
First Atlantic Commerce Hosted Page Integration Guide for Plugins

Version 1.9, 14 February, 2020

Contents

Introduction	4
Hosted Pages.....	5
Overview	5
Simple integration with the Merchant’s checkout page using an Iframe	6
PART 1 - Designing a Payment Page	7
Implementing the Page.....	7
Page HTML Format.....	7
Permitted Fields	9
Using Merchant Administration Portal to Create your Hosted Page	11
Appendix 1 - Testing Considerations	23
Appendix 2 – Test Cards for FAC Test Environment	25
Appendix 3 – Response Codes	27
Appendix 3.1 – System Response Codes and Reason Codes.....	27
Appendix 3.2 – ISO Response Codes.....	30
Appendix 3.3 – 3D-Secure Response Codes	34
Appendix 3.4 – AVS Response Codes.....	35
Appendix 3.5 – CVV Response Codes	36
Appendix 7.6 – Fraud Control Response Codes.....	37
Appendix 4 - Glossary of Terms	39

Change Log

Document Version	Description	Release Date
V1.0	Initial version	20 th Jan 2012
V1.1	Web service name updated	9 th Jan 2013
V1.2	Fraud Control and other Enhancements	18 th Apr 2013
V1.3	Updated formatting, clarified several sections, added appendices	24 th Jul 2013
V1.4	Updated Device Data Collector form name in code snippet to correct form name	28 th Jul 2015
V1.5	Updated RecurringDetails in Detailed Field Descriptions Added XML POST specifications Added SOAP message sample for HostedPageResults Request Restructured code snippets into separate Appendices (6 - PHP and 7 - C#) Added C# code snippets for: <ul style="list-style-type: none"> • HostedPageAuthorize • HostedPageResults • ComputeHash Added new Appendix (8) Signature and URL Encoding of the Signature	22 nd Aug 2018

	Expanded information on Page Templates Removed references to deprecated "MerRespURL" Updated CKEditor/CKFinder help links	
V1.6	Updated ExecutionDate format	21 nd Feb 2019
V1.7	Updated to use new KOUNT specifications	10 th July 2019
V1.9	Updated HPP Editor Documentation Added common Error/Response Codes	14 th February 2020

Introduction

This document will guide a developer through the integration process required to use First Atlantic Commerce's (FAC) Payment Gateway (PG) Hosted Page (HP) Service and additional operations for managing your transactions. The document describes in detail the integration process, general steps in generating/publishing a payment page to FAC's servers along with requirements for implementing your Hosted Payment Hosted Page.

The Hosted Payment Page transaction specifications within the document include the following:

- Standard Authorization Only or Authorization with Capture (with or without Address Verification)
- 3D Secure Authentication with Authorization or Authorization with Capture (with or without Address Verification)
- Tokenized Authorization Transactions
- Recurring Transactions
- Fraud Control (with Kount®)

Additional web services and operations outside of the Hosted Payment Page that can be used to manage your transactions include:

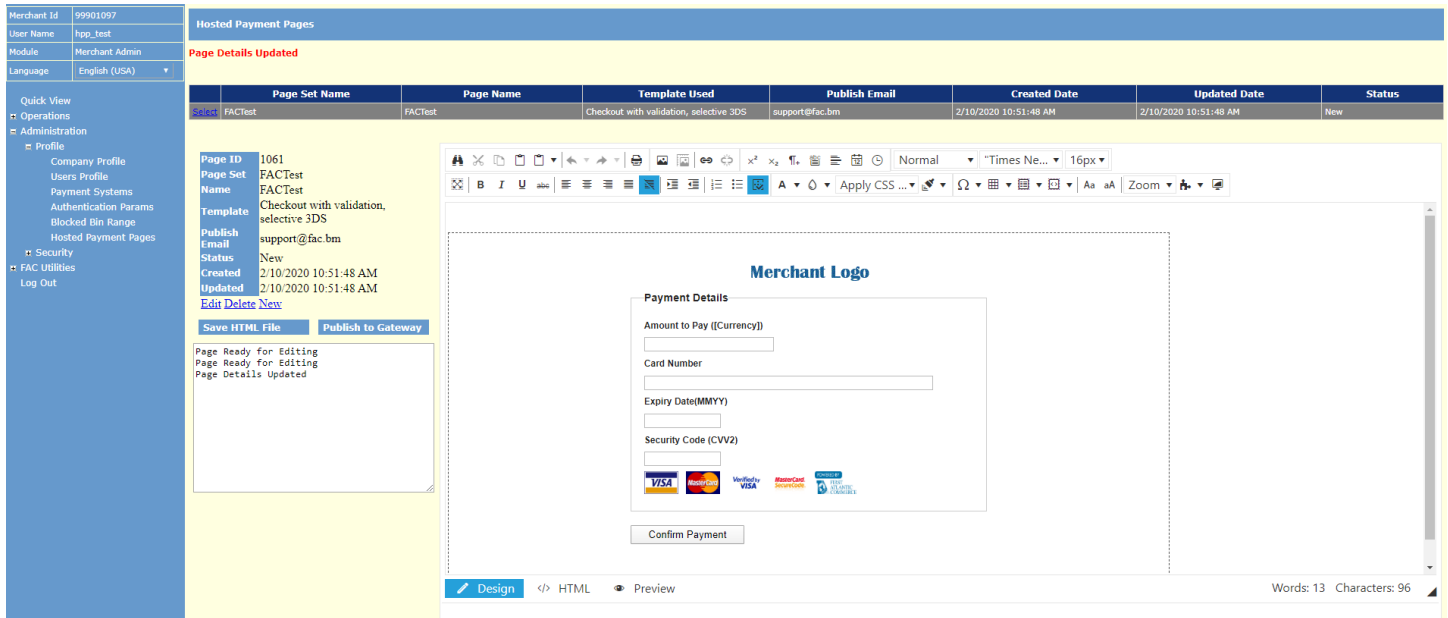
- Transaction Modification (for Captures, Reversals or Refunds)
- TransactionStatus
- Notifications

A few important details to note about Hosted Payment Pages

- Using a Hosted Page, a merchant never needs to never have access to or know the Card Number (PAN) used by the Cardholder.
- Although FAC's servers are hosting the merchant's payment page, the creation, coding and management of the page is of the responsibility of the merchant or merchant's developer(s). A payment page could be as simple or complex as a merchant would like it to be.
- Please note that integration via Hosted Page is not a way of reducing the work required to integrate to the Payment Gateway, the integration via a Hosted Page is just as complex as the integration via our API.
- The advantages of using Hosted Pages can be great, especially when you consider the PCI Audit requirements that come into scope when you store Card Numbers on your servers.
- It is also important to note that in order to integrate a merchant's site or payment module to FAC's gateway, a developer must be able to provide client-side security to be able to connect to FAC using HTTPS as to pass data via SSL.

Overview

- Hosted pages are complete pages of HTML that reside on servers at FAC.
- They are designed and maintained by the Merchant in the “Hosted Payment Pages” section of the FAC Merchant Administration Portal, as follows:



The screenshot displays the 'Hosted Payment Pages' management interface. On the left is a navigation menu with options like 'Quick View', 'Operations', 'Administration', and 'Profile'. The main area shows a table of page sets and a detailed view of a specific page set.

Page Set Name	Page Name	Template Used	Publish Email	Created Date	Updated Date	Status
FACTest	FACTest	Checkout with validation, selective 3DS	support@fac.bm	2/10/2020 10:51:48 AM	2/10/2020 10:51:48 AM	New

The detailed view for the selected page set includes the following information:

- Page ID:** 1061
- Page Set Name:** FACTest
- Page Name:** FACTest
- Template:** Checkout with validation, selective 3DS
- Publish Email:** support@fac.bm
- Status:** New
- Created:** 2/10/2020 10:51:48 AM
- Updated:** 2/10/2020 10:51:48 AM

Below the details are buttons for 'Save HTML File' and 'Publish to Gateway', and a log showing 'Page Ready for Editing', 'Page Ready For Editing', and 'Page Details Updated'.

The main editor area shows a preview of the payment page layout, which includes a 'Merchant Logo' section and a 'Payment Details' form with fields for:

- Amount to Pay ((Currency))
- Card Number
- Expiry Date(MMY)
- Security Code (CVV2)

At the bottom of the form are logos for VISA, MasterCard, American Express, and Discover, along with a 'Confirm Payment' button.

(Please treat all data shown here as fictitious. All screenshots are for exemplary purposes only.)

