <b>'merchant host'</b> , <b>'acquirer host'</b> , <b>'card scheme'</b> , <b>'issuer'</b>
<b>cardNumberMask</b>	Always	Card number masked so only the last 4 digits are visible - for example:  *****1234
<b>cardTypeCode</b>	Always	The code of card used. See appendix A-2 for a full list.
<b>cardType</b>	Always	The description of the card used. See Appendix A-2 for a full list.

### 3.2 3D Secure Fields

When a 3D Secure transaction is processed then the following additional fields may be returned.

Field Name	Returned?	Description
<b>threeDSEnabled</b>	Yes	The 3D Secure status of the merchant account.  Possible values are: <b>N</b> – the merchant is not 3DS enabled <b>Y</b> – the merchant is 3DS enabled
<b>threeDSEnrolled</b>	Yes	The 3D Secure enrolment status for the credit card.  Possible values are: <b>Y</b> - Enrolled. <b>N</b> - Not Enrolled. <b>U</b> - Unable To Verify <b>E</b> - Error Verifying Enrolment.  Refer to Appendix 3.2A-4 for further information.
<b>threeDSAAuthenticated</b>	No	The 3D Secure authentication status for the credit card.  Possible values are: <b>Y</b> - Authentication Successful. <b>N</b> - Not Authenticated. <b>U</b> - Unable To Authenticate. <b>A</b> - Attempted Authentication. <b>E</b> - Error Checking Authentication.  Refer to Appendix 3.2A-4 for further information.
<b>threeDSPaReq</b>	No	Payer Authentication Request (PaReq) that is sent to the Access Control Server (ACS) in order to verify the 3D Secure status of the credit card.
<b>threeDSPaRes</b>	No	Payer Authentication Response (PaRes) that is returned from the Access Control Server (ACS) determining the 3D Secure status of the credit card.
<b>threeDSACSURL</b>	No	The URL of the Access Control Server (ACS) to which the Payer Authentication Request (PaReq) should be sent.
<b>threeDSECI</b>	No	This contains a two digit Electronic Commerce Indicator (ECI) value, which is to be submitted

		<p>in a credit card authorization message.</p> <p>This value indicates to the processor that the customer data in the authorization message has been authenticated.</p> <p>The data contained within this property is only valid if the <b>threeDSAuthenticated</b> value is <b>Y</b> or <b>A</b>.</p>
<b>threeDSCAVV</b>	No	<p>This contains a 28-byte Base-64 encoded Cardholder Authentication Verification Value (CAVV).</p> <p>The data contained within this property is only valid if the <b>threeDSAuthenticated</b> value is <b>Y</b> or <b>A</b>.</p>
<b>threeDSCAVVAlgorithm</b>	No	<p>This contains the one digit value which indicates the algorithm used by the Access Control Server (ACS) to generate the CAVV.</p> <p>Valid algorithms include (amongst others):  <b>0</b> - HMAC  <b>1</b> - CVV  <b>2</b> - CVV with ATN</p> <p>The data contained within this property is only valid if the <b>threeDSAuthenticated</b> value is <b>Y</b> or <b>A</b>.</p>
<b>threeDSXID</b>	No	<p>A unique identifier for the transaction as used in the 3D Secure process. This is normally a 20 character string.</p>
<b>threeDSErrorCode</b>	No	<p>Any error response code returned by the 3D Secure Access Control Server (ACS) should there be an error in determining the cards 3D Secure status.</p>
<b>threeDSErrorDescription</b>	No	<p>Any error response description returned by the 3D Secure Access Control Server (ACS) should there be an error in determining the cards 3D Secure status.</p>
<b>threeDSMerchantPref</b>	No	<p>Any merchant 3D Secure preference used to block or allow this transaction should the card not be authorized. These preferences can be set in the merchant control panel.</p>
<b>threeDSVETimestamp</b>	No	<p>The time the card was checked for 3D Secure enrolment.</p>
<b>threeDSCATimestamp</b>	No	<p>The time the card was checked for 3D Secure authentication.</p>

## A-1 Response Codes

The gateway will always issue a **responseCode** to report the status of the transaction. These codes should be used rather than the **responseMessage** field to determine the outcome of a transaction.

