



Payment Page Integration Guide

Version 2.4 – July 2019

Table of contents

About this Guide	Error! Bookmark not defined.
Introduction	Error! Bookmark not defined.
Benefits of the Hosted Payment Page:.....	4
Submitting a Payment Request	5
Payment Request parameters.....	5
Example of a Payment Request	6
Securing your payment request submission	6
Optional cardholder and delivery parameters	7
Example of a Payment Request with optional parameters	7
Payment Callback Response	9
Configuring your account to receive a Callback Response	9
Example code used for payment Callback Response	11
Shopper Return URLs	12
Configuring the shopper Return URLs	12
URL Override	13
Payment Callback Response & Return URL parameters.....	13
CVV/AVS check values	14
Payment Page customisation	15
Basic customisation.....	15
Advanced customisation	16
Payment Page container files.....	16
Style sheets, images and hyperlinks	18
The payment page's styles	19
Going Mobile	19
Uploading files to your customisation directory	20
Reviewing your customisations	20
Testing your Integration & Going Live	21
Appendix A: Payment System Response Codes	22
Appendix B: Payment Page Screen shots	24
Appendix C: Card types returned in callack response	24



About this guide

Welcome to the CashFlows Payment Page Integration Guide. This document is designed to provide you comprehensive details on how to integrate your business' website to the CashFlows Payment Gateway. This document assumes a working knowledge of HTML, online forms, and HTTP(S); however, due to the simplicity of this integration method you will not need in-depth knowledge of these concepts to integrate with us and accept card payments through CashFlows.

In addition to this guide we have a team of specialists providing technical support during your integration with CashFlows. To receive support, please visit our website - <http://support.cashflows.com>

The latest version of this guide is always available from:
<https://www.cashflows.com/user-and-integration-guides>

Copyright

2019 © Cashflows Europe limited

While every effort has been made to ensure the accuracy of the information contained in this publication, the information is supplied without representation or warranty of any kind, is subject to change without notice and does not represent a commitment on the part of CashFlows Europe limited. CashFlows Europe limited, therefore, assumes no responsibility and shall have no liability, consequential or otherwise, of any kind arising from this material or any part thereof, or any supplementary materials subsequently issued by CashFlows Europe limited. CashFlows Europe limited has made every effort to ensure the accuracy of this material.



Introduction

The Hosted Payment Page integration method provides web developers a quick integration to the online Payment Gateway and full Payment Page functionality for processing online card payments.

To process an online payment using the Payment Page, your website store will need to send a HTML payment request to our online payment servers to initiate the transaction. We then display a compliant payment page to the shopper where they securely enter their card details. We immediately process the payment when the details are submitted to us. The shopper will then be returned to your website store with confirmation that the payment has been processed.

The Hosted Payment Page can also be fully customised to match the look and feel of your website.

Benefits of the Hosted Payment Page:

No cost for an SSL certificate: Payment Card Industry Data Security Standards (PCI DSS) requires that web pages accepting credit card information must have SSLv3 128-bit minimum certificates. The Hosted Payment Page has a 128-bit to 256-bit certificate with full "green bar" functionality for extra customer confidence.

Reduced PCI DSS considerations: PCI DSS also states that any site accepting card information must NEVER store the CVV, and if it does store the card number, it must be 256-bit AES encrypted. Most web servers log traffic to and from them which may include card numbers. These logs would have to be audited on a continual basis to ensure that card numbers are not being stored.

For further information about PCI DSS and your security requirements, please visit

<http://support.cashflows.com/pcidss/>

Ease of integration: As opposed to other integration methods, the Hosted Payment Page integration is our simplest method. You just have to submit a web form to us and then display the response that our host sends back.



Submitting a payment request

When your customer is ready to pay for their goods or services, your website store will need to send an HTML payment request to our online payment servers to initiate the transaction.

The payment request is sent as an HTML form **POST** containing a description of the goods or services being purchased and the total cost and your CashFlows Profile ID. The payment request must be UTF-8 encoded and submitted to:

<https://secure-int.cashflows.com/gateway/standard> for the Integration environment.

<https://secure.cashflows.com/gateway/standard> for the Production environment.

Please contact techsupport@cashflows.com if you require an integration account.

If the purchase consists of more than one item, your shopping cart system must total all the items into a single description, total the cost and submit a single combined payment request.

Payment Request parameters

The following table lists the minimum parameters that must be sent in the payment request in order for us to successfully process the payment.

Note: All payment request parameters are mandatory unless specified.

Parameter	Description
store_id	Your CashFlows Profile ID
cart_id	Your reference for the transaction (max of 255 characters).
amount	Transaction amount to 2 decimal places, e.g. 24.99. (The currency symbol must not be included.)
currency	Transaction currency, 3 character (uppercase) ISO code.
description	Your description of the item(s) being purchased. This will be displayed to the customer on the payment pages (max of 99 characters).
test	0 (Please contact techsupport@cashflows.com if you require an integration account)
check	A security Hash value used to ensure that no-one has tampered with the payment request. For further details, please refer to Securing your payment request submission (Optional depending on configuration)
Additional fields for merchants with the MCC 6012 (Financial Institutions)	
primary_recipient_dob	Customer's Date of Birth. Format is YYYYMMDD (8 numeric characters)
primary_recipient_surname	Customer's Surname or Last name (2-64 characters alpha characters, including -)
primary_recipient_postcode	Customer's Postcode (2 to 16 characters alpha characters, including spaces)
primary_recipient_account_number	Customer's Account Number (1 to 32 alpha numeric characters, including /-) For PAN Numbers: First 6 and Last 4

When the payment request is received by CashFlows, it is checked to ensure that all the required data is present, and that the security check is valid. Once the initial validation has been passed, a secure payment page will be displayed to the shopper confirming the details of the purchase and requesting the shopper's credit or debit card details and cardholder information.

The card details and cardholder information the shopper supplies is processed, and the result (authorised or declined) is displayed back to them. If the transaction is not authorised, the shopper is given the option of trying another card or to cancel the transaction.