- Once the page has been created and published, the merchant needs to use the PageSet, PageName and MerID to in order to use the page in a staging or live environment.

Simple integration with the Merchant's checkout page using an iFrame

- The Hosted Payment Page can be presented to the user on an **iFrame** within the merchant's web page. When integrating the hosted page this way, it blends in with the Merchant's checkout page, so the user will see a seamless page experience.
- The Hosted Page design is fully customizable with CSS, javascript and popular javascript libraries.
- Here's an example of how an **iFrame** would look like within a sample merchant checkout page:

Please Complete your subscription

Enjoy your plan:
You'll be charged starting on March 1st, and then the subscription will be automatically renewed on a monthly basis. You can cancel at any time, just give us call.

Subscribe now

Your Plan includes:

- 150 minutes of worldwide long distance calling
- 2500 local text messages
- Unlimited local calling
- 6gb of data

1 year subscription	\$64.99
Taxes	\$6.49
Total Billed now	\$71.48

I
F
R
A
M
E

PART 1 - Designing a Payment Page

Implementing the Page

Page HTML Format

The HTML page must adhere to a certain format, the FAC Payment Gateway expects to see one Form (and ONLY one form, with ID of "FrmCheckout") on the page. Here is an example of how the page should look like before fields are added:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-GB">
<head>
<title></title>
<link rel="stylesheet" href="css/blueprint/screen.css" type="text/css" media="screen, projection"/>
<meta http-equiv="Content-Type" content="application/xhtml+xml; charset=utf-8" />
</head>
<body>
<form id="FrmCheckout" method="post" action="" style="background-color: #FFFFCC" class="span-24">
  <div class="container">
    <div class="span-24">
      <p></p>
    </div>

    <div class="span-24">
      <p>
        <br />
        Content Goes Here
      <br />
    </p>
    </div>