A zero response code always indicates a successful outcome.

Response codes are grouped as follows, the groupings are for informational purposes only and not all codes in a group are used;

Acquirer (FI) Error codes: 1-99	
Code	Description
<b>0</b>	Successful / authorised transaction. Any code other than <b>0</b> indicates an unsuccessful transaction
<b>2</b>	Card referred
<b>4</b>	Card declined – keep card
<b>5</b>	Card declined
<b>30</b>	An error occurred. Check <b>responseMessage</b> for more detail

General Error Codes: 65536 - 65791	
Code	Description
<b>65536</b>	Transaction in progress. Refer to Pay Global if this error occurs
<b>65537</b>	Reserved for future use. Refer to Pay Global if this error occurs
<b>65538</b>	Reserved for future use. Refer to Pay Global if this error occurs
<b>65539</b>	Invalid Credentials: <b>merchantID</b> is unknown
<b>65540</b>	Permission denied: caused by sending a request from an unauthorized IP address
<b>65541</b>	Reserved for future use. Refer to Pay Global if this error occurs
<b>65542</b>	Request Mismatch: fields sent while completing a request do not match initially requested values. Usually due to sending different card details when completing a 3D Secure transaction to those used to authorise the transaction
<b>65543</b>	Request Ambiguous: request could be misinterpreted due to inclusion of mutually

	exclusive fields
<b>65544</b>	Request Malformed: couldn't parse the request data
<b>65545</b>	Suspended Merchant account
<b>65546</b>	Currency not supported by Merchant
<b>65547</b>	Request Ambiguous, both <b>taxValue</b> and <b>discountValue</b> provided when should be one only
<b>65548</b>	Database error
<b>65549</b>	Payment processor communications error
<b>65550</b>	Payment processor error
<b>65551</b>	Internal communications error
<b>65552</b>	Internal error

#### 3D Secure Error Codes: 65792 - 66047

Code	Description
<b>65792</b>	3D Secure transaction in progress. Refer to Pay Global if this error occurs
<b>65793</b>	Unknown 3D Secure Error
<b>65794</b>	3D Secure processing is unavailable. Merchant account doesn't support 3D Secure
<b>65795</b>	3D Secure processing is not required for the given card
<b>65796</b>	3D Secure processing is required for the given card
<b>65797</b>	Error occurred during 3D Secure enrolment check
<b>65798</b>	Reserved for future use. Refer to Pay Global if this error occurs
<b>65799</b>	Reserved for future use. Refer to Pay Global if this error occurs
<b>65800</b>	Error occurred during 3D Secure authentication check
<b>65801</b>	Reserved for future use. Refer to Pay Global if this error occurs
<b>65802</b>	3D Secure authentication is required for this card
<b>65803</b>	3D Secure enrolment or authentication failure and Merchant 3DS preferences are to STOP processing



Missing Request Field Error Codes: 66048 - 66303	
Code	Description
<b>66048</b>	Missing request. No data posted to integration URL
<b>66049</b>	Missing <b>merchantID</b> field
<b>66050</b>	Reserved for future use. Refer to Pay Global if this error occurs.
<b>66051</b>	Reserved for internal use. Refer to Pay Global if this error occurs
<b>66052</b>	Reserved for internal use. Refer to Pay Global if this error occurs
<b>66053</b>	Reserved for internal use. Refer to Pay Global if this error occurs
<b>66054</b>	Reserved for internal use. Refer to Pay Global if this error occurs
<b>66055</b>	Missing <b>action</b> field
<b>66056</b>	Missing <b>amount</b> field
<b>66057</b>	Missing <b>currencyCode</b> field
<b>66058</b>	Missing <b>cardNumber</b> field
<b>66059</b>	Missing <b>cardExpiryMonth</b> field
<b>66060</b>	Missing <b>cardExpiryYear</b> field
<b>66061</b>	Missing <b>cardStartMonth</b> field (reserved for future use)
<b>66062</b>	Missing <b>cardStartYear</b> field (reserved for future use)
<b>66063</b>	Missing <b>cardIssueNumber</b> field (reserved for future use)
<b>66064</b>	Missing <b>cardCVV</b> field
<b>66065</b>	Missing <b>customerName</b> field
<b>66066</b>	Missing <b>customerAddress</b> field
<b>66067</b>	Missing <b>customerPostCode</b> field
<b>66068</b>	Missing <b>customerEmail</b> field
<b>66069</b>	Missing <b>customerPhone</b> field (reserved for future use)
<b>66070</b>	Missing <b>countyCode</b> field