When the transaction has been processed, or if the shopper cancels the transaction, we will display a result page enabling the shopper to return to your store. The shopper can automatically be redirected to your store or they can select the “Continue Shopping” button. The URL that your shopper returns to your store can be configured to your requirements; please refer to Shopper Return URLs

Example of a Payment Request

Example of a HTML from that will POST the payment request parameters to the CashFlows payment gateway for authorisation.

```
<form action="https://secure.cashflows.com/gateway/standard" method="post">
<input type="hidden" name="store_id" value="1" />
<input type="hidden" name="cart_id" value="Cart001" />
<input type="hidden" name="amount" value="13.99" />
<input type="hidden" name="currency" value="GBP" />
<input type="hidden" name="test" value="0" />
<input type="hidden" name="description" value="CD Collection" />
<input type="hidden" name="check"
value="a661070510ef18f8ca3d79363705247500d74d31dc5f5518e7cfdbecf1b02372" />
<input type="submit" value="Buy now" />
</form>
```

Securing your payment request submission

To protect the payment request from being tampered with whilst being transferred to the payment gateway, the payment request can include a cryptographic hash [digital signature](#).

The [digital signature](#) or ‘message digest’ can be generated by our administration system or by your own server side scripting to create unique values for each of your payment requests.

The ‘message digest’ must be generated using one of 3 algorithms methods MD5, SHA1 or SHA256 and contain the following values:

```
secret_key:store_id:cart_id:amount:currency:test:description
```

Each section of data is separated using a ‘:’ (colon) character, and the data must be organised in the exact sequence shown.

If you are a Financial Institution and have an MCC of 6012 the ‘message digest’ MUST also include values of the additional fields:

```
secret_key:store_id:cart_id:amount:currency:test:description:primary_recipient_dob:primary_recipient_account_
umber:primary_recipient_postcode:primary_recipient_surname
```

Note: We recommend that when generating the ‘message digest’ that you use the SHA256 algorithm as it is the most secure. We would also strongly advise against the use of no hashing.

The ‘message digest’ can then be included into your payment request using the *check* parameter.

The CashFlows Payment Gateway compares the ‘message digest’ against its own ‘message digest’ created from your order information supplied. As only you and the CashFlows Payment Gateway know the *secret_key* element of the ‘message digest’, the transaction will only be processed if the two ‘message digest’ match.

To generate a ‘message digest’ for each of your payment requests you can use the hash generator function within your CashFlows Account’s Management System. For further information about configuring your account to

use the payment page integration model, please refer to your [administration guide](#).

Warning: At no time should the actual pre-set secret key be included in any FORM or web page that is held on your server.

Optional cardholder and delivery parameters

In addition to the standard payment requests parameters above, you may wish to send optional information such as the shoppers' name, address, email address or phone number to the payment page. By including the optional cardholder and delivery details in your payment request it will help to reduce dropout rates on the payment page, as much of the information will be prefilled.

Note: The shoppers will have the ability to edit the cardholder information before proceeding with the transaction.

Parameters	Use
name	Shopper's billing name
address	Shopper's billing address, not including the postcode or country. (Multiple lines should be separated using a comma. The HTML tag will also be treated as a newline.)
postcode	Shopper's billing post/area/zip code
country	Shopper's billing country. (This must be sent as a 2 character ISO3166 country code.)
tel	Shopper's billing telephone number
email	Shopper's email address
delv_name	Shopper's delivery name
delv_address	Shopper's delivery address, not including the postcode or country. (Multiple lines should be separated using a comma. The HTML tag will also be treated as a newline.)
delv_postcode	Shopper's delivery post/area/zip code
delv_country	Shopper's delivery country. (This must be sent as a 2 character ISO3166 country code.)
delv_tel	Shopper's delivery telephone number

Note: If you're passing the delivery details in the payment request (i.e. 'delv_' parameters), we strongly recommend that you retain this information on your own server as the delivery values are not stored within the transaction record held by CashFlows.

Example of a Payment Request with optional parameters

```
<form action="https://secure.cashflows.com/gateway/standard" method="post">
<input type="hidden" name="store_id" value="1" />
<input type="hidden" name="cart_id" value="Cart001" />
<input type="hidden" name="amount" value="13.99" />
<input type="hidden" name="currency" value="GBP" />
<input type="hidden" name="test" value="0" />
<input type="hidden" name="description" value="CD Collection" />
<input type="hidden" name="name" value="Joe Bloggs" />
<input type="hidden" name="address" value="CPC1 Capital Park, Cambridge" />
<input type="hidden" name="postcode" value="CB22 5LD" />
<input type="hidden" name="country" value="GB" />
<input type="hidden" name="tel" value="+44 (0)1223 550920" />
```

```
<input type="hidden" name="email" value="joe.bloggs@cashflows.com" />
<input type="hidden" name="delv_name" value=" Joe Bloggs" />
<input type="hidden" name="delv_address" value=" CPC1 Capital Park, Cambridge" />
<input type="hidden" name="delv_postcode" value="CB22 5LD" />
<input type="hidden" name="delv_country" value="GB" />
<input type="hidden" name="delv_tel" value="+44 (0)1223 550920" />
<input type="hidden" name="check"
value="a661070510ef18f8ca3d79363705247500d74d31dc5f5518e7cfdbecf1b02372" />
<input type="submit" value="Buy now" />
</form>
```




Payment callback response

To inform your site when a transaction has been Authorised, Declined or Cancelled you will need to create and configure a payment Callback Response.

A payment Callback Response can be used to update your transaction record, send emails to different departments or create a dispatch request in your ordering system/shopping cart. The payment Callback Response however, is not used to display any additional information to the shopper, for this you will need to use the [Shopper Return URLs](#).

Configuring your account to receive a Callback Response

To configure your Callback Response URL's, login to the Account Management System and select 'Integration Settings' from the 'Gateway Administration' Menu.

