PAY BUTTON

USER GUIDE

Version: 1.3

1 About Pay Button 3
2 Using the Pay Button Creator 3
2.1 Fields 4
2.2 Inserting the Link/QR Code 7
3 Advanced Integration 12
3.1 Advanced Integration 12
3.1.1 About This Guide 12
3.1.2 New Customers Testing 12
3.1.3 Pre-Requisites 13
3.1.4 3D Secure 13
3.1.5 Test Cards 13
3.2 Gateway Request 14
3.2.1 General Fields 14
3.2.2 Redirection and Verification Fields 17
3.2.3 Customer Details Fields 18
3.2.4 American Express and Diners Card Fields 19
3.2.5 Merchant Data Field 20
3.3 Gateway Response 22
3.3.1 Response Fields 22
3.3.2 3D Secure Fields 24
A-1 Response Codes 28
A-2 Types of Card 36
A-3 AVS / CV2 Check Response 37
A-4 3D Secure Enrolment/Authentication Codes 39
A-5 Example Code 40
A-6 Signing Your Request 42

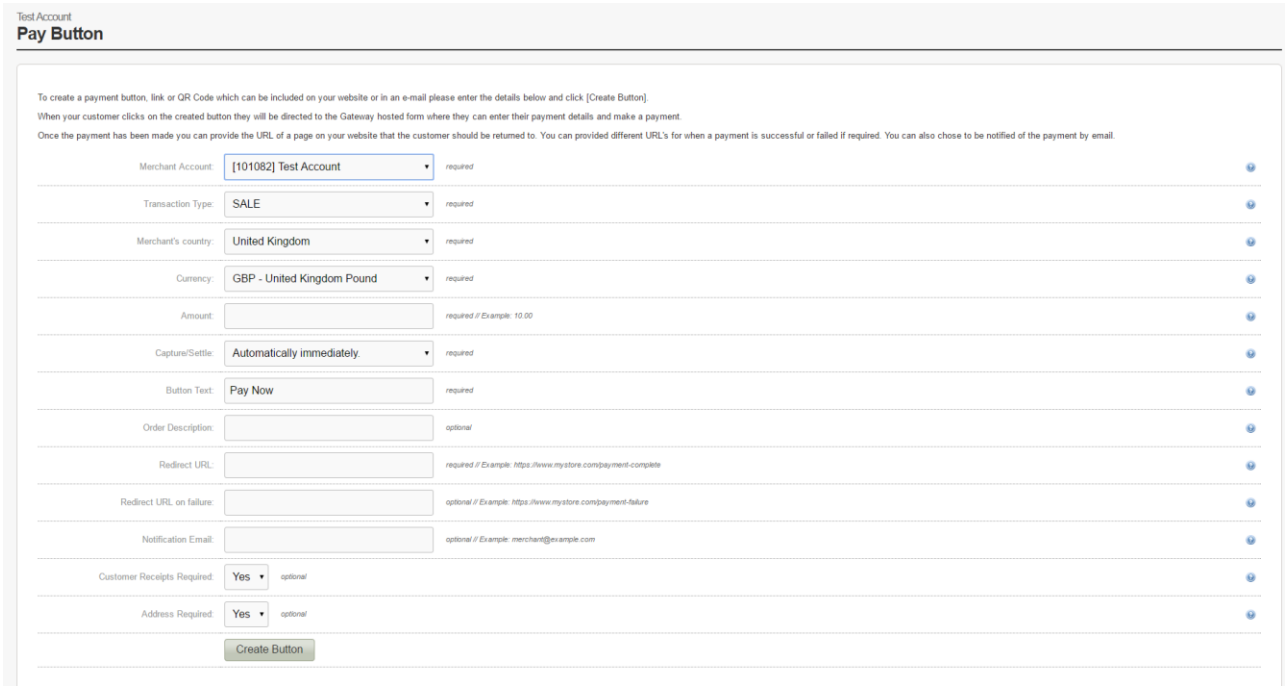
1 About Pay Button

The *Pay Button* function gives the user the ability to create an HTML link that can be embedded into HTML content (e.g. a website or HTML email). When clicked, it will allow a payment to be taken via the hosted form that will be pre-populated with the data specified when creating the link.

The advantage of *Pay Button* is that it offers the functionality of the Gateway without having to complete a Hosted or Direct integration, meaning it can be included in basic HTML without the need for any scripting languages.

2 Using the Pay Button Creator

The *Pay Button* creation page can be accessed via the *Pay Button* menu item on the main menu in the MMS (Merchant Management System).