    <div class="span-24">
      <p></p>
    </div>
  </div>
</form>
</body>
</html>
```

- Please note that we allow the use of the CSS library “Blueprint”. This is for convenience and allows the use of div elements in a tabular format without too much CSS programming. It keeps your HTML clean of embedded STYLE elements.
 - For more information on Blueprint, please see: <http://blueprintcss.org/>
 - And, specifically, this tutorial is the most useful:
 - <http://net.tutsplus.com/tutorials/html-css-techniques/a-closer-look-at-the-blueprint-css-framework/>

Page Rules:

- The Page must start with an HTML element
- It must include a HEAD element with the links as shown above
- It must include a FORM element called “FrmCheckout”
- All the fields added must be one of the permitted fields (see the next section)
- All fields must be INPUT element fields
- There must be a button or mechanism that submits (POSTS) the Form.
- INPUT id and name attributes must be the same.

Permitted Fields

- The FAC Payment Gateway expects to see fields with specific names and descriptions. In addition, we recommend that validation be added to restrict the data entered to only the data required, in line with OWASP standards.
- Some fields can be processed either by passing into the call to **HostedPageAuthorize** or by including on the form. If included on the form, the value of these fields takes precedence over any values passed into **HostedPageAuthorize**. In this case, you should ensure that values on the form are valid and completed by the user before being processed.

Here is a Table of all INPUT fields of type TEXT allowed on hosted payment pages, with validation rules:

Category	Input "id"/"name"	Format	Notes
Card Details	Amount	N(4-10) "#0.00"	Optional. For displaying of amount to user. If added to the form will be auto-populated with Amount passed in call to HostedPageAuthorize. Will not be processed by hosted page. If edited by the user, should be used to populate the (hidden) PurchaseAmt field in Currency unit format (see below).
	CardNo	N(16 – 19)	Mandatory. Max 16 for non-Amex, 19 for Amex. <u>Numeric only</u>
	CardExpDate	N(4)	Mandatory. MMY Format
	CardCVV2	N(3 - 4)	Conditional. May be required depending on processor. Usually 3 digits.
	IssueNumber	N(2)	Required for Debit Cards Only where applicable (e.g. UK Debit cards)
	StartDate	N(4)	MMYY Format. Debit Cards only and is usually required if Issue number is not mandatory.
	PurchaseAmt	N(12) or N(4-10) Decimal "#0.00" format.	Optional. Transaction Amount in Currency units or Decimal format. Currency unit format is padded left with Zeros. E.g.: 10.00 = 0000000001000. If included in Form will override what has been passed into HostedPageAuthorize. Decimal format ("#0.00") will be converted to Currency Unit format when hosted page is posted.
	PurchaseCurrency	N(3)	Optional. ISO Numeric Currency code. E.g. 840 for US Dollars
	PurchaseCurrency Exponent	N(1)	Optional. Number of decimal places. Usually 2 for most currencies
	SessionId	AN(30)	Optional. A Unique ID for Kount Fraud Control Processing. See the Fraud Control Section for more information.
Billing Details (all optional)	BillToFirstName	AN(30)	
	BillToMiddleName	AN(30)	
	BillToLastName	AN(30)	
	BillToAddress1	AN(50)	

	BillToAddress2	AN(50)	
	BillToCity	AN(30)	
	BillToState	AN(2)	State Code. Max A(2) if USA only. You could hide this field and use a drop down to set the value. Max A(3) for non US.
	BillToCounty	AN(15)	County Name
	BillToPostCode	AN(10)	Or Zip Code. Strictly Alpha-Numeric only.
	BillToCountry	N(3)	Country Code. Hide this field and use a drop down to set the value.
	BillToTelephone		
	BillToEmail		
	BillToFax	AN(30)	
	BillToMobile	AN(30)	
Shipping Details (all optional)	ShipToFirstName	AN(30)	
	ShipToMiddleName	AN(30)	
	ShipToLastName	AN(30)	
	ShipToAddress1	AN(50)	
	ShipToAddress2	AN(50)	
	ShipToCity	AN(30)	
	ShipToState	A(3)	State Code. Max A(2) if USA only. You could hide this field and use a drop down to set the value. Max A(3) for non US.
	ShipToCounty	AN(15)	County Name
	ShipToPostCode	AN(10)	Strictly Alpha-Numeric only.
	ShipToCountry	N(3)	Country Code. Hide this field and use a drop down to set the value.
	ShipToTelephone	AN(30)	
	ShipToEmail	AN(50)	
	ShipToFax	AN(30)	
	ShipToMobile	AN(30)	

Address Text Validation Rules (for a full list, see the [Appendix](#)):

- No special characters
- No accents
- No special Symbols
- Avoid all unnecessary symbols
- Standard punctuation is OK
- Mandatory fields MUST have values

Using Merchant Administration Portal to Create your Hosted Page

- While it is possible to create a Page from scratch, it is advisable to use a template from our Merchant Hosted Page Administration App as a starting point for the Page implementation. This is accessible via FAC's Merchant Administration online portal.
- You will need to use the Hosted Page Administration Application in Merchant Administration to publish the page on the FAC's Merchant Pages site.
- To create a page, the developer/designer must follow some steps within the Hosted Page Administrator.
- FAC will provide you with access and login credentials to the Merchant Administration Online Portal. Here you will be able to create and manage your page(s).
- The URL to the Merchant Administration portal:
 - Test environment -
<https://ecm.firstatlanticcommerce.com/sentry/paymentgateway/merchant/administration/WFrmLogin.aspx>
 - Production environment -
<https://marlin.firstatlanticcommerce.com/sentry/paymentgateway/merchant/administration/WFrmLogin.aspx>
 - Once you are logged in, you can navigate to the Hosted Pages Administration Application under the left hand side menu.