66071	Missing <b>transactionUnique</b> field (reserved for future use)
66072	Missing <b>orderRef</b> field (reserved for future use)
66073	Missing <b>remoteAddress</b> field (reserved for future use)
66074	Missing <b>redirectURL</b> field
66075	Missing <b>callbackURL</b> field (reserved for future use)
66076	Missing <b>merchantData</b> field (reserved for future use)
66077	Missing <b>origin</b> field (reserved for future use)
66078	Missing <b>duplicateDelay</b> field (reserved for future use)
66079	Missing <b>itemQuantity</b> field (reserved for future use)
66080	Missing <b>itemDescription</b> field (reserved for future use)
66081	Missing <b>itemGrossValue</b> field (reserved for future use)
66082	Missing <b>taxValue</b> field (reserved for future use)
66083	Missing <b>discountValue</b> field (reserved for future use)
66084	Missing <b>taxDiscountDescription</b> field (reserved for future use)
66085	Missing <b>xref</b> field (reserved for future use)
66086	Missing <b>type</b> field (reserved for future use)
66087	Reserved for future use
66088	Reserved for future use
66089	Missing <b>transactionID</b> field (reserved for future use)
66090	Missing <b>threeDSRequired</b> field (reserved for future use)
66091	Missing <b>threeDSMD</b> field (reserved for future use)
66092	Missing <b>threeDSPaRes</b> field
66093	Missing <b>threeDSECI</b> field
66094	Missing <b>threeDSCAVV</b> field
66095	Missing <b>threeDSXID</b> field

Invalid Request Field Error Codes: 66304 - 66559	
Code	Description
66304	Invalid request
66305	Invalid <code>merchantID</code> field
66306	Reserved for future use. Refer to Pay Global if this error occurs
66307	Reserved for internal use. Refer to Pay Global if this error occurs
66308	Reserved for internal use. Refer to Pay Global if this error occurs
66309	Reserved for internal use. Refer to Pay Global if this error occurs
66310	Reserved for internal use. Refer to Pay Global if this error occurs
66311	Invalid <code>action</code> field
66312	Invalid <code>amount</code> field
66313	Invalid <code>currencyCode</code> field
66314	Invalid <code>cardNumber</code> field
66315	Invalid <code>cardExpiryMonth</code> field
66316	Invalid <code>cardExpiryYear</code> field
66317	Invalid <code>cardStartMonth</code> field
66318	Invalid <code>cardStartYear</code> field
66319	Invalid <code>cardIssueNumber</code> field
66320	Invalid <code>cardCVV</code> field
66321	Invalid <code>customerName</code> field
66322	Invalid <code>customerAddress</code> field
66323	Invalid <code>customerPostCode</code> field
66324	Invalid <code>customerEmail</code> field
66325	Invalid <code>customerPhone</code> field
66326	Invalid <code>countyCode</code> field

66327	Invalid <b>transactionUnique</b> field (reserved for future use)
66328	Invalid <b>orderRef</b> field (reserved for future use)
66329	Invalid <b>remoteAddress</b> field
66330	Invalid <b>redirectURL</b> field
66331	Invalid <b>callbackURL</b> field (reserved for future use)
66332	Invalid <b>merchantData</b> field (reserved for future use)
66333	Invalid <b>origin</b> field (reserved for future use)
66334	Invalid <b>duplicateDelay</b> field (reserved for future use)
66335	Invalid <b>itemQuantity</b> field
66336	Invalid <b>itemDescription</b> field
66337	Invalid <b>itemGrossValue</b> field
66338	Invalid <b>taxValue</b> field
66339	Invalid <b>discountValue</b> field
66340	Invalid <b>taxDiscountDescription</b> field (reserved for future use)
66341	Invalid <b>xref</b> field
66342	Invalid <b>type</b> field
66343	Reserved for future use
66344	Reserved for future use
66345	Invalid <b>transactionID</b> field
66356	Invalid <b>threeDSRequired</b> field
66347	Invalid <b>threeDSMD</b> field
66348	Invalid <b>threeDSPaRes</b> field
66349	Invalid <b>threeDSECI</b> field
66350	Invalid <b>threeDSCAVV</b> field
66351	Invalid <b>threeDSXID</b> field