2.1 Fields

Merchant Account	Required	This specifies the Merchant Account to receive the payments into. The list will show all your merchant accounts and a default test account.
Merchant Password	Required if set	This field is only presented if the account already has a merchant password setup via the preferences page. We advise using signatures instead which are handled automatically when the button is created if a signature key is set using the preferences page.
Transaction Type	Required	This specifies the Transaction Type between SALE, PREAUTH and VERIFY. * **These transaction types depend on the Merchants and Acquirers set-up.*
Country	Required	The country in which the merchant is based.
Currency	Required	This is the currency for the transactions. The list will show all the currencies that the selected Merchant Account can handle.
Amount	Required	The amount due for payment by the customer. NOTE: The value should be given without the currency symbol, e.g. 10.00.
Capture/Settle	Required	This specifies whether or not the funds should be captured immediately, in (x) amount of days or manually when required.

Button Text	Required	This is the value to display as the link text.
Order Reference	Optional	This value will be logged with any transaction made using the link and will be shown in the MMS. It can be used for order tracking, etc.
Redirect URL	Required	The location to go to after the payment has taken place. This can be any URL you wish to direct the customer to after a payment or attempted payment has been made. NOTE: If a value for Redirect URL on Failure is supplied, the URL specified for Redirect URL will only be used when a payment has been successful.
Redirect URL on Failure	Optional	The location to go after a payment has failed. If no value is supplied the value from Redirect URL will be used.
Notification Email	Optional	If a payment is successful, a notification email will be sent to this address. If left blank, then the default notification email address set in the preferences page for the merchant account will be used.
Customer Receipts Required	Optional	If set to 'Yes' and the payment is successful, a notification email will be sent to the Customer if they supply a valid e-mail address during checkout.
Address Required	Optional	If set to 'Yes', the 'Address' and 'Postcode' sections on the hosted form are marked as required and cannot be omitted. If set to 'No', the

		'Address' and 'Postcode' fields are optional. The default value for this field is 'No'.

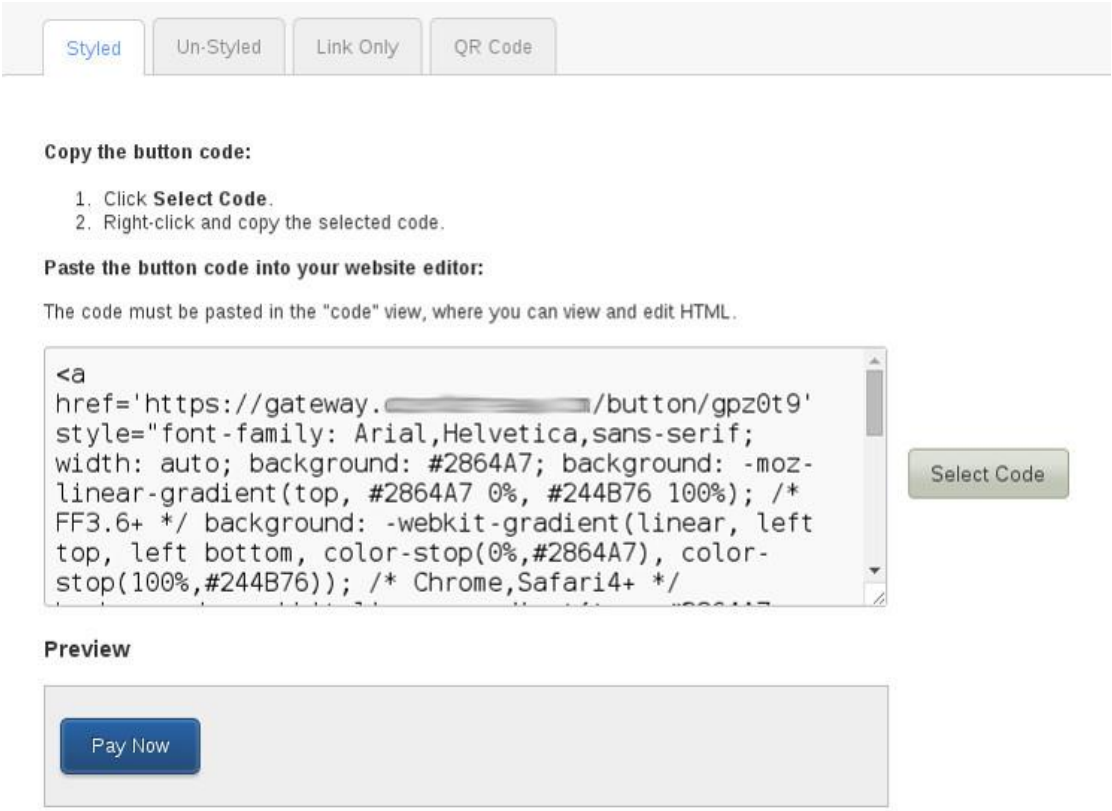
2.2 Inserting the Link/QR Code

Once 'Create Button' has been clicked, the link will be formatted and displayed on the next page.