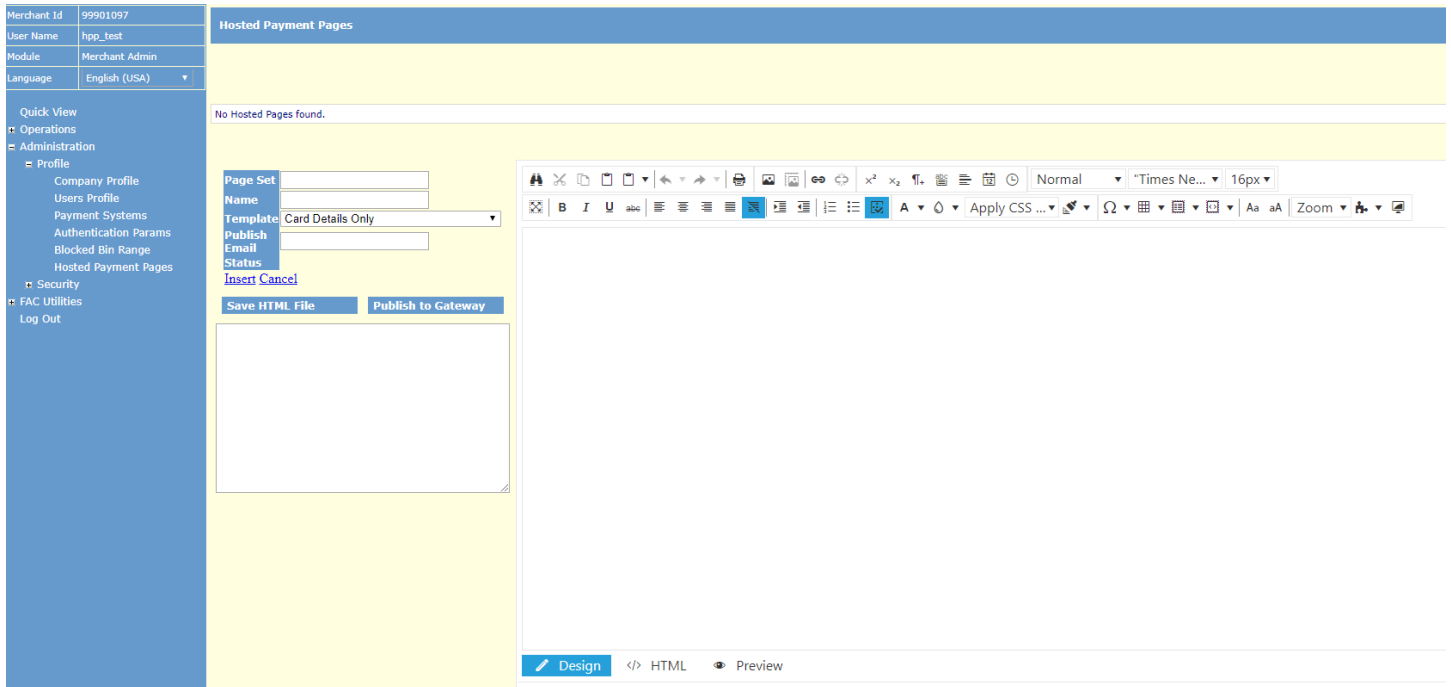
Creating a new blank page

- As you can see, there are no pages defined for your account, so the “No Hosted Pages found” message is displayed.
- To create a new page, click the “Create New Page” link, then a blank form is displayed:

The screenshot displays the Merchant Admin interface. On the left is a navigation menu with categories like Quick View, Operations, Administration, Profile, Company Profile, Users Profile, Payment Systems, Authentication Params, Blocked Bin Range, Hosted Payment Pages, Security, FAC Utilities, and Log Out. The main content area is titled 'Hosted Payment Pages' and shows a message: 'No Hosted Pages found.' Below this message is a 'Create New Page' link. To the right of the link are two buttons: 'Save HTML File' and 'Publish to Gateway'. A rich text editor toolbar is visible above a large blank text area. At the bottom of the editor, there are tabs for 'Design', 'HTML', and 'Preview', and a status bar showing 'Words: 0 Characters: 0'.

Choosing a template and filling up additional information

- The next step is choosing a template and filling up additional information such as Page Set and Page Name.
- FAC has a series of HTML Templates that provide different fields and formats and validations. More Details about these templates are explained below.



The fields have the following meanings:

HPP Fields	
Page Set	<p>The Name of a Set of Pages. This can be anything although it should reflect your business division name.</p> <ul style="list-style-type: none"> • This gives assurance to Cardholders that they are dealing with the Merchant even when paying directly to FAC. • Note: Do not put any spaces in the name, as it forms part of the URL for the Page.
Page Name	<p>The Name of the Page. e.g. PayPage, PayNow, Payment. Can be whatever you decide.</p>

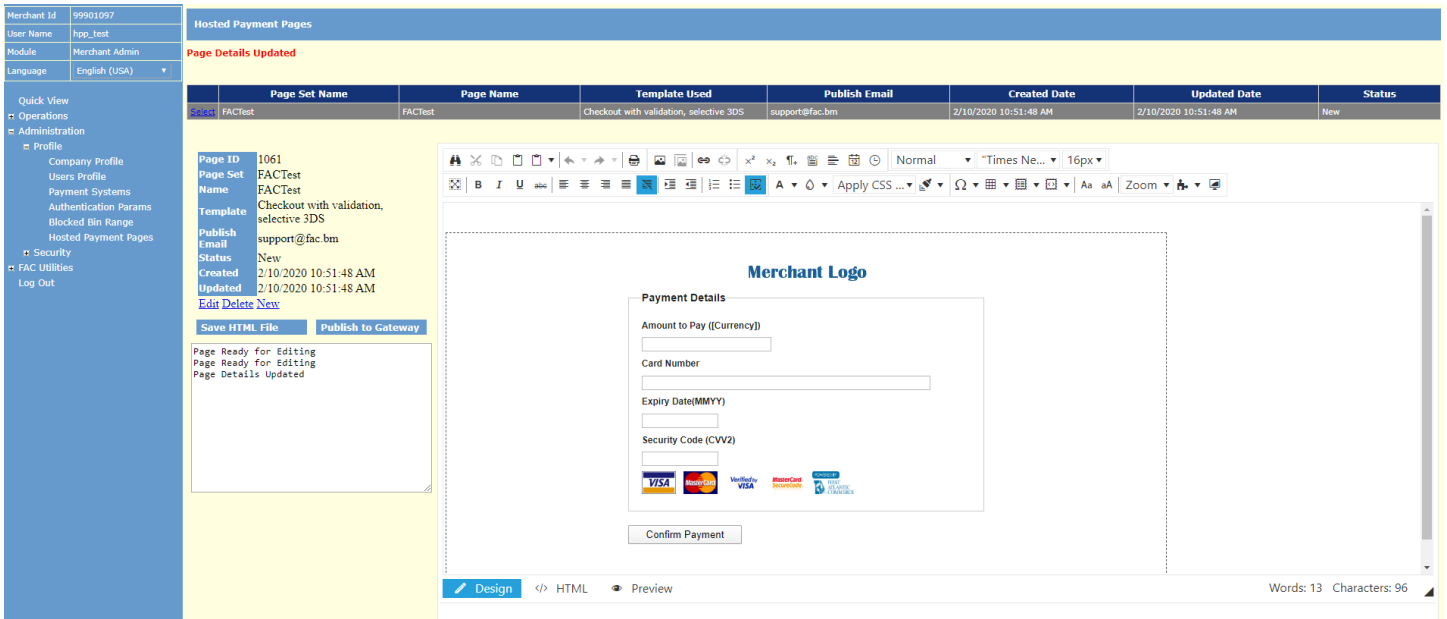
	<ul style="list-style-type: none"> • Again, do not use any spaces, as it is part of the Page URL.
Publish Email	The email address of the Author is a good candidate here. If there are any issues with the Page, FAC will contact the Author by using this email address. Note that the “Publish Email” is never visible to cardholders / end users of the payment page.
Status	Read only field that shows the state of the page (New or Published).

Hosted Payment Page Templates	
Card Details Only	<ul style="list-style-type: none"> • Fields: Amount to Pay, Card Number, Expiry Date(MMY), Security Code (CVV2). • NOTE: This is the most basic template containing the minimum fields required. • There is no data validation built-in to the “Card Details Only” template. Merchants who use this template must add their own data validation. <p>If you need a basic template with data validation already built-in, use the “CheckoutWithValidation” template (see F below).</p>
Card and Billing	<ul style="list-style-type: none"> • Fields: All of the above (Card Details) plus BILLING address fields: • First Name, Last Name, Street Address, City, State/Region, Zip/Postal Code, Country Code, Telephone, Email. • NOTE: Billing address fields are OPTIONAL and not supported by all banks/processors. • There is no data validation built-in to the “Card and Billing” template. Merchants who use this template must add their own data validation.
Card, Billing and Shipping	<ul style="list-style-type: none"> • Fields: All of the above (Card and Billing Details) plus SHIPPING address fields: • First Name, Last Name, Street Address, City, State/Region, Zip/Postal Code, Country Code, Telephone, Email.

	<ul style="list-style-type: none"> • NOTE: Billing and Shipping address fields are OPTIONAL and not supported by all banks/processors. <p>There is no data validation built-in to the “Card, Billing and Shipping” template. Merchants who use this template must add their own data validation.</p>
Debit/Credit Card Only	<ul style="list-style-type: none"> • Fields: Amount to Pay, Card Number, Expiry Date(MMYY), Security Code (CVV2), Issue Number, Start Date(MMYY) • NOTE: Issue Number, Start Date(MMYY) fields are OPTIONAL and not supported by all banks/processors. It is best to avoid using this template unless instructed by FAC support. • There is no data validation built-in to the “Debit/Credit Card Only” template. Merchants who use this template must add their own data validation.
Blank Template	<ul style="list-style-type: none"> • If you are starting from scratch, choose the Blank Template.
Checkout With Validation	<ul style="list-style-type: none"> • Fields: Amount to Pay ([Currency]), Card Number, Expiry Date(MMYY), Security Code (CVV2). • NOTE: The “CheckoutWithValidation” template contains the minimum fields required, PLUS it will enforce validation of the Card Number, Expiry Date(MMYY), and Security Code. • For merchants’ convenience, data validation is built-in to the template for these 3 fields. • Merchants should replace the “Merchant Logo” image with their own logo, and replace “[Currency]” with their own merchant currency (e.g. “USD”). • This template also includes the ‘Visa’, ‘MasterCard’, ‘Verified by Visa’, ‘MasterCard SecureCode’ and ‘Powered by FAC’ logos. All of these logos are required for merchants processing 3DSecure. Merchants processing NON-3Dsecure should remove the ‘Verified by Visa’ and ‘MasterCard SecureCode’ logos, as they are not applicable to non-3DS. • This template, when properly customized per above guidelines, meets FAC’s basic requirements

	that we review during End to End testing and Site Review of your website’s payment process.