The screenshot shows the 'Integration Settings' page in the Cashflows Account Management System. The page is divided into a sidebar menu and a main content area. The sidebar menu includes sections for Business Accounts, Merchant Accounts, Profile details, Gateway transactions, Virtual Terminal, and Gateway administration. The 'Gateway administration' section is expanded, showing sub-sections like Integration settings, URL Override, Generate a Hash Code, Payment page customisation, Customisation file upload, and Country restrictions. The main content area is titled 'Integration Settings' and contains three main sections: 'Request Token', 'Callback URLs', and 'Shopper Return URLs'. The 'Request Token' section includes a 'Hash type' dropdown menu set to 'None', a 'Secret Key' input field, a 'Referrer' input field, a 'Enduser' dropdown menu set to 'None', and a 'Lifetime' dropdown menu set to '15'. The 'Callback URLs' section includes input fields for 'Authorised', 'Failed', 'Cancelled', 'Password', and 'Email'. The 'Shopper Return URLs' section includes input fields for 'Authorised' and 'Cancelled', a dropdown menu for 'Automatic Redirect' set to 'Disabled', and a dropdown menu for 'HTTP Method' set to 'GET'. An 'Update' button is located at the bottom of the 'Shopper Return URLs' section. The page also features a top navigation bar with links for Home, Password change, Contact us, Support knowledgebase, and Guide, and a 'Sign Out' button.

Figure: Integration settings page in your Account Management System

Here you will be able set up your payment Callback Response URLs to inform your system of the result of a payment made through the hosted payment page.

Authorised - Enter the full URL that you wish the Callback Response to be sent to when a payment request has been authorised.

Failed - Enter the full URL that you wish the Callback Response to be sent to when a payment request has failed.

Note: The shopper may try again therefore this is not an indication that the purchase will not be completed.

Cancelled - Enter the full URL that you wish the Callback Response to be sent to when a payment request has been cancelled.

Password - To provide additional reassurance that the Callback Response has been sent by us you may wish to enter a Callback Response password into the field provided. The Callback Response password we will be returned to you in the Callback Response, providing you with a basic security check.

Email – Enter an email address which will receive an email notification in the event of a callback failure.

Dear Customer

You are receiving this email as an error occurred whilst processing a transaction via our hosted payment page. We have been unable to successfully deliver the transaction result via callback to your system.

Transaction Details:

*Auth Message: Authorised
Trans Reference: 01S00000165
Card Holder Name: Mr Tester
Cart ID: 1
Amount: 10.00*

We recommend that you log into the CashFlows Account Management System and verify the transaction result against our records.

We recommend that you pass this information onto your web-developer/website Administrator to correct the cause of the error.

Reason for Callback Failure: Could not connect to Host

Note: We classify any HTTP STATUS response codes that are not 200 as a callback failure.

We recommend that you pass this information onto your web-developer/website Administrator to correct the cause of the error.

*For further information about Callbacks and the Hosted Payment Page, please refer to
https://support.cashflows.com/kb/payment_page_integration_guide.pdf*

Your sincerely,

*Technical support
CashFlows
<http://www.cashflows.com>*

Figure: Callback Failure Email Example

When you have configured the Callback Response URL's, the CashFlows payment gateway will directly contact your website and pass details of the transaction including the cart_id and amount. For a full list of parameters sent in the Callback Response, please refer to [Callback Response & Return parameters](#).

Example code used for payment Callback Response

This example shows how to create a Callback Response using PHP to read the parameters returned in the payment response and to send an email to different email addresses within your business.

```
<?php
$billName = $_POST['bill_name'];
$billAddress = $_POST['bill_address'];
$billPostcode = $_POST['bill_postcode'];
$billCountry = $_POST['bill_country'];
$billEmail = $_POST['bill_email'];
$billTel = $_POST['bill_tel'];
$cartCost = $_POST['cart_cost'];
$cartCurrency = $_POST['cart_currency'];
$cartId = $_POST['cart_id'];
$cartDesc = $_POST['cart_desc'];
$tranRef = $_POST['tran_ref'];
$tranTestmode = $_POST['tran_testmode'];
$authStatus = $_POST['auth_status'];
$authCode = $_POST['auth_code'];
$authMessage = $_POST['auth_message'];
$authAVS = $_POST['auth_avs'];

if ( $authStatus == "A" ) {
$recipient = "sales.team@my-domain.com";
} elseif ( $authStatus == "C" ) {
$recipient = "cancelled_orders@my-domain.com";
} else {
$recipient = "failed_orders@my-domain.com";

    $subject = "$tranStatus"." Website Order Received ".$tranRef." ".$billName;

    $message = "Order Details\n\r";
    $message .= "".$cartDesc. "\n\r";
    $message .= "".$cartCurrency. " ".$cartCost. "\n\r";
    $message = "Customer Details\n\r";
    $message .= "".$billName. "\n\r";
    $message .= "".$billAddress. "\n\r";
    $message .= "".$billPostcode. "\n\r";
    $message .= "".$billCountry. "\n\r";
    $message .= "".$billEmail. "\n\r";
    $message .= "".$billTel. "\n\r";
    $message = "Transaction Details\n\r";
    $message .= "tran_ref : ".$tranRef. "\n\r";
    $message .= "tran_testmode : ".$tranTestmode. "\n\r";
    $message .= "auth_avs : ".$authAVS. "\n\r";
    $message .= "auth_status : ".$authStatus. "\n\r";
    $message .= "auth_message : ".$authMessage. "\n\r";

    $headers = "From: sales@my-domain.com\n\r";
    $headers .= "Content-Type: text/plain; charset=iso-8859-1\n\r";
    $headers .= "Reply-To: $email\n\r";
```

```
$headers .= "X-Priority: 1\n";
mail($recipient, $subject, $message, $headers);
```

```
?>
```

Shopper Return URLs

When the transaction has been processed, or if the shopper cancels the transaction, the shopper's browser will be presented with a page showing them the results of the transaction, including the auth code if relevant. The result page enables the shopper to return to your store by selecting the "Continue Shopping" button or by automatic redirection.

Configuring the shopper Return URLs

To configure the shopper Return URLs, login to the Account Management System and select 'Integration Settings' from the 'Gateway Administration' Menu.

Here you will be able to set up the Return URLs which enables the shopper to return to your website.

Authorised - Enter the full Return URL including any parameters that you wish to include on your payment successful result page.

Cancelled - Enter the full Return URL including any parameters that you wish to include on your payment cancelled result page.

Within the configured Return URL's, it is possible to include details of the transaction by including parameters after the URL.

Note: This is not a secure method of sending transaction information as it is relayed via the shopper's browser and could be tampered with.