There are 4 options presented: Styled, Un-Styled, Link only and QR Code which can be selected using the tabs on the page. Previews of all the styling options can be seen in the Preview window.

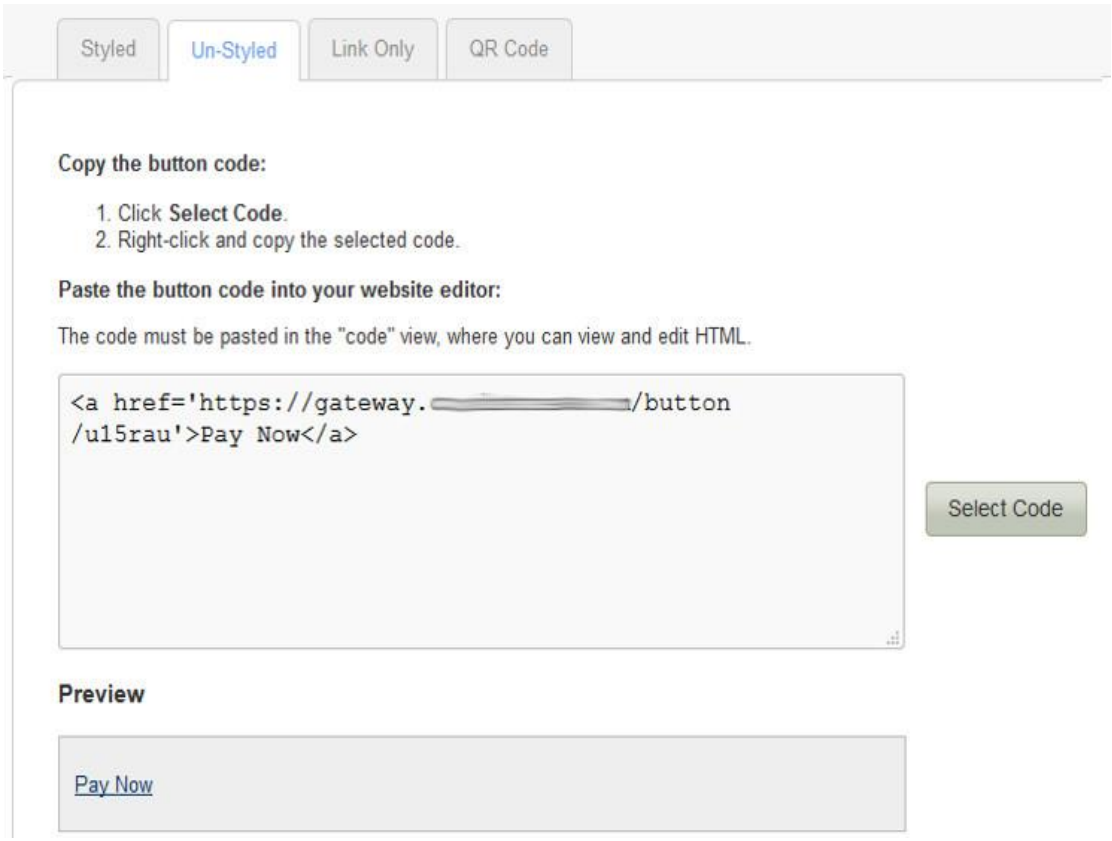
To insert the code into HTML content, click the Select Code button and then right click and copy the selected code. The code must be pasted into the code view of your HTML content, where you can view and edit the raw HTML and edit any inline CSS. The link will then be ready for use.