Card Details , Selective 3DS	<ul style="list-style-type: none"> • Same functionality as Card Details Only Template. Adds 3DS downgrade for for AMEX/Discover cards
Checkout with Validation , Selective 3DS	<ul style="list-style-type: none"> • Same functionality as Checkout with Validation Template. Adds 3DS downgrade for AMEX/Discover Cards.

Once completed, select the “Insert” link. The page will be added and the default template will appear in the editor:



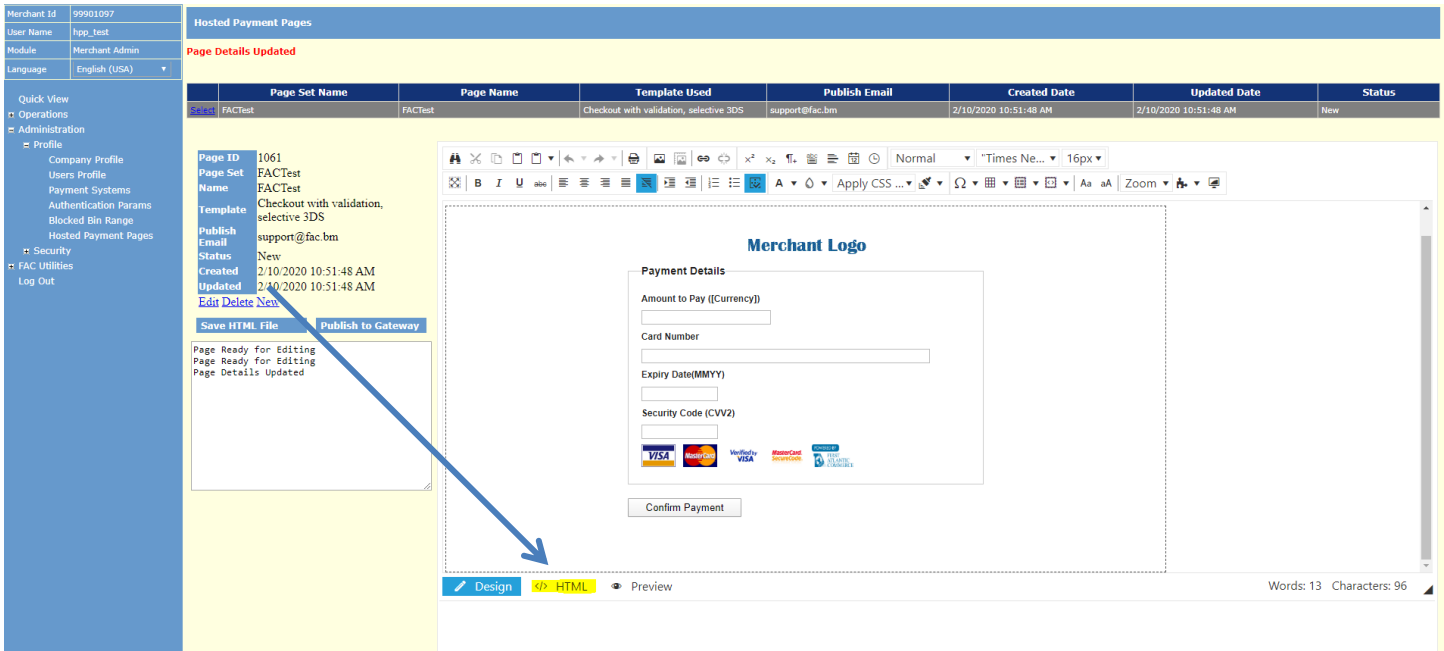
The screenshot shows the 'Hosted Payment Pages' management interface. On the left is a sidebar with navigation options like 'Quick View', 'Operations', 'Administration', and 'Profile'. The main area displays a table of page sets with columns for Page Set Name, Page Name, Template Used, Publish Email, Created Date, Updated Date, and Status. Below the table, there's a detailed view of a page set (Page ID: 1061) with fields for Name, Template, Publish Email, Status, Created, and Updated. The main editor area shows a payment form template with a 'Merchant Logo' placeholder and a 'Payment Details' section containing input fields for 'Amount to Pay ((Currency))', 'Card Number', 'Expiry Date(MMY)', and 'Security Code (CV2)', along with a 'Confirm Payment' button. The interface also includes a 'Design' toolbar and a status bar at the bottom.

- The hosted page can be customized according to the merchant needs. You can even use JavaScript libraries (from a CDN source) to enhance the page with UI widgets not available in plain HTML.
- Our recommendation is to:
 - **to enhance the page to look like one of your own**
 - **to add data validation to the payment page fields to ensure the data passed is valid, scrubbed or rendered to the proper format.**

- The templates adhere to the following guidelines by default:
 1. A form set to the “post” method
 2. A fieldset element to group “text” type input elements.
 3. A label element related to each “text” input
 4. Simple 3-column layout using Blueprint CSS
 5. A single input with submit type for posting the form.
- You are free to use any of the templates elements as they are or change them for your own.
- Please note the input fields posted with the form must exist in our “[Permitted Fields](#)” list.
- The editor on the form is a standard HTML editor that has many features, it is called Telerik RadEditor.
- You can get plenty of information about this editor by looking at these links:
 - The Telerik RadEditor itself: <https://demos.telerik.com/aspnet-ajax/editor/examples/overview/defaultcs.aspx>

Editing HTML directly

You can use the built in page designer to create and modify the hosted page or you can also use the integrated HTML editor by clicking in the “HTML” view button on the bottom of the editor’s.



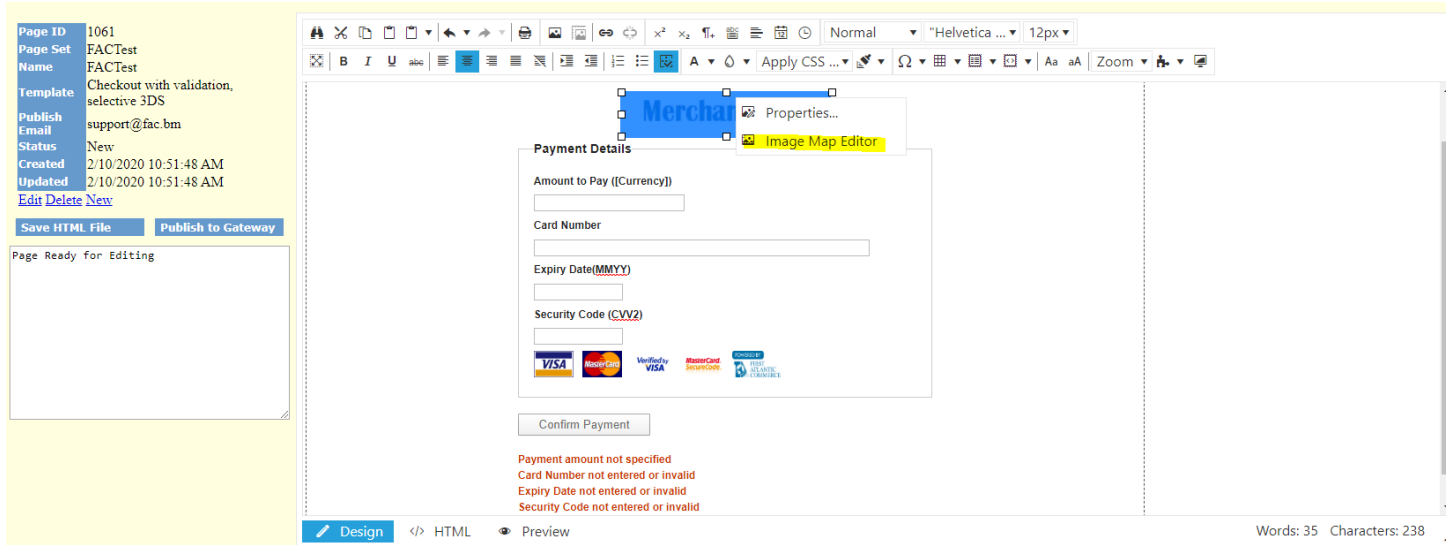
The screenshot displays the FAC Hosted Payment Pages management interface. On the left is a navigation menu with options like 'Company Profile', 'Users Profile', and 'Administration'. The main area shows a table of 'Hosted Payment Pages' with columns for Page Set Name, Page Name, Template Used, Publish Email, Created Date, Updated Date, and Status. Below the table, a 'Page Details' panel shows information for Page ID 1061, including its name, template, publish email, status, and creation/updated dates. A 'Save HTML File' button is highlighted with a blue arrow pointing to the 'HTML' view button at the bottom of the editor. The editor itself shows a payment form with fields for 'Amount to Pay', 'Card Number', 'Expiry Date', and 'Security Code', along with a 'Confirm Payment' button and logos for Visa, MasterCard, and American Express.

It’s entirely possible to copy the source text and paste it into your favorite editor, and then paste it back once edited.

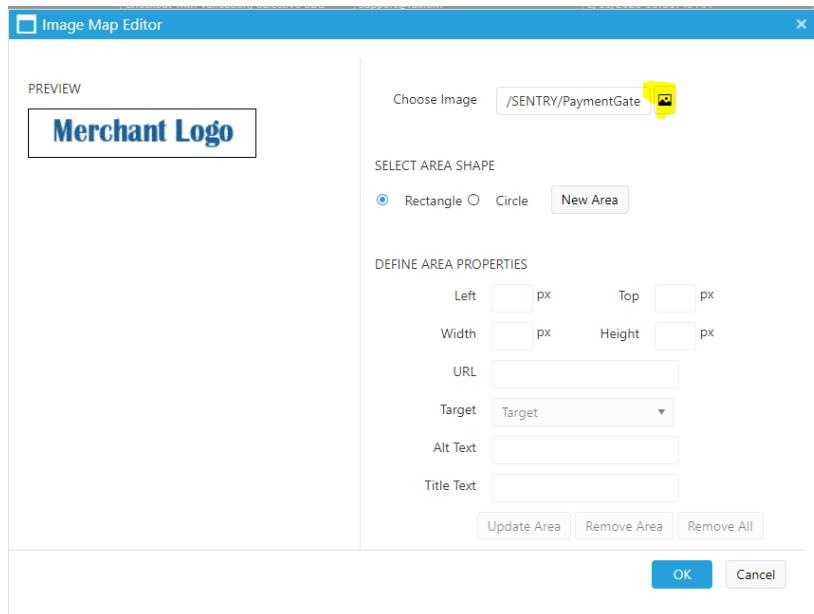
Uploading Images

- One thing you will definitely need to do is change the image on the Template page from the FAC default image to something related to your business. Of course, you can also delete the image. Hosted Pages allow you upload many image files for inclusion on your pages for, say, the company logo, card types accepted icons, etc.

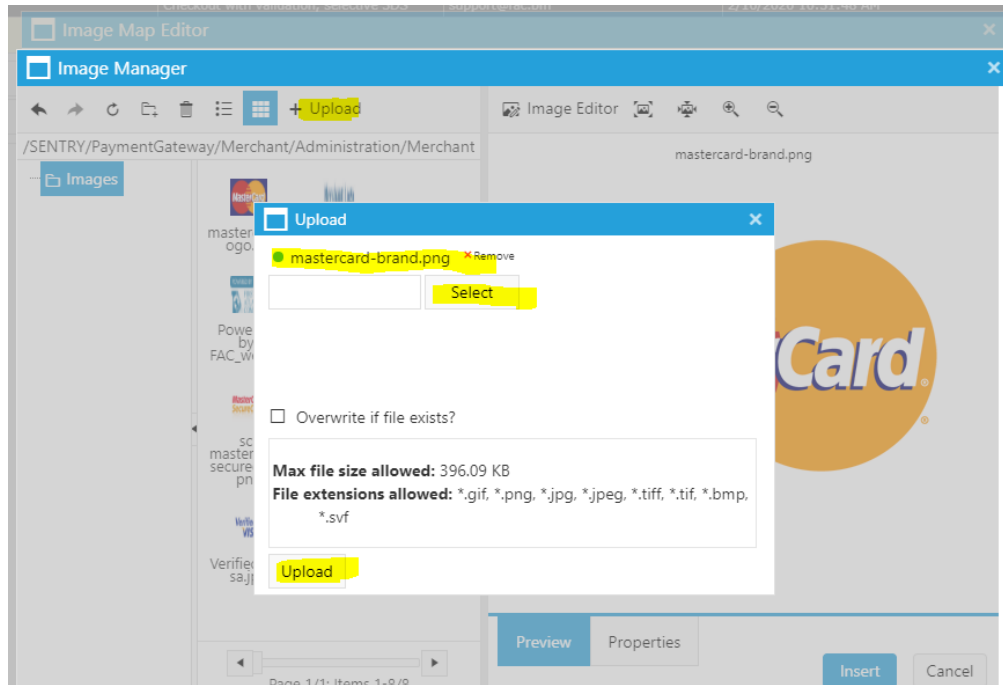
- 1) To change the image, click and select the image in the editor, then right click and select “Image Map Editor”, as seen in the screenshot below: You will then see an Image Map Editor dialog.



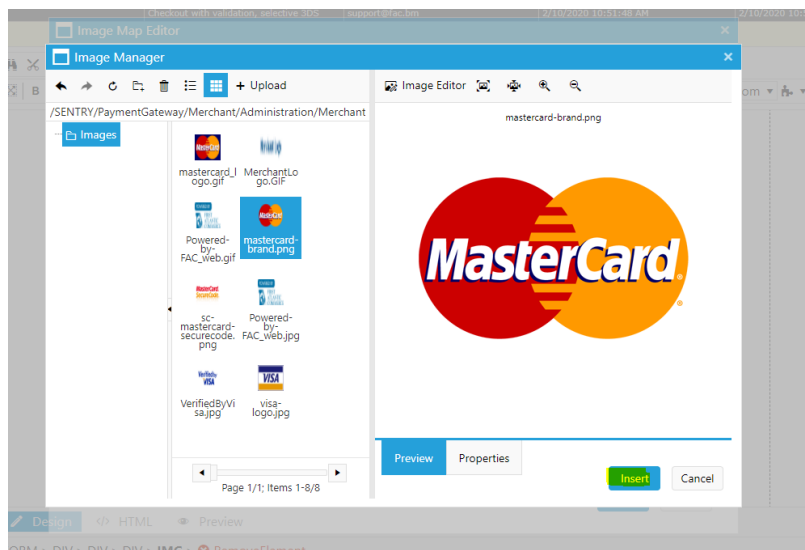
- 2) Image Map Editor - Click the image icon to browse to the desired image



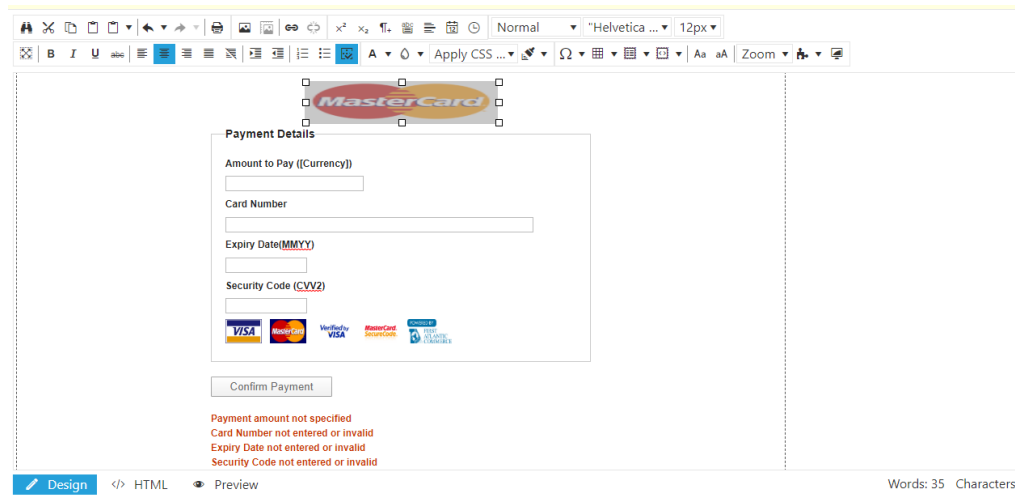
- 3) Press the Upload button then the Select button to browse to the desired image. Once selected press upload in the bottom left hand corner.
 - Here you also have the option to select multiple images to upload.



- 4) You will then be taken back to the Image Manager.
 - Please press insert and an image will be available to the HPP



5) Image on Page



Saving and Publishing the Page

- Once you finished with your edits, it is important to select the “Save HTML File” highlighted link to the left of the editor.
 - If you do not do this, you will lose all your HTML edits.

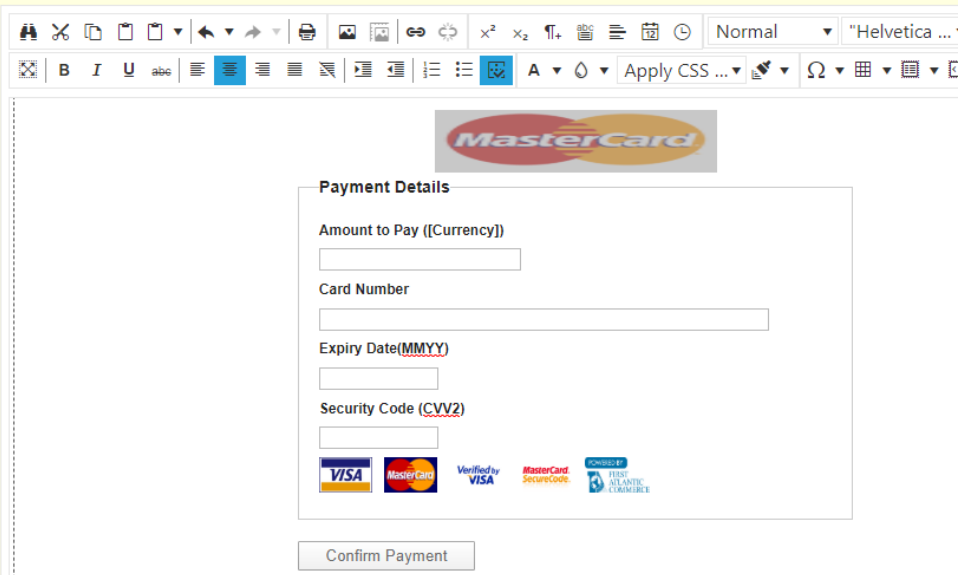
Page Set Name	Page Name	Template Used	Publish Email	Created
FACTest	FACTest	Checkout with validation, selective 3DS	support@fac.bm	2/10/2020 10:51:48 AM

Page ID 1061
 Page Set FACTest
 Name FACTest
 Template Checkout with validation, selective 3DS
 Publish Email support@fac.bm
 Status New
 Created 2/10/2020 10:51:48 AM
 Updated 2/10/2020 10:51:48 AM
[Edit](#) [Delete](#) [New](#)

Save HTML File [Publish to Gateway](#)