To include transaction information into the Return URL, add any of the following payment response parameters to the URL using the `@[parameter]@` format, for example:

```
https://yoursite.com/thank_you.php?cart=@@cart_id@@&ref=@@tran_ref@@
```

It is also possible for the transaction information to be sent to your web server via a HTTP POST method instead of using the GET URL string. To enable the POST method, include the payment response parameters to the URL and select POST from the HTTP methods dropdown.

We recommend that you only use the Return URLs to display additional order confirmation details to the shopper and that you use a tamperproof Callback Response for updating your order/store details.

Warning: We strongly advise that both your Return URL and Callback Response use a secure `https` connection wherever possible.

You can automatically redirect a shopper to a Return URL which provides you greater control of what your shopper will see as a result page and what transaction information you wish to display. We would therefore recommend that you automatically redirect shopper to the Return URLs to provide a better customer experience.

To enable the automatic redirection, simply select **Enabled** from the Automatic Redirect dropdown.

URL Override

You can override your profiles default Return URL and Callback Responses settings by sending URL Override values with the payment request. This enables you to set both the Return URL and Callback Responses per transaction, provide you with full control over the payment processing. You can create your URL Overrides by logging into the Account Management System and selecting 'URL Override' from the 'Gateway Administration' Menu. For further information, please refer to your [Account Management System guide](#).

Payment Callback Response & Return URL parameters

The following table lists the parameters that can be sent back to you in the payment Callback Response.

Note: Not all parameters can be included in the Return URL's, including the billing address and callback password.

Parameters	Description
store_id	Your CashFlows Profile ID
cart_id	A reference from your store for this transaction
cart_desc	The description of the item(s) purchased
cart_cost	The cost of the items purchased
cart_currency	The currency code of the transaction, 3 character code.
tran_ref	CashFlows unique transaction reference
tran_testmode	0 (Live)
auth_status	The authorisation result of the transaction. A = Authorised, C=Cancelled, any other status value indicates a failure.
auth_message	Message describing the authorisation result
auth_code	Authorisation code from the acquiring bank, only sent if auth_status = 'A'
auth_avs	Result of the AVS comparison check, see CVV/AVS check values below. (Callback only)
auth_cvv	Result of the CVV comparison check, see CVV/AVS check values below. (Callback only)
check	A generated 'message digest' using your chosen hash type and secret_key. The format of the 'message digest' contains the following parameter values: secret_key:cart_id:cart_desc:cart_cost:cart_currency:tran_ref:auth_status
bill_name	Shopper's name (Callback only)
bill_address	Shopper's address(Callback only)
bill_postcode	Shopper's post/zip/area code (if supplied) (Callback only)
bill_country	Shopper's country(Callback only)
bill_email	Shopper's email address(Callback only)
bill_tel	Shopper's telephone number (if supplied) (Callback only)
Password	Optional Callback password as configured in the Account Management System, see Configuring our account to receive callbacks above. (Callback only)
error_code	Response code indicating why the transaction failed, see Appendix A.

card_pan	Shoppers obfuscated card number in format 4444*****0011 (callback only)
Card_type	Shoppers card type, see Appendix C. (callback only)
Additional parameters for authorised 3d Secure Transactions (Callback only)	
acs_eci	The response from the Access Control Server, stating the 3DS method and result: VbyV - Full Authentication = 5, VbyV - Attempted Authentication = 6, VbyV - No Authentication = 7, MasterCard SecureCode - Full Authentication = 2 MasterCard SecureCode - Attempted Authentication = 1 MasterCard SecureCode - No Authentication = 0
acs_cavv	The Cardholder Authentication Verification Value from the Access Control Server, 28 characters.
acs_xid	The unique Authentication Id for transaction from the Access Control Server, 28 characters.
acs_check	A generated 'message digest' using your chosen hash type and secret_key. The format of the 'message digest' contains the following parameter values: secret_key:acs_eci:acs_cavv:acs_acs_xid

CVV/AVS check values

The CVV/AVS result is a 3 digit value, each digit representing a different check. The first value is the CVV check, the second is the address and the third is the postcode.

Value	Meaning
0	Not Checked
1	Check was not available
2	Full match
3	Partial match
4	Not matched
5	Error

The possible values for each digit are as follows:
A partial match is only possible for the address or postcode data, not for CVV check.
Not all acquirers or issuers support all of these checks, in which case the results will be either 0 or 1.

Example Response	CVV	Address	Postcode
232	Full match	Partial match	Full match
400	Not matched	Not checked	Not checked



Payment page customisation

To help you customise your payment page so that it looks like the rest of your website, you can use the basic customisation tools provided by the Account Management System, or with some experience in HTML and CSS you can fully customised your payment page using payment page container files.

Basic customisation

To change the colour scheme of the payment page using our basic customisation facility, login to the Account Management System and select 'Payment Page Customisation' from the 'Gateway Administration' menu. Here you will be able to change the colour scheme of a wide range of elements that are displayed on the payment page and specify a secure (https://) URL for the top banner image.