Styled



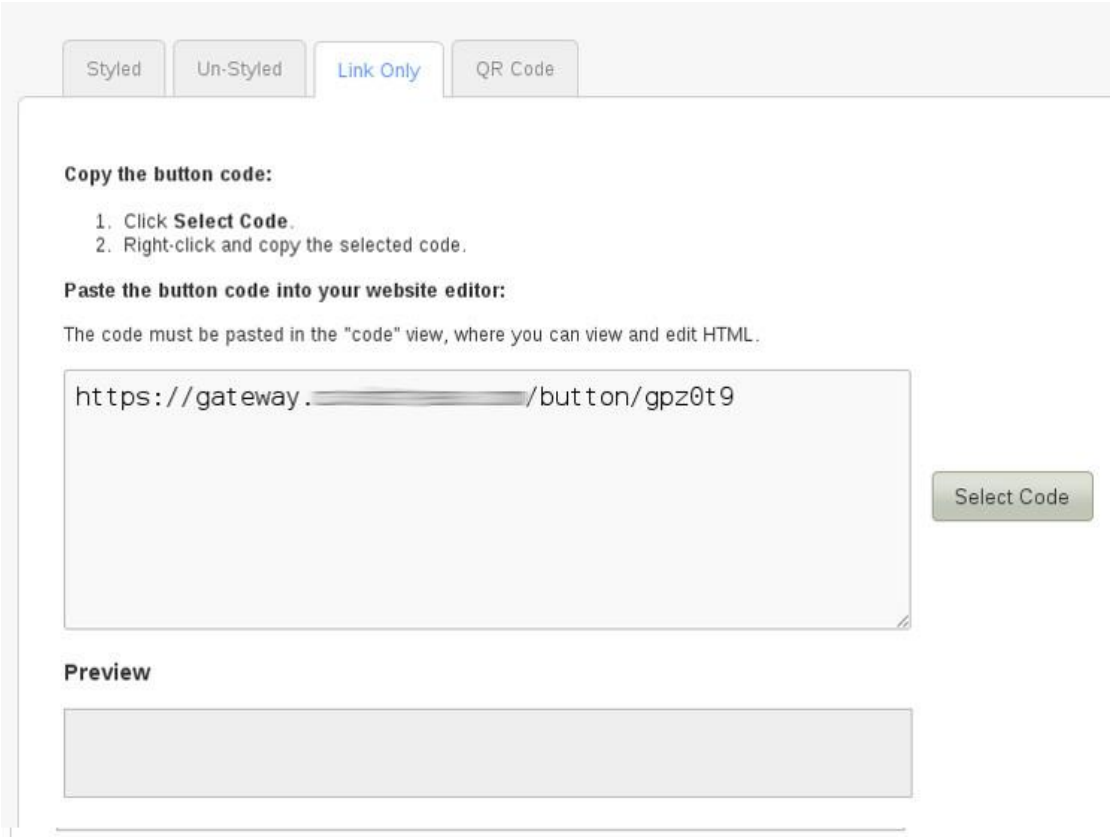
The styled option makes the link look like a pre-formatted button. This is useful for displaying on websites to fit of the style/content of a web-page. It isn't always suitable to send across e-mail clients as the client may not support formatted CSS.

Un-Styled



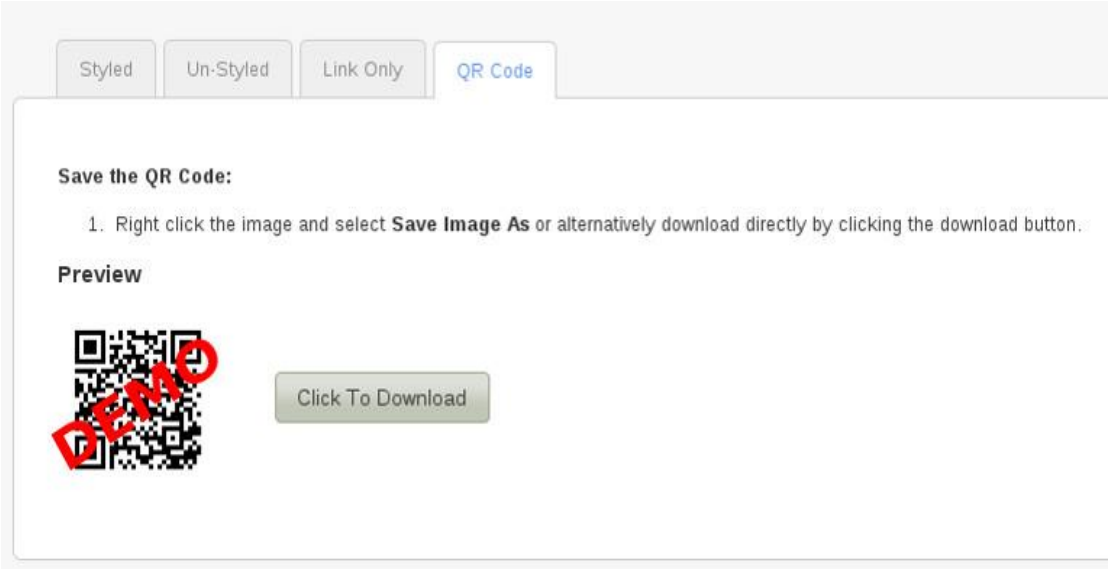
The Un-Styled option creates a standard link that can be styled later using CSS or used as is. This is useful if you want a base to work from to create a button of your choice using CSS.

Link Only



The link only option provides the raw URL without embedding it in an HTML link. If you want a simple link to send to customers, this is the best option.

QR Code



The QR Code option adds the ability for a QR Code to be downloaded. It is automatically generated and is displayed on the page for testing/preview purposes. Click the download button to save it in a file which can then be uploaded or placed wherever you wish. Alternatively, you can right click the preview image and save it from your browser.

A QR Code scanner has to be used to 'read' the code, which will then send the link of the payment form to the device.