```

Page Ready for Editing
Validating HTML...
Validation Passed
Creating back-up of existing file...
Saving HTML File...
File Saved
    
```



Payment Details

Amount to Pay ((Currency))

Card Number

Expiry Date(MMY)

Security Code (CVV2)

- Once the page is saved and you are ready to release the page, select the “Publish to Gateway” link.
 - This will validate the page and may fail if it finds issues.
 - Common errors can be a misspelled input names or ids so you may need to edit and re-publish.
 - Once published, the page is ready to be used as a Hosted Page on your e-commerce transactions.
 - The details on how you integrate this Hosted Payment Page on your website is covered in the next section (Part 2).


Page Published

Page Set Name	Page Name	Template Used	Publish Email	Created Date	Updated Date	Status
FACTest	FACTest	Checkout with validation, selective 3DS	support@fac.bm	2/10/2020 10:51:48 AM	2/12/2020 4:05:44 PM	Published

Page ID: 1061
 Page Set: FACTest
 Name: FACTest
 Template: Checkout with validation, selective 3DS
 Publish Email: support@fac.bm
 Status: New
 Created: 2/10/2020 10:51:48 AM
 Updated: 2/10/2020 10:51:48 AM
[Edit](#) [Delete](#) [New](#)

[Save HTML File](#) [Publish to Gateway](#)