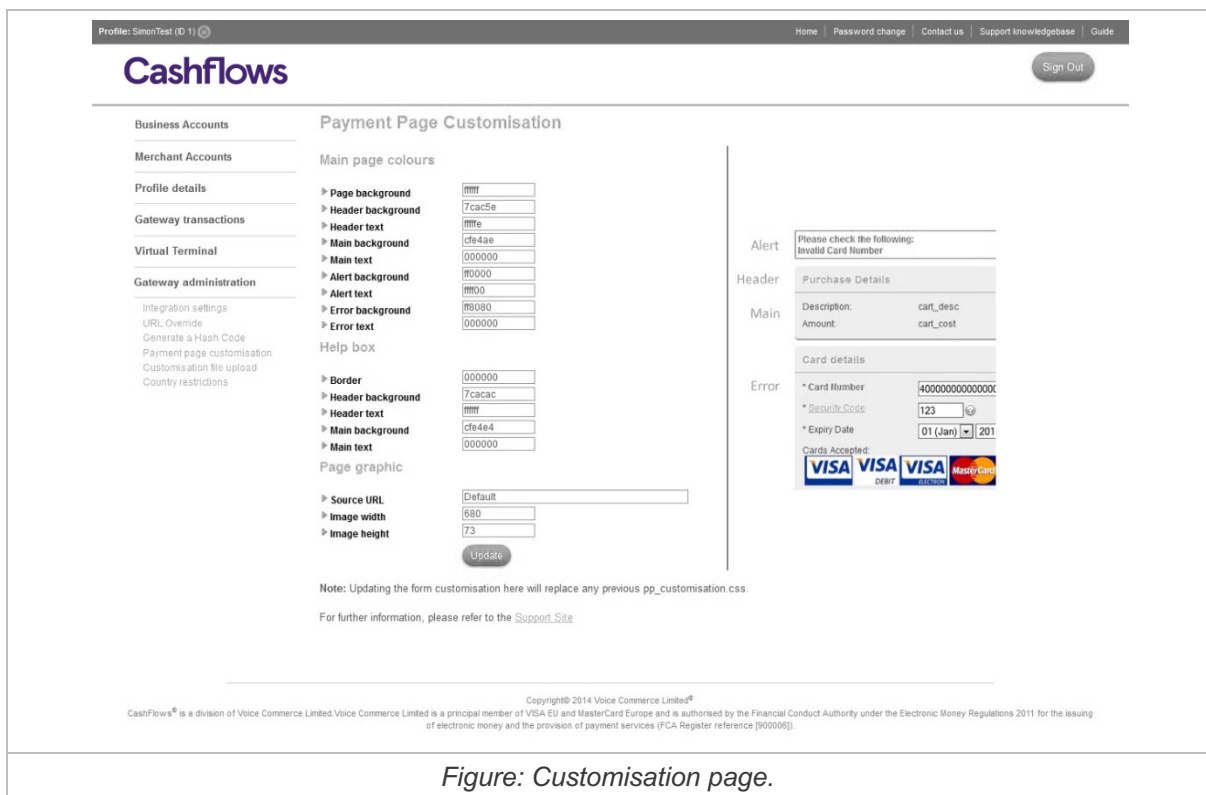


Figure: Customisation page.

To change the colour of a payment page element, enter a Hex colour reference without the # prefix into the fields provided. For a list of the entire web safe colours, including their Hex reference visit:

http://www.w3schools.com/html/html_colornames.asp

http://www.w3schools.com/css/css_colors.asp

If you wish to replace the standard payment page logo at the top of the page, specify the full secure URL, for example, <https://www.cashflows.com/images/logo.png>. You will also need to specify the size of the image in the fields provided as this may lead to distortion of the image.

Advanced customisation

You can completely customise the payment pages look and feel to match your websites design, by uploading your own style sheet, images and payment page container files, helping reduce form dropout rates and instils brand confidence to your consumers.

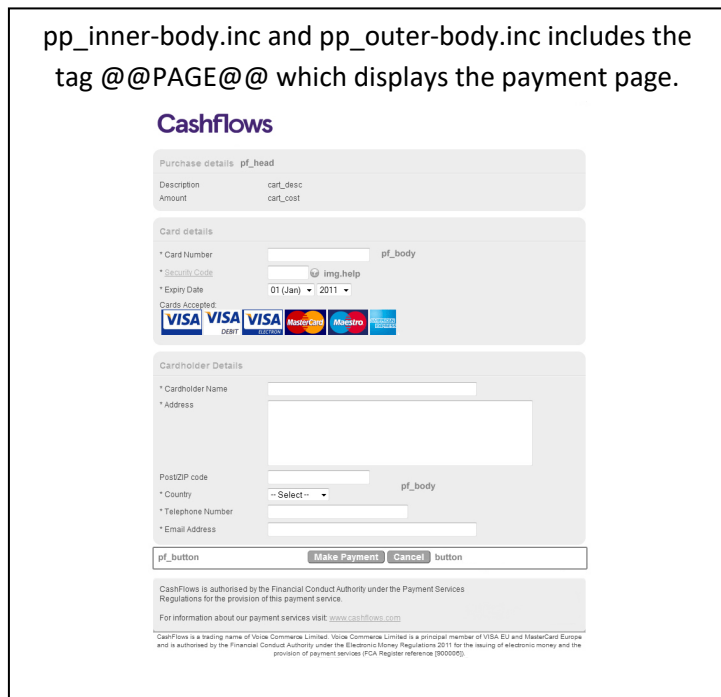
To fully change the look of the payment page you will need to upload HTML payment page container files, containing references to your style sheet and images.

Payment Page container files

There are three container files that are used to display the payment page and enable you to customise the payment page.

The payment page container files are structured as follows:

Layout.html includes the html tag, Meta data, the @@head@@ tag and @@body@@ tag which pulls in the body includes files.



layout.html

The layout.html file is used for all payment pages including the result pages and allows you to add your own Meta data to the head element including changing the title tag. The layout.html file **must** contain the @@HEAD@@ and @@BODY@@ tag, as the @HEAD@@ tag contains all the default style sheets elements and the @@BODY@@ tag pulls in the body include files.

Default layout.html

```

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html lang="en">
<head>
<title>@@TITL@@</title>
@@HEAD@@
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
<meta name="description" content="Payment Page - Powered by CashFlows"/>
<meta name="keywords" content="Payment Page - Powered by CashFlows"/>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/>
<meta name="viewport"
      content="width=device-width,initial-scale=1.0,maximum
scale=1.0,user_scalable=no"/>
</head>
<body class="@@CTXT@@">
@@BODY@@
</body>
</html>

```

Warning: The use of server (Java, PHP, ASP, .Net), or client side (JavaScript, AJAX) scripting within the payment page container files is **prohibited** and will cause the uploading of the files to your customisation directory to fail.

pp_outer-body.inc

The pp_outer-body.inc file enables you to add you own header and footer html elements so that it matches your website design. The pp_outer-body.inc **must** contain the **@@PAGE@@** tag which is substituted with the payment page content when rendered to the shopper.

Default pp_outer-body.inc

```

<div class="container">
/* your HTML header content here */
@@LOGO@@
/* Payment Page */
@@PAGE@@
/* your HTML Footer content here */
@@COPY@@
</div>

```

The **@@LOGO@@** tag will be substituted with the logo that you have specified in the 'Payment Page Customisation' facility. The **@@COPY@@** tag is our default copyright statement which you can replace with your own text, if required.