3 Advanced Integration

3.1 Advanced Integration

3.1.1 About This Guide

Our Pay Button Advanced 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 take 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.

3.1.2 New Customers Testing

New customers who have not yet received their merchant ID can still perform a test integration. Simply enter **TEST** as your merchant ID and use one of our test cards.

This guide provides the information required to integrate with the Gateway, 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 integration support.

If you do require programming assistance, please contact us on 0845 223 4935 or via email to support@fidelipay.co.uk.

3.1.3 Pre-Requisites

You will need the following information to integrate our Hosted Forms via a Pay Button.

Gateway Merchant ID	Your Merchant user ID enables you to access and communicate with the payment gateway. Please note that these details will differ to the login supplied to access the administration panel. You should have received these details when your account was set up. You may also use test account IDs (if you have been issued with a test ID) and swap these for your live account details when you receive them. **NB: You can also enter "TEST" as the Merchant ID to test the system. This allows prospective customers to test the integration prior to signing up for an account.**
Integration URL	https://gateway.fidelipay.co.uk/button/{YOUR_LINK}

3.1.4 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.

3.1.5 Test Cards

To download the latest copy of the Gateway test cards, for both 3D Secure and non 3D Secure transactions, please contact us for our Integration Guides/Test Cards.

3.2 Gateway Request

To create the button, 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). This is then base64 encoded with all padding characters (=) stripped and the following characters +, / replaced with – and _ respectively. This string is then appended to the gateway URL to give the final link.

Please note that the field names are cAsE sEnSiTiVe.

3.2.1 General Fields

Field Name	Mandatory?	Description
merchantID	Yes	Your Merchant user ID, or "TEST" if you are just testing.
amount	Yes	The amount of the transaction in minor currency. For the UK, this is pence, so £10.99 should be sent as 1099. **Numeric values only – no decimal points or currency symbols.**
action	Yes	The transaction action. Possible values are: **PREAUTH** 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 reserves the funds for, then new, unreserved funds will be taken from the cardholders account. **SALE** This will collect an amount from the customer's card. **VERIFY** This will create a new transaction and attempt to verify that the card account exists with the Acquirer. The transaction will result in no transfer of funds and no hold on any funds on the Cardholder's account. It cannot be captured and will not be settled. The transaction **amount** must always be zero.
type	Yes	The type of transaction. Possible values are: **1** - Cardholder Not Present: Ecommerce. **2** - Cardholder Not Present: Mail Order. **3** - Point of Sale: Card Keyed. **4** - Point of Sale: Card Swiped. **5** - Point of Sale: Card Chip & Pin.
countryCode	Yes	ISO standard country code for the merchant's location.
currencyCode	Yes	ISO standard currency code for this transaction. You may only use currencies that are enabled for your merchant account.

transactionUnique	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.
orderRef	No	This text field allows you to describe the order or provide an invoice number/reference number for the merchant's records.

3.2.2 Redirection and Verification Fields

The Hosted Form, after completion, will redirect the customer to the **redirectURL** or **redirectURLFail**, 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
redirectURL	Yes	The URL to which the customer will be redirected and the transaction result will be POSTed.
redirectURLFail	No	The URL to which the customer will be redirected and the transaction result will be POSTed if the transaction fails. If left blank, the **redirectURL** will be used.
callbackURL	No (Recommended)	A non-public URL which will receive a copy of the transaction result by POST.
notifyEmail	No	An RFC 2822 compliant email address or list to which the merchant will receive a confirmation email on a successful transaction.
customerReceiptsRequired	No	Set this to 'Y' to allow customers to receive email when they enter a valid RFC 2822 email address.

3.2.3 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. Usually the customer will enter this data into the hosted form, however if it is previously known it can be included in the button code to pre-populate the fields. All data is stored and accessible within the administration panel.

Field Name	Mandatory?	Description
customerName	No	The customer or cardholder's name.
customerAddress	Yes, if AVS enabled	The customer or cardholder's address. For AVS checking this must be the registered billing address of the card.
customerPostCode	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.
customerEmail	No	The customer's email address.
customerPhone	No	The customer's telephone number.
customerAddressMandatory	No	If set to 'Y' makes the **customerAddress** & **customerPostCode** fields mandatory on the hosted form.

3.2.4 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†	A short text description of the item.
item1Quantity	Yes†	The quantity of the item purchased.
item1GrossValue	Yes†	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.

†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
taxValue	No	The total amount of tax for this order.
taxDiscountDescription	No	A text field to describe the tax applied *(e.g. "VAT at 20%")*

OR

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

3.2.5 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 the Gateway.

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**.

Data sent in this field can be viewed in the Merchant Management System.

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

3.3 Gateway Response

The 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.