<b>66416</b>	Invalid card expiry date. Must be a date sometime in the next 10 years
<b>66417</b>	Invalid card start date. Must be a date sometime in the last 10 years
<b>66418</b>	Invalid item count. Tried to supply more than 6 line item details
<b>66419</b>	Invalid item sequence. Out of sequence line item details

## A-2 Types of card

The following is a list of card types which may be returned by the gateway.

Card Code	Card Type
AM	American Express
CF	Clydesdale Financial Services
DI	Diners Club
EL	Electron
JC	JCB
MA	International Maestro
MC	Mastercard
SO	Solo
ST	Style
SW	Domestic Maestro (Formerly Switch)
VC	Visa Credit
VD	Visa Debt
VP	Visa Purchasing

## A-3 AVS / CV2 Check Response

The AVS/CV2 Check Response Message field **avscv2ResponseMessage** is sent back in the raw form that is received from the acquiring bank and can contain the following values:

Response	Description
<b>ALL MATCH</b>	AVS and CV2 match.
<b>SECURITY CODE MATCH ONLY</b>	CV2 match only.
<b>ADDRESS MATCH ONLY</b>	AVS match only.
<b>NO DATA MATCHES</b>	No matches for AVS and CV2.
<b>DATA NOT CHECKED</b>	Supplied data not checked.
<b>SECURITY CHECKS NOT SUPPORTED</b>	Card scheme does not support checks.

The AVS/CV2 Response Code **avscv2ResponseCode** is made up of six characters and is sent back in the raw form that is received from the acquiring bank. The first 4 characters can be decoded as below, the remaining 2 characters are currently reserved for future use:

Position 1 Value	Description
<b>0</b>	No additional information available.
<b>1</b>	CV2 not checked.
<b>2</b>	CV2 matched.
<b>4</b>	CV2 not matched.
<b>8</b>	Reserved.

Position 2 Value	Description
0	No additional information available.
1	Postcode not checked.
2	Postcode matched.
4	Postcode not matched.
8	Postcode partially matched.

Position 3 Value	Description
0	No additional Information.
1	Address numeric not checked.
2	Address numeric matched.
4	Address numeric not matched.
8	Address numeric partially matched.

Position 4 Value	Description
0	Authorising entity not known.
1	Authorising entity – merchant host.
2	Authorising entity – acquirer host.
4	Authorising entity – card scheme.
8	Authorising entity – issuer.



## **A-4 3D Secure Enrolment/Authentication Codes**

The 3D Secure enrolment check field **threeDSEnrolled** can return the following values:

- Y - Enrolled:** The card is enrolled in the 3D Secure program and the payer is eligible for authentication processing.
- N - Not Enrolled:** The checked card is eligible for the 3D Secure (it is within the card association's range of accepted cards) but the card issuing bank does not participate in the 3D Secure program. If the cardholder later disputes the purchase, the issuer may not submit a chargeback to the merchant.
- U - Unable To Verify Enrolment:** The card associations were unable to verify if the cardholder is registered. As the card is ineligible for 3D Secure, merchants can choose to accept the card nonetheless and precede the purchase as non-authenticated and submits authorization with ECI 7. The Acquirer/Merchant retains liability if the cardholder later disputes making the purchase.
- E - Error Verify Enrolment:** The Pay Global system encountered an error. This card is flagged as 3D Secure ineligible. The card can be accepted for payment, yet the merchant may not claim a liability shift on this transaction in case of a dispute with the cardholder.