```
Page Ready for Editing
Validating HTML...
Validation Passed
Creating back-up of existing file...
Saving HTML File...
File Saved
Page Published
```




Payment Details

Amount to Pay ((Currency))

Card Number

Expiry Date(MMY)

Security Code (CVV2)



Payment amount not specified
 Card Number not entered or invalid
 Expiry Date not entered or invalid

Appendix 1 - Testing Considerations

When testing your payment page and payment process it is important that you consider testing for the following:

✓ Data Validation

FAC performs basic data validation on parameter values submitted for credit card payments. The information that will be provided to FAC from the Hosted Payment Page should be validated or rendered to the proper format prior to payment submission as to avoid rejected transactions. If the formatting is improper, it will be processed as is (is not modified), therefore if invalid data is supplied or does not meet FAC's specifications, the transaction will fail or be rejected outright. It is highly recommended that you implement data validation to ensure the data passed is valid, scrubbed or rendered to the proper format. Parameters and their specifications are all outlined in this integration guide and it includes a quick reference table in the Appendix.

As an example: The 'CardNumber' specifications are that it be a 16 digit numeric value. FAC will not accept spaces, dashes, alpha characters or other symbols. If submitted the transaction will result in failure. In the event a Cardholder enters an invalid card number like 4111-1111-1111-1111, how do you want to handle this? Will the Cardholder see a message on the screen asking them to check their card number and allow them to try again? Will information be provided on the screen to the cardholder to advise them of the acceptable format? Will the Cardholder be restricted from entering anything but numbers?

NOTE: If you are utilizing Address Verification (AVS), it very important that you follow the guidelines for data formats. Issuers only validate standard alpha and numeric values. Ensuring that you are passing the appropriate data formats will not only reduce or eliminate rejections but you will get a more accurate AVS result.

✓ Transaction Approvals

Testing approvals seems quite simple, however you may want to consider any of your processes that are initiated by an approval. As an example, is there any additional customer validations that need to take place? Does the Cardholder receive an email confirmation or a receipt? Will an internal process be initiated internally with the business administrative staff or trigger a change in inventory?

✓ Transaction Declines

When testing Issuer/Processor declines you will want to be certain that your system is handling these according to the businesses requirements. Depending on the returned 'ReasonCode' you may want to display a particular message to the Cardholder. You may want to restrict how many times a Cardholder reattempt a transaction or notify them to contact a customer service agent to assist with their payment on the website. Your team may want to receive a notification when a Cardholder reaches a threshold of attempts.

✓ Transaction Errors

Once a transaction has been processed, it can have one of three statuses. It can be approved by the Issuer, declined by the Issuer/Processor and lastly, it could have failed. In case of a transaction failure, there is a problem with processing the transaction. It could be for a number of reasons but in all cases, FAC will respond with a 'ResponseCode' of 3. In

these cases, you will want to check that your payment module is handling these as you require. As an example in a live real-time environment, you may choose to display a message to the Cardholder to try again later and initiate a notification to your team for investigation.

✓ **Page Errors**

The Hosted Payment Page has a life cycle of 5 minutes, so you may want to consider how your site will handle cases where the Cardholder takes more than 5 minutes to complete their payment details and submit a payment. Perhaps in this circumstance you may want to display a message stating that their payment session expired and to try again or maybe also bring the Cardholder back to the payment page or home page.

✓ **Payment Page Browser Rendering (Page Format)**

You can design your payment page how you wish. It can be very simple and basic or you can add a lot more complexity to it. This can have an effect on how different browsers display your page and the functionality of buttons, fields or drop-downs (if used). Assuming the merchant's customers will be using other browsers other than Internet Explorer it may be wise to test your payment page from different internet browsers to validate how they are rendered.

✓ **Captures, Refunds and Reversals**

If you are using the 'TransactionModification' method for processing capturing (in a two-pass processing method), reversing or refunding transactions you will want to test that this is functional especially within the production environment. You will want to test cases where the requests are not only approved but denied as to ensure your system is handling them as deemed necessary by the business.

As an example, should a refund be denied because the refund cutoff period on your merchant account has expired, how will your system handle this? Will notification be sent out to the technical team? Will the person that processed the refund see on their screen a message stating that the refund did not go through?

As a second example, if you have implemented or are using address verification (AVS), depending on the AVS result, you may want to reverse a transaction to cancel it or capture a transaction if you wish to proceed with the payment.

✓ **Overall Cardholder Payment Experience**

It is up to the merchant and the business to determine how they want to represent themselves, products, and services to their customers and how they want the overall customer experience to be when making a credit card payment on their site including your Hosted Payment Page. Although this is outside the scope of FAC we recommend that ample quality assurance be done on our site to satisfy the needs of the business and that it supports their required functions of the site/payment process.

Appendix 2 – Test Cards for FAC Test Environment

The following is a list of test cards you can use to receive specific responses for testing purposes.

It is important to note the following:

- These test cards do not apply to \$0 AVS-Only testing. For this type of transaction, use real credit cards so as to get valid AVSResult data.
- Any valid expiry date and any 3 digit CVV2 value will work for these test cards
- Note: “Normal Approval” means ResponseCode=1, ReasonCode=1 and “Normal Decline” means ResponseCode=2, ReasonCode=2 in the web responses returned for Auth only and Auth/Capture transactions.
- All card numbers not listed above are defaulted to Normal Approval.
- For every approved transaction, you will receive the same ‘dummy’ authorization ID of 123456.
- These cards are **only to be used in the test environment** (ecm.firstatlanticcommerce.com). Once you are on the production platform, **live** cards must be used.

Visa

Card Number	Response
4111111111111111	Normal Approval, CVV2Result=M
4111111111112222	Normal Approval, CVV2Result=N
4333333333332222	Normal Approval, CVV2Result=U
4444444444442222	Normal Approval, CVV2Result=P
4555555555552222	Normal Approval, CVV2Result=S
4666666666662222	Normal Decline, OriginalResponseCode=05, CVV2Result=N
4111111111113333	Normal Decline, OriginalResponseCode=05
4111111111114444	Normal Approval, AVSResult=M
4111111111115555	Normal Approval, AVSResult=A
4111111111116666	Normal Approval, AVSResult=Z
4111111111117777	Normal Approval, AVSResult=N
4111111111118888	Normal Approval, AVSResult=G
4111111111119999	Normal Decline, OriginalResponseCode=98
4111111111110000	Normal Decline, OriginalResponseCode=91
4222222222222222	Normal Approval, CVV2Result=M, AVSResult=N

MasterCard

Card Number	Response
5111111111111111	Normal Approval, CVV2Result=M
5111111111112222	Normal Approval, CVV2Result=N
5333333333332222	Normal Approval, CVV2Result=U
5444444444442222	Normal Approval, CVV2Result=P
5555555555552222	Normal Approval, CVV2Result=S
5555666666662222	Normal Decline, OriginalResponseCode=05, CVV2Result=N
5111111111113333	Normal Decline, OriginalResponseCode=05
5111111111114444	Normal Approval, AVSResult=Y
5111111111115555	Normal Approval, AVSResult=A
5111111111116666	Normal Approval, CVV2Result=M, AVSResult=Z
5111111111117777	Normal Approval, CVV2Result=M, AVSResult=N
5111111111118888	Normal Approval, CVV2Result=N, AVSResult=U
5111111111119999	Normal Decline, OriginalResponseCode=98
5111111111110000	Normal Decline, OriginalResponseCode=91
5222222222222222	Normal Approval, CVV2Result=N, AVSResult=U

Appendix 3 – Response Codes

Appendix 3.1 – System Response Codes and Reason Codes

The ResponseCode, ReasonCode and ReasonCodeDescription fields of the AuthorizeResponse and TransactionStatusResponse messages can hold the following code combinations.

NOTE: If you are using Fraud Control services there will be additional potential Reason Codes and Reason Code Descriptions than described below (refer to [Fraud Response and Reason Codes](#)).

ResponseCode Values

Response Code	Description
1	Approved
2	Declined
3	Error

Reason Code for “Approved” Response Code (1)

Reason Code	Reason Text (ReasonCodeDescription)	Note
1	Transaction is approved.	Normal Approval.

Reason Codes for “Decline” Response Code (2)

Reason Code	Reason Text (ReasonCodeDescription)	Note
2	Transaction is declined.	Normal Decline.
3	Transaction is declined.	Referral. Call for further details on this transaction.
4	Transaction is declined.	Pick up card (if possible) or report to authorities.
35	Unable to process your request. Please try again later.	Merchant exceeds allowed limit.
38	Transaction processing terminated. Please try again later.	Transaction is not permitted to merchant.
39	Issuer or switch not available. Please try again later	Issuing bank or switch not available. Transaction has timed-out.

Reason Codes for “Error” Response Code (3)

Reason Code	Reason Text (ReasonCodeDescription)	Note
5	Connection not secured.	Connection was not secured.
6	HTTP Method not POST.	HTTP Method not POST.
7	“Field” is missing.	Named field is missing.
8	“Field” format is invalid.	Named field format is invalid.
10	Invalid Merchant.	Not such merchant.
11	Failed Authentication (Signature computed incorrectly).	Merchant was found but computed signature does not match one included in the request.
12	Merchant is inactive.	Merchant is not enabled for processing.
14	Merchant is not allowed to process this currency.	Currency supplied is not permitted.
15	Merchant settings are not valid.	Merchant record is not correctly setup in the system.
16	Unable to process transaction.	Unable to authenticate merchant now. Try later.