As you can see from the example on the next page, using the **@@PAGE@@** tag within the pp_outer-body.inc file allows you full control over the placement of the payment page.

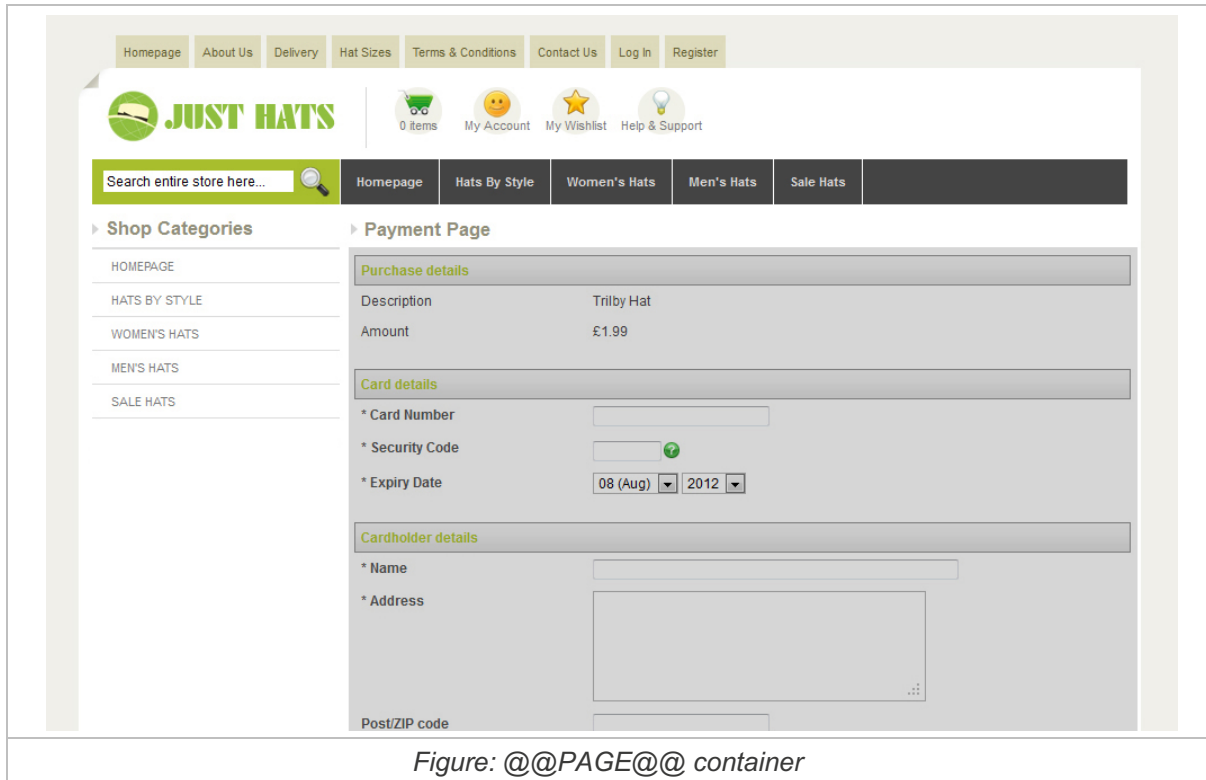


Figure: @@PAGE@@ container

pp_inner-body.inc

The pp_innner-body.inc is used to display information within an Iframe, therefore the container file does not contain the outer-body elements.

Default pp_inner-body.inc

```
<div class="container">
/* Payment Page */
@@PAGE@@
</div>
```

To view and download the default payment container files, please visit:

<https://secure.cashflows.com/templates/{name of container file}>

Style sheets, images and hyperlinks

If your payment page container file includes a style sheet or an image, they must be uploaded to your customisation directory and referenced correctly.

To reference an image within your payment page container file your will need to include your customisation directory location as shown in the following example:

```

```

When the payment page is displayed to the shopper the @@PROF@@ tag is substituted with your profile id.

To include a style sheet (CSS) within your payment page container file you will need to reference it's customisation directory location as shown in the following example:

```
<link href="/customisation/@@PROF@@/style.css" rel="STYLESHEET" type="text/css" media="all" />
```

Warning: To reference a CSS file or image that is not included in your customisation directory you must use the full URL path and the file must be located on a secure (https://) server. If the file does not reside on a secure server then the shopper's browser could generate a security alert, not display the image, or both. This leads to reduced consumer confidence in your store and payment page abandonment.

Any style sheet classes that have a background image must have the full URL path including your profile id, for example (123456):

```
.pf_help_head {
background:url(https://secure.cashflows.com/customisation/123456/nav_bg.png) bottom left repeat-x;}
```

Any hyperlinks included in your payment page container file must also include the full URL path.

The payment page's styles

To change the colour scheme of the payment page you can use the basic customisation facility within the Account Management System. However to change the look and feel further you will need to amend the profile.css file to include your change to the default styles.

The payment pages profile.css file can override a number of different style *rules* used by the payment page to enable you to hide content, display background images, change fonts and colours and re-arrange content. For example to change the colour and font of the payment pages footer you could include the following style sheet rule to the profile.css file.

```
/* Include customisation performed in administration system */
@import url('pp_customisation.css');

/* Put your own overrides here ... */
.copyright {
border-top: 2px solid #454545;
color: #00853f;
font-size: 8px;}
```

To help you understand how the payment page use the default styles, please download the annotated default style sheet from: http://support.cashflows.com/downloads/payment_page.css

To view the usage of the style rules in the design of the payment page, please also refer to [Appendix B](#).

Going Mobile

To enable your payment page to be rendered correctly for different screen sizes, you can simple add a @media statement to your profile.css file. This will make the payment page content responsive and enable you to fully change the user experience if viewed on mobile device.

Example Mobile CSS

```
@media only screen and (min-width: 0px) and (max-width: 568px) {
.container {width: 100%}
.header {width: 100%}
.footer {width: 100%}
.pf_body .rightside {width: 100%}
.pf_body .rightside_small {width: 100%}
.pf_body .textarea{ width: 100%}
.pf_body input.amount { width: 100%}
.mandatory {width: 100%}
.optional {width: 100%}
}
```

Uploading files to your customisation directory

To enable you to fully customise your payment page you must upload your payment page container files, images and style sheets to your customisation directory located on our servers.