The 3D Secure authentication check field **threeDSAAuthenticated** can return the following values:

- Y - Authentication Successful:** The Issuer has authenticated the cardholder by verifying the identity information or password. A CAVV and an ECI of 5 is returned. The card is accepted for payment.
- N - Not Authenticated:** The cardholder did not complete authentication and the card should not be accepted for payment.
- U - Unable To Authenticate:** The authentication was not completed due to technical issues or another problem. A transmission error prevented authentication from completing. The card should be accepted for payment but no authentication data will be passed on to authorization processing and no liability shift will occur.
- A - Attempted Authentication:** A proof of authentication attempt was generated. The cardholder is not participating, but the attempt to authenticate was recorded. The card should be accepted for payment and authentication information passed to authorization processing.
- E - Error Checking Authentication:** The Pay Global system encountered an error. The card should be accepted for payment but no authentication information will be passed to authorization processing and no liability shift will occur.

## A-5 Example Code

The following example shows how to send the initial request using a HTML form to POST the data to the Pay Global integration URL:

/myshop/orderconfirmation.php:

```
<?php
// PreShared Key entered on MMS. The demo accounts is fixed, but merchant accounts can
be updated from the MMS.
$pre_shared_key = "Drawn34Salmon43Speed";

$fields = array(
    "merchantID"      =>    "101661",
    "amount"          =>    "1050",
    "countryCode"     =>    "826",
    "currencyCode"    =>    "826",
    "transactionUnique" =>    "AZ2045-PY",
    "orderRef"        =>    "Groceries",
    "redirectURL"     =>    "http://www.shop.com/ordercomplete.php"
);

// Sort the array
ksort($fields);

?>
<form action="https://gateway.payglobal.org/paymentform/" method="post">
<input type="hidden" name="merchantID" value="101661" />
<input type="hidden" name="amount" value="1050" />
<input type="hidden" name="countryCode" value="826" />
<input type="hidden" name="currencyCode" value="826" />
<input type="hidden" name="transactionUnique" value="AZ2045-PY" />
<input type="hidden" name="orderRef" value="Groceries" />
<input type="hidden" name="redirectURL" value="http://www.shop.com/ordercomplete.php"
/>
<input type="hidden" name="signature" value="<?= hash("SHA512",
http_build_query($fields) . $pre_shared_key) ?>" />
<input type="submit" value="Pay Now" />
</form>
```

When the user submits the form their browser will be taken to the Pay Global integration page at <https://gateway.payglobal.org/paymentform/> where the user will be given the option to enter their card details and billing address. If additional customer or transaction information is supplied in the HTTP POST request, then the values sent will be used to populate the initial values of the controls on the Pay Global hosted form. When the customer submits this hosted form the transaction will be attempted and the results sent as a HTTP POST request to the specified **redirectURL** an example of which is given below:

/myshop/ordercomplete.php:

```
if( $_POST['responseCode'] === "0" ) {

    echo "<p>Thank you for your payment</p>";

}else{

    echo "<p>Failed to take payment: " . htmlentities($_POST['responseMessage']) .
"</p>";

}
```

## A-6 Test Cards

The expiry date used for each test card should be December of the current year; in two digit format – E.g. 12/15 for December 2015

The authorisation response is dependent on the transaction amount:

Amount range from	Amount range to	Expected response
101 (£1.01)	4999 (£49.99)	AUTH CODE: XXXXXX
5000 (£50.00)	9999 (£99.99)	CARD REFERRED
10000 (£100.00)	14999 (£149.99)	CARD DECLINED
15000+ (£150.00+)		CARD DECLINED – KEEP CARD*

\* If applicable to transaction / merchant / acquirer type

### Visa Credit

Card Number	CVV Number	Address
4929421234600821	356	Flat 6 Primrose Rise 347 Lavender Road Northampton NN17 8YG
4543059999999982	110	76 Roseby Avenue Manchester M63X 7TH
4543059999999990	689	23 Rogerham Mansions 4578 Ermine Street Borehamwood WD54 8TH

### Visa Debit

Card Number	CVV Number	Address
4539791001730106	289	Unit 5 Pickwick Walk 120 Uxbridge Road Hatch End Middlesex HA6 7HJ
4462000000000003	672	Mews 57 Ladybird Drive Denmark 65890