3.3.1 Response Fields

Field Name	Returned?	Description
responseCode	Always	A numeric code providing the outcome of the transaction. Possible values are: **0** - Successful / authorised transaction. **2** - Card referred. **4** - Card declined - keep card **5** - Card declined. Check **responseMessage** for more detail or any error that occurred. For a full list of error codes please refer to the table in Appendix A.
responseMessage	Always	The message received from the acquiring bank, or any error message.
xref	Always	The merchant may store the cross reference for repeat transactions and refunds.
transactionUnique	If supplied	The value supplied in the initial request, if any.

amountReceived	On success	The amount of the transaction. This field used in conjunction with **transactionUnique** can help provide a measure of security.
transactionID	Always	The ID of the transaction on the Gateway system – can be used to easily reconcile transactions in the administration panel.
orderRef	If supplied	The value supplied in the initial request, if any.
avscv2ResponseCode	Optional	The result of the AVS/CV2 check. Please see Appendix 39 for a full list of possible responses.
avscv2ResponseMessage	Optional	The message received from the acquiring bank, or any error message with regards to the AVS/CV2 check. Please see Appendix 39 for a full list of possible responses.
cv2Check	Optional	Textual description of the AVS/CV2 CV2 check as described in Appendix 39. Possible values are: **'not known', 'not checked', 'matched', 'not matched', 'partially matched'**
addressCheck	Optional	Textual description of the AVS/CV2 address check as described in Appendix 39. Possible values are: **'not known', 'not checked', 'matched', 'not matched', 'partially matched'**

postcodeCheck	Optional	Textual description of the AVS/CV2 postcode check as described in Appendix 39. Possible values are: **'not known', 'not checked', 'matched', 'not matched', 'partially matched'**
avscv2AuthEntity	Optional	Textual description of the AVS/CV2 authorizing entity. Possible values are: **'not known', 'merchant host', 'acquirer host', 'card scheme', 'issuer'**
cardNumberMask	Always	Card number masked so only the last 4 digits are visible - for example: **********1234
cardTypeCode	Always	The code of card used. See appendix 36 for a full list.
cardType	Always	The description of the card used. See Appendix 36 for a full list.

3.3.2 3D Secure Fields

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

Field Name	Returned?	Description
threeDSEnabled	Yes	The 3D Secure status of the merchant account. Possible values are: **N** – the merchant is not 3DS enabled **Y** – the merchant is 3DS enabled

threeDSEnrolled	Yes	The 3D Secure enrolment status for the credit card. Possible values are: **Y** - Enrolled. **N** - Not Enrolled. **U** - Unable To Verify **E** - Error Verifying Enrolment. Refer to Appendix 39 for further information.
threeDSAuthenticated	No	The 3D Secure authentication status for the credit card. Possible values are: **Y** - Authentication Successful. **N** - Not Authenticated. **U** - Unable To Authenticate. **A** - Attempted Authentication. **E** - Error Checking Authentication. Refer to Appendix 39 for further information.
threeDSPaReq	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.
threeDSPaRes	No	Payer Authentication Response (PaRes) that is returned from the Access Control Server (ACS) determining the 3D Secure status of the credit card.
threeDSACSURL	No	The URL of the Access Control Server (ACS) to which the Payer

		Authentication Request (PaReq) should be sent.
threeDSECI	No	This contains a two digit Electronic Commerce Indicator (ECI) value, which is to be submitted in a credit card authorization message. This value indicates to the processor that the customer data in the authorization message has been authenticated. The data contained within this property is only valid if the **threeDSAuthenticated** value is **Y** or **A**.
threeDSCAVV	No	This contains a 28-byte Base-64 encoded Cardholder Authentication Verification Value (CAVV). The data contained within this property is only valid if the **threeDSAuthenticated** value is **Y** or **A**.
threeDSCAVVAlgorithm	No	This contains the one digit value which indicates the algorithm used by the Access Control Server (ACS) to generate the CAVV. Valid algorithms include (amongst others): **0** - HMAC **1** - CVV **2** - CVV with ATN The data contained within this property is only valid if the

		threeDSAuthenticated value is **Y** or **A**.
threeDSXID	No	A unique identifier for the transaction as used in the 3D Secure process. This is normally a 20 character string.
threeDSErrorCode	No	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.
threeDSErrorDescription	No	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.
threeDSMerchantPref	No	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.
threeDSVETimestamp	No	The time the card was checked for 3D Secure enrolment.
threeDSCATimestamp	No	The time the card was checked for 3D Secure authentication.