To upload your files, login to the Account Management System and select 'Customisation file upload' from the 'Gateway Administration'.

Note: Uploaded images must be in the format of either: .gif, .png, .jpg or .jpeg.

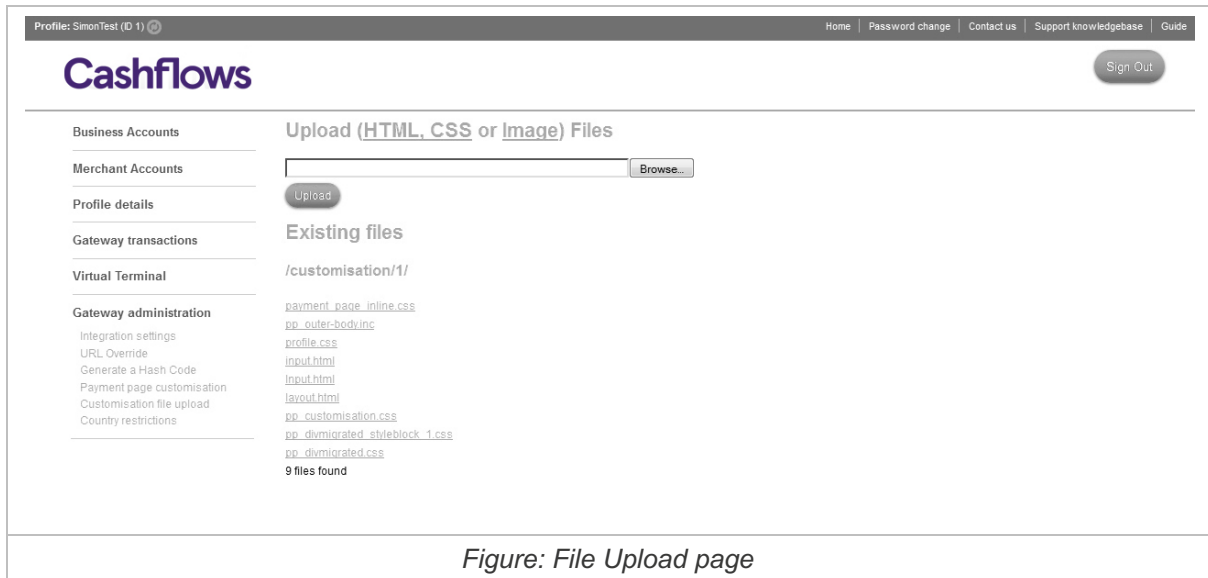


Figure: File Upload page

Reviewing your customisations

To review the changes that you have made to the payment page, you will need to submit a test payment request. This can be achieved quickly and easily using the Account Management System's Hash generator. For further information about the Hash generator, please refer to your Account Management System guide at:

<http://support.cashflows.com/guides>



Testing your integration & going live

To test your integration to our payment page your payment request will need to be sent to the INTEGRATION environment (<https://secure-int.cashflows.com/gateway/standard>) using a valid card number.

CashFlows have provided the following test card numbers to allow you to complete your integration:

Card Number	Expiry Date	CW
4000000000000002 (VISA)	Any valid expiry date (mm/yy)	123
4462030000000000 (VISA prepaid)	Any valid expiry date (mm/yy)	444
5555555555554444 (MasterCard)	Any valid expiry date (mm/yy)	321
5597507644910558 (MasterCard prepaid)	Any valid expiry date (mm/yy)	888

Once you are satisfied that your integration is complete you can start processing live transactions by switching to the PRODUCTION URL (<https://secure.cashflows.com/gateway/standard>) and switching your integration store_id for your production store_id.

Warning: Please ensure that you update your production account details with relevant callback and/or return URL's and customisation files; taking care to change the store_id in any customisation files.



Appendix A: Payment system response codes

Status 'A' is authorised, anything else is not. The auth code and auth message for authorised transactions cannot be predicted (as they can change from one bank/issuer to the next).

'V' is a validation error (e.g. invalid card number)

'D' is a decline

'B' is a blocked transaction

'R' is a referral (has to be treated as a decline)

'C' is a cancelled transaction (e.g. user pressed cancel on payment page)

'S' is a system error

These will be followed by a 3 digit code. The first digit is an internal code which can be ignored. The second two digits are the actual error code for the given status. Attached is a list of the current error codes. (Please note this list is subject to change).

The list is given as, for example, Vx01 which means it is the result for V101, V201, V301 etc.

Code	Reason
Vx01	Invalid merchant details
Vx02	Invalid expiry date
Vx03	Invalid start date
Vx04	Invalid issue number
Vx05	Invalid CVV
Vx06	Invalid card number
Vx07	Card holder name not set
Vx08	Insufficient address details
Vx09	Invalid country code
Vx10	Invalid cart ID
Vx11	Invalid email address
Vx12	Invalid phone number
Vx13	Invalid amount
Vx14	Invalid currency code
Vx15	Invalid customer IP
Vx16	Original trans not found
Vx17	Invalid merchant IP
Vx18	Unknown transaction type
Vx19	Card number changed
Vx20	Currency changed
Vx21	Original trans ref required
Vx22	Amount exceeds original
Vx23	Can not refund this type of transaction
Vx24	Amount changed
Vx25	User account details required
Vx26	Invalid request
Vx27	Original trans not pre-auth
Vx28	Transaction mode changed
Vx29	Card/Currency combination not supported
Vx30	Unknown card type
Vx31	Issue number required
Vx32	Issue number not required
Vx33	Duplicate transaction
Vx34	Unable to void transaction
Vx35	Original trans was not authorised