**MasterCard Credit**

Card Number	CVV Number	Address
5301250070000191	419	25 The Larches Narborough Leicester LE10 2RT
5413339000001000	304	Pear Tree Cottage The Green Milton Keynes MK11 7UY
5434849999999951	470	34a Rubbery Close Cloisters Run Rugby CV21 8JT
5434849999999993	557	4-7 The Hay Market Grantham NG32 4HG

**MasterCard Debit**

Card Number	CVV Number	Address
5573 4712 3456 7898	159	Merevale Avenue Leicester LE10 2BU

**UK Maestro**

Card Number	CVV Number	Address
6759 0150 5012 3445 002	309	The Parkway 5258 Larches Approach Hull North Humberside HU10 5OP
6759 0168 0000 0120 097	701	The Manor Wolvey Road Middlesex TW7 9FF

**JCB**

Card Number	CVV Number	Address
3540599999991047	209	2 Middle Wallop Merideth-in-the-Wolds Lincolnshire LN2 8HG

**Electron**

Card Number	CVV Number	Address
4917480000000008	009	5-6 Ross Avenue Birmingham B67 8UJ

**American Express**

Card Number	CVV Number	Address
374245455400001	4887	The Hunts Way Southampton SO18 1GW

**Diners Club**

Card Number
36432685260294

## A-7 3D Secure Test Cards

3D Secure test cards for MasterCard using SecureCode

The expiry date used for each test card should be December of the current year; in two digit format – E.g. 12/15 for December 2015

Card Number	CVV Number	Address	Postcode	Amount	Test Scenario
503396198900000818	332	31	18	£11.01	Enrolled International Maestro account number – valid SecureCode (multiple cardholder). Select 'MEGAN SANDERS' with SecureCode password: secmegan1
5453010000070789	508	20	52	£11.02	Enrolled account number - valid SecureCode (single) SecureCode password: sechal1
5453010000070151	972	22	08	£11.03	Enrolled account number – mixed SecureCode (multi) SecureCode password: Hannah – sechannah1 (bad) Haley – sechaley1 (good)
5453010000070284	305	35	232	£11.04	Enrolled account number – invalid SecureCode Invalid SecureCode password: invseccode
5453010000084103	470	73	170	£11.05	Attempts processing
5453010000070888	233	1	248	£11.06	Account number not enrolled
5199992312641465	006	21	14	£11.07	Card range not participating

3D Secure test cards for Visa using Verified by Visa

The expiry date used for each test card should be December of the current year; in two digit format – E.g. 12/15 for December 2015

Card Number	CVV Number	Address	Postcode	Amount	Test Scenario
4909630000000008				£12.01	Card range not participating
401201000000000009				£12.02	Card registered with VbV (automated ACS response – click on Submit button)
4012001037141112	083	16	155	£12.03	Card registered with Visa (automated ACS response – click on Submit button)

4012001037484447	450	200	19	£12.04	Failed authentication – issuer database unavailable
4015501150000216				£12.05	Attempts processing (automated ACS response – click on Submit button)

## A-8 Signing Your Request

A message can be signed by hashing the whole URL encoded Name=Value request string with a secret passphrase appended. This security passphrase can be configured on a per merchant account basis in the Merchant Management System (MMS).

Care must be taken to normalise any embedded line ending to just use a single New Line character (ascii character 10).

Various hashing algorithms are supported allowing you to choose the one most suitable for your integration language. SHA512 is the default and preferred, if using an algorithm other than SHA512 then the algorithm name should be pre-pended to the hash enclosed in braces.

The following algorithms are supported (from most secure to least secure order): SHA512, SHA256, SHA1, MD5, CRC32.

The hash must be sent in the signature field. This field must not be included in the message that is used to generate the hash.

Note: when a secret is configured for the merchant account then every message must be signed – failure to sign a message will cause it to be rejected due to a missing signature. The gateway will also sign any response and any details POSTed to any Callback URL using the same signature allowing the merchant to verify that any response has not been tampered with.