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**
0	Successful / authorised transaction. Any code other than **0** indicates an unsuccessful transaction
2	Card referred
4	Card declined – keep card
5	Card declined
30	An error occurred. Check **responseMessage** for more detail

General Error Codes: 65536 - 65791	
Code	**Description**
65536	Transaction in progress. Refer to Support if this error occurs
64437	Reserved for future use. Refer to Support if this error occurs
65538	Reserved for future use. Refer to Support if this error occurs
65539	Invalid Credentials: **merchantID** is unknown

65540	Permission denied: caused by sending a request from an unauthorized IP address
65541	Reserved for future use. Refer to Support if this error occurs
65542	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
65543	Request Ambiguous: request could be misinterpreted due to inclusion of mutually exclusive fields
65544	Request Malformed: couldn't parse the request data
65545	Suspended Merchant account
65546	Currency not supported by Merchant
65547	Request Ambiguous, both **taxValue** and **discountValue** provided when should be one only
65548	Database error
65549	Payment processor communications error
65550	Payment processor error
65551	Internal communications error
65552	Internal error

3D Secure Error Codes: 65792 - 66047	
Code	**Description**
65792	3D Secure transaction in progress. Refer to Support if this error occurs
65793	Unknown 3D Secure Error
65794	3D Secure processing is unavailable. Merchant account doesn't support 3D Secure
65795	3D Secure processing is not required for the given card
65796	3D Secure processing is required for the given card
65797	Error occurred during 3D Secure enrolment check
65798	Reserved for future use. Refer to Support if this error occurs
65799	Reserved for future use. Refer to Support if this error occurs
65800	Error occurred during 3D Secure authentication check
65801	Reserved for future use. Refer to Support if this error occurs
65802	3D Secure authentication is required for this card
65803	3D Secure enrolment or authentication failure and Merchant 3DS preferences are to STOP processing

Missing Request Field Error Codes: 66048 - 66303	
Code	**Description**
66048	Missing request. No data posted to integration URL

66049	Missing **merchantID** field
66050	Reserved for future use. Refer to Support if this error occurs.
66051	Reserved for internal use. Refer to Support if this error occurs
66052	Reserved for internal use. Refer to Support if this error occurs
66053	Reserved for internal use. Refer to Support if this error occurs
66054	Reserved for internal use. Refer to Support if this error occurs
66055	Missing **action** field
66056	Missing **amount** field
66057	Missing **currencyCode** field
66058	Missing **cardNumber** field
66059	Missing **cardExpiryMonth** field
66060	Missing **cardExpiryYear** field
66061	Missing **cardStartMonth** field (reserved for future use)
66062	Missing **cardStartYear** field (reserved for future use)
66063	Missing **cardIssueNumber** field (reserved for future use)
66064	Missing **cardCVV** field
66065	Missing **customerName** field
66066	Missing **customerAddress** field
66067	Missing **customerPostCode** field
66068	Missing **customerEmail** field

66069	Missing **customerPhone** field (reserved for future use)
66070	Missing **countyCode** field
66071	Missing **transactionUnique** field (reserved for future use)
66072	Missing **orderRef** field (reserved for future use)
66073	Missing **remoteAddress** field (reserved for future use)
66074	Missing **redirectURL** field
66075	Missing **callbackURL** field (reserved for future use)
66076	Missing **merchantData** field (reserved for future use)
66077	Missing **origin** field (reserved for future use)
66078	Missing **duplicateDelay** field (reserved for future use)
66079	Missing **itemQuantity** field (reserved for future use)
66080	Missing **itemDescription** field (reserved for future use)
66081	Missing **itemGrossValue** field (reserved for future use)
66082	Missing **taxValue** field (reserved for future use)
66083	Missing **discountValue** field (reserved for future use)
66084	Missing **taxDiscountDescription** field (reserved for future use)
66085	Missing **xref** field (reserved for future use)
66086	Missing **type** field (reserved for future use)
66087	Reserved for future use

66088	Reserved for future use
66089	Missing **transactionID** field (reserved for future use)
66090	Missing **threeDSRequired** field (reserved for future use)
66091	Missing **threeDSMD** field (reserved for future use)
66092	Missing **threeDSPaRes** field
66093	Missing **threeDSECI** field
66094	Missing **threeDSCAVV** field
66095	Missing **threeDSXID** field

Invalid Request Field Error Codes: 66304 - 66559	
Code	**Description**
66304	Invalid request
66305	Invalid **merchantID** field
66306	Reserved for future use. Refer to Support if this error occurs
66307	Reserved for internal use. Refer to Support if this error occurs
66308	Reserved for internal use. Refer to Support if this error occurs
66309	Reserved for internal use. Refer to Support if this error occurs
66310	Reserved for internal use. Refer to Support if this error occurs
66311	Invalid **action** field
66312	Invalid **amount** field