Vx36	Invalid PIN
Vx37	Unknown transaction class
Vx38	Original transaction type does not match
Vx39	Card expired
Vx40	CVV Required
Vx41	Original transaction already settled
Vx42	Original transaction already cancelled
Vx43	This card does not support the required transaction type
Vx44	Transaction details do not match original
Vx48	User Details not valid
Vx52	3DS Not Enabled
Vx53	3DS Data Invalid
Vx54	Concurrent Authorisations
Vx55	Invalid Funds Recipient Date (MCC 6012 Merchants)
Dx01	Non-specific decline
Dx02	Declined due to funds (insufficient/limit exceeded)
Dx03	Retain card response
Dx05	On our blacklist
Dx07	Live/test mismatch
Dx08	Refund: Insufficient merchant funds in account
Dx10	Card authorisation attempt limit reached
Dx11	Monthly Scheme Decline Rate limit reached
Dx40	Continuous Authority cancelled for the transaction
Dx41	Continuous Authorities cancelled for the merchant
Dx43	Continuous Authorities cancelled for the card
Dx90	Pre-Authorisation anti-fraud block
Dx91	Post-Authorisation anti-fraud block
Rx01	Not Authorised
Ex01	Transaction error
Cx01	Transaction cancelled
Cx02	Transaction expired
Sx00	Invalid transaction Request
Sx01	Connection failure
Sx02	Invalid response
Sx03	Response timeout
Sx04	Server error
Sx05	Server error
Sx06	No response from issuer

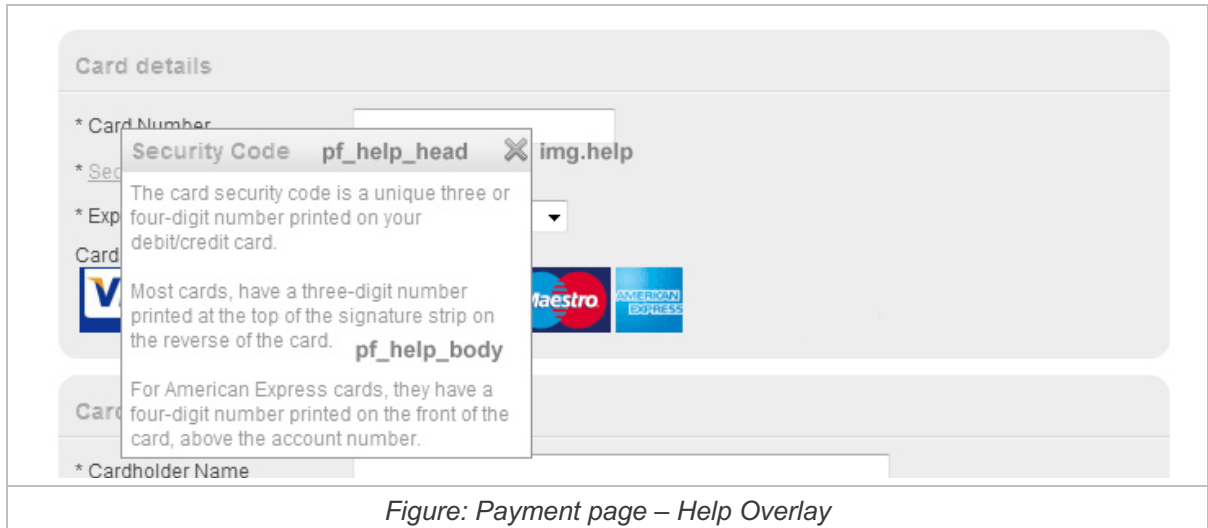


Figure: Payment page – Help Overlay

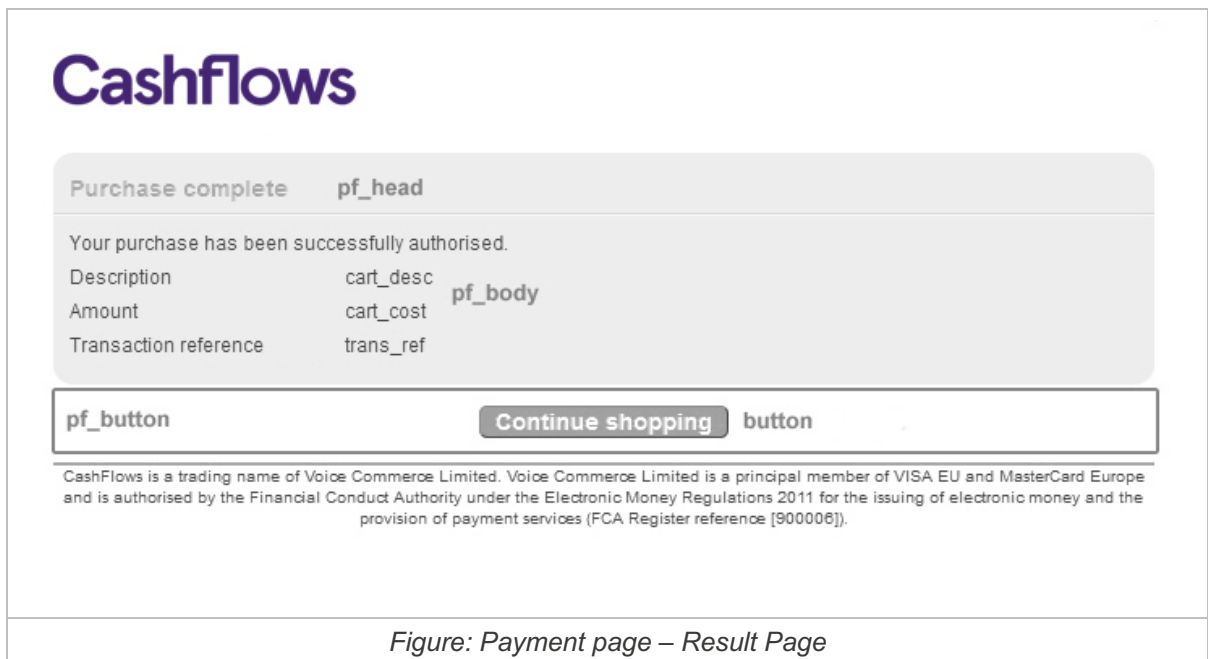


Figure: Payment page – Result Page

**Appendix C: Card types returned in callback response**

Visa Corporate Credit	Visa Corporate Debit
Visa Purchasing Credit	Visa Purchasing Debit
Visa Credit	Visa Debit (Delta)
Visa Prepaid	Visa Electron
Mastercard Corporate Credit	Mastercard Corporate Debit
Mastercard Credit	MasterCard Debit
Mastercard Prepaid	Maestro
Maestro UK (Was Switch)	Amex
Amex Purchasing	