66313	Invalid **currencyCode** field
66314	Invalid **cardNumber** field
66315	Invalid **cardExpiryMonth** field
66316	Invalid **cardExpiryYear** field
66317	Invalid **cardStartMonth** field
66318	Invalid **cardStartYear** field
66319	Invalid **cardIssueNumber** field
66320	Invalid **cardCVV** field
66321	Invalid **customerName** field
66322	Invalid **customerAddress** field
66323	Invalid **customerPostCode** field
66324	Invalid **customerEmail** field
66325	Invalid **customerPhone** field
66326	Invalid **countyCode** field
66327	Invalid **transactionUnique** field (reserved for future use)
66328	Invalid **orderRef** field (reserved for future use)
66329	Invalid **remoteAddress** field
66330	Invalid **redirectURL** field
66331	Invalid **callbackURL** field (reserved for future use)
66332	Invalid **merchantData** field (reserved for future use)
66333	Invalid **origin** field (reserved for future use)
66334	Invalid **duplicateDelay** field (reserved for future use)
66335	Invalid **itemQuantity** field

66336	Invalid **itemDescription** field
66337	Invalid **itemGrossValue** field
66338	Invalid **taxValue** field
66339	Invalid **discountValue** field
66340	Invalid **taxDiscountDescription** field (reserved for future use)
66341	Invalid **xref** field
66342	Invalid **type** field
66343	Reserved for future use
66344	Reserved for future use
66345	Invalid **transactionID** field
66356	Invalid **threeDSRequired** field
66347	Invalid **threeDSMD** field
66348	Invalid **threeDSPaRes** field
66349	Invalid **threeDSECI** field
66350	Invalid **threeDSCAVV** field
66351	Invalid **threeDSXID** field
66416	Invalid card expiry date. Must be a date sometime in the next 10 years
66417	Invalid card start date. Must be a date sometime in the last 10 years
66418	Invalid item count. Tried to supply more than 6 line item details
66419	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
ALL MATCH	AVS and CV2 match.
SECURITY CODE MATCH ONLY	CV2 match only.
ADDRESS MATCH ONLY	AVS match only.
NO DATA MATCHES	No matches for AVS and CV2.
DATA NOT CHECKED	Supplied data not checked.
SECURITY CHECKS NOT SUPPORTED	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
0	No additional information available.
1	CV2 not checked.
2	CV2 matched.
4	CV2 not matched.
8	Reservered.

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 3DSecure program and the payer is eligible for authentication processing.

N - Not Enrolled: The checked card is eligible for the 3DSecure (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 Gateway 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 **threeDSAuthenticated** 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 Gateway 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 generate a button URL and format it as an HTML link:

```
<?php

     function createSignature(array $data, $key, $algo =
null) {

          if ($algo === null) {
               $algo = 'SHA512';
          }

          ksort($data);

          // Create the URL encoded signature string
          $ret = http_build_query($data, '', '&');

          // Normalise all line endings (CRNL|NLCR|NL|CR)
to just NL (%0A)
          $ret = preg_replace('/%0D%0A|%0A%0D|%0A|%0D/i',
'%0A', $ret);

          // Hash the signature string and the key
together
          $ret = hash($algo, $ret . $key);

          // Prefix the algorithm if not the default
          if ($algo !== 'SHA512') {
               $ret = '{' . $algo . '}' . $ret;
          }

          return $ret;
     }

     $gateway_url =
'https://gateway.fidelipay.co.uk/button/';
     $signature_key = 'Custom29Simple14Marker';

     $fields = array(
          'merchantID'         => 101093,
          'amount'       => 101,
          'action'       => 'SALE',
          'type'               => 1,
          'countryCode'  => 826,
          'currencyCode'       => 826,
          'transactionUnique' => uniqid(),
          'orderRef'           => 'Button Test',
```

```
          'redirectURL'        => ($_SERVER['HTTPS'] ==
'on' ? 'https' : 'http') . '://' .
$_SERVER['HTTP_HOST'] . $_SERVER['REQUEST_URI'],
          'merchantData'       => 'CS-PayByLink',
     );

     $fields['signature'] = createSignature($fields,
$signature_key);

     //Convert array to Query String
     $link = http_build_query($fields);

     //Optionally compress the string to make the link
smaller
     $link = gzdeflate($link, 9);

     //Base64 encode the string and remove any padding or
invalid
     //URL characters including =,+,/
     $link = strtr(trim(base64_encode($link), '='), '+/',
'-_');

     $link = $gateway_url . $link;

     echo "<p><a href='{$link}'>Pay Now</a></p>";
```

When the user clicks the 'Pay Now' button they will be taken to the Gateway integration page via the button URL that has been created. Here, 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 button creation process, then the values sent will be used to populate the initial values of the controls on the hosted form. When the customer submits this hosted form, the transaction will be attempted and the results will be sent as a HTTP POST request to the specified **redirectURL.** An example 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 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 endings 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 you are 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 (ordered from most secure to least secure): 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.