36	Credit Cardholder canceled the request.	Credit Cardholder canceled the request.
37	Card Entry Retry Count exited allowed limit.	Card Entry Retry Count exited allowed limit.
40	Duplicate Order Not Allowed	Merchant order identification numbers must be unique
42	Illegal Operation by Card Holder. Check Order Status.	Cardholder Pressed the back button while the transaction was processing. Check the status of that order.
60	Duplicate Order Not Allowed.	A transaction for the same card number and same amount was processed previously and thus this transaction has been blocked (optional setting)
90	General Error during processing. Please try again later.	An unexpected error occurred in the system.
98	System is temporarily down. Try later.	System is temporarily down. Try later.
401	Cycle interrupted by the user or client/browser connection not available.	Client Browser connection not available or card holder referred in the process (Back/F5).
994	FACPGWS BeginTransactionStatus Failure	Error while attempting to run the TransactionStatus Operation Try again. If this persists, contact FAC support at support@fac.bm for assistance.

995	FACPGWS EndTransactionStatus Failure	Error while attempting to run TransactionStatus Operation. Try again. If this persists, contact FAC support at support@fac.bm for assistance.
996	Not a web-based transaction	The transaction for which you are requesting the response data is not a web-based transaction. It is a MOTO transaction and as such there is no web-based response data for this transaction.
997	FACPGAppWS Failure	Error while attempting to run the TransactionStatus Operation. Try again. If this persists, contact FAC support at support@fac.bm for assistance.
998	Missing Parameter	One of the parameters required by the TransactionStatus Operation was not supplied.
999	No Response	There is no response data for the Order ID provided.
1001	FACPGWS Invalid Protocol. Only HTTPS Allowed	The request was sent via HTTP not HTTPS.
1002	Missing Parameter(s)	One or more of the required parameters is missing in the web method you have called.
1003	Invalid Parameter Settings	Both "AVS Only" and "PreAuthenticated" flags have been included in the TransactionCode when calling the Authorize web method. This is not allowed.
1004	Invalid Amount. Not 12 characters in length	Amount must be exactly 12 characters in length, right-aligned, left-padded with zeros. For example, \$12.00 = 000000001200
1010	FACPGWS Authorize HTTP Response Not OK	Error while attempting to run the Authorize Operation. Try again. If this persists, contact FAC support at support@fac.bm for assistance.
1020	FACPGWS Authorize Failure	Error while attempting to run the Authorize web method. Try again. If this persists, contact FAC support at support@fac.bm for assistance.
1030	FACPG BeginCRRError	Error while attempting to run either the Capture, Reversal or Refund web methods. Try again. If this persists, contact FAC support at support@fac.bm for assistance.
1031	FACPG EndCRRError	Error while attempting to run either the Capture, Reversal or Refund web methods. Try again. If this persists, contact FAC support at support@fac.bm for assistance.

Appendix 3.2 – ISO Response Codes

The response codes for an Authorization are returned in the OriginalResponseCode field of the Response. See also AuthorizeResponse, TransactionModificationResponse, or TransactionStatusResponse (see main FACPG2 Integration Guide). They are specific to the Card Issuer.

VISA

Response Code & Description		Response Code & Description	
00	Approved	53	No savings account
01	Refer to issuer	54	Expired card
02	Refer to issuer (special)	55	Incorrect PIN
03	Invalid merchant	56	No card record
04	Pick-up card	57	Transaction not permitted to card
05	Do not honor	58	Transaction not permitted to card
06	Error	59	Suspected fraud
07	Pick-up card (special)	60	Card acceptor contact acquirer
08	Honor with identification	61	Exceeds withdrawal limit
09	Request in progress	62	Restricted card
10	Approved for partial amount	63	Security violation
11	VIP Approval	64	Original amount incorrect
12	Invalid transaction	65	Activity count exceeded
13	Invalid amount	66	Card acceptor call acquirer
14	Card number does not exist	67	Card pick up at ATM
15	No such issuer	68	Response received too late
16	Approved, update track 3	75	Too many wrong PIN tries
17	Customer cancellation	76	Previous message not found
18	Customer dispute	77	Data does not match original message
19	Re-enter transaction	80	Invalid date
20	Invalid response	81	Cryptographic error in PIN
21	No action taken (no match)	82	Incorrect CVV
22	Suspected malfunction	83	Unable to verify PIN
23	Unacceptable transaction fee	84	Invalid authorization life cycle
24	File update not supported by receiver	85	No reason to decline
25	Unable to locate record	86	PIN validation not possible
26	Duplicate file update record	88	Cryptographic failure
27	File update field edit error	89	Authentication failure
28	File temporarily unavailable	90	Cutoff is in process
29	File update not successful	91	Issuer or switch inoperative
30	Format error	92	No routing path
31	Issuer sign-off	93	Violation of law

32	Completed partially	94	Duplicate transmission
33	Expired card	95	Reconcile error
34	Suspected fraud	96	System malfunction
35	Card acceptor contact acquirer	97	Format Error
36	Restricted card	98	Host Unreachable
37	Card acceptor call acquirer	99	Errored Transaction
38	Allowable PIN tries exceeded	N0	Force STIP
39	No credit account	N3	Cash Service Not Available
40	Function not supported	N4	Cash request exceeds issuer limit
41	Pick-up card (lost card)	N7	Decline for CVV2 failure
42	No universal account	P2	Invalid biller information
43	Pick-up card (stolen card)	P5	PIN Change Unblock Declined
44	No investment account	P6	Unsafe PIN
51	Not sufficient funds	XA	Forward to issuer
52	No checking account	XD	Forward to issuer

MasterCard

Response Code & Description		Response Code & Description	
00	Approved	44	No investment account
01	Refer to issuer	51	Not sufficient funds
02	Refer to issuer (special)	52	No checking account
03	Invalid merchant	53	No savings account
04	Pick-up card	54	Expired card
05	Do not honor	55	Incorrect PIN
06	Error	56	No card record
07	Pick-up card (special)	57	Transaction not permitted to card
08	Honor with identification	58	Transaction not permitted to card
09	Request in progress	59	Suspected fraud
10	Approved for partial amount	60	Card acceptor contact acquirer
11	VIP Approval	61	Exceeds withdrawal limit
12	Invalid transaction	62	Restricted card
13	Invalid amount	63	Security violation
14	Card number does not exist	64	Original amount incorrect
15	No such issuer	65	Activity count exceeded
16	Approved, update track 3	66	Card acceptor call acquirer
17	Customer cancellation	67	Card pick up at ATM
18	Customer dispute	68	Response received too late
19	Re-enter transaction	75	Too many wrong PIN tries
20	Invalid response	76	Previous message not found

21	No action taken (no match)	77	Data does not match original message
22	Suspected malfunction	80	Invalid date
23	Unacceptable transaction fee	81	Cryptographic error in PIN
24	File update not supported by receiver	82	Incorrect CVV
25	Unable to locate record	83	Unable to verify PIN
26	Duplicate file update record	84	Invalid authorization life cycle
27	File update field edit error	85	No reason to decline
28	File temporarily unavailable	86	PIN validation not possible
29	File update not successful	88	Cryptographic failure
30	Format error	89	Authentication failure
31	Issuer sign-off	90	Cutoff is in process
32	Completed partially	91	Issuer or switch inoperative
33	Expired card	92	No routing path
34	Suspected fraud	93	Violation of law
35	Card acceptor contact acquirer	94	Duplicate transmission
36	Restricted card	95	Reconcile error
37	Card acceptor call acquirer	96	System malfunction
38	Allowable PIN tries exceeded	97	Format Error
39	No credit account	98	Issuer Unreachable
40	Function not supported	99	Errored Transaction
41	Pick-up card (lost card)	XA	Forward to issuer
42	No universal account	XD	Forward to issuer
43	Pick-up card (stolen card)		

AMEX

Response Code & Description	
000	Approved
001	Approved with ID
100	Deny
101	Expired Card
106	PIN tries Exceeded
107	Please Call Issuer
109	Invalid Service Establishment
110	Invalid Amount
111	Invalid Account
115	Requested Function Not Support
117	Incorrect PIN
121	Limit Exceeded

122	Invalid Manually Entered 4DBC
183	Invalid Currency Code
199	Valid PIN
200	Deny - Pick up Card
290	Refused, Retain Card
300	Successful
301	Not supported by receiver
302	Unable to locate record
303	Duplicate record
304	Field edit error
380	File update not accepted, high
400	Reversal Accepted
800	Accepted
880	File Fully Accepted
881	File Partially Accepted
882	File Fully Rejected
899	Table not found. Default used
900	Advice Accepted

Appendix 3.3 – 3D-Secure Response Codes

Reason Code	Reason Text (ReasonCodeDescription)	Note
13	Merchant is not allowed to process cards in this Payment system.	Merchant is blocked.
17	Unable to process transaction.	System cannot process a Card Range Request.
18	Unable to process transaction.	System cannot build a Verify Enrollment Request.
19	Unable to process transaction.	System cannot contact Visa Directory.
20	Unable to process transaction.	System cannot build a Payment Authentication.
21	Unable to process transaction.	System could not contact Issuer ACS Server
22	Unable to process transaction.	Issuer ACS responded with invalid data or returned data failed.
23	Unable to process transaction.	System cannot process a Verify Enrollment Request.
31	Authentication successful.	3-D Secure Payment Authentication successful.
32	Authentication failed.	3-D Secure Payment Authentication failed.
33	Authentication successful with attempt.	Attempt authentication was performed.
34	Authentication failed with error.	Authentication result not expected.
41	Card Holder Session Expired.	Cardholder's Session expired while performing a 3DS Transaction. Possibly because he/she closed the window, or pressed the back button in the middle of the transaction.
42	Illegal Operation by Card Holder. Check Order Status.	Cardholder Pressed the back button while the transaction was processing. Check the status of that order.
50	Verify Enrollment response unavailable.	The VERes message came back from the MPI as "U".
51	BIN Not Enrolled.	The VERes message came back from the MPI as "N"
52	Card Not Enrolled.	The VERes message came back from the MPI as "N"
53	Payer Authentication Response Unavailable	The PARes message came back from the MPI as "U".
96	Merchant URL is Missing	Merchant URL is Missing
98	System is temporarily down. Try later.	System is temporarily down. Try later.
401	Cycle interrupted by the user or client/browser connection not available.	Client Browser connection not available or cardholder referred in the process (Back/F5).
1001	FACPGWS Invalid Protocol. Only HTTPS Allowed	The request was sent via HTTP not HTTPS.
1002	Missing Parameter or Parameters	One or more of the required parameters is missing in the web method you have called.
1004	Invalid Amount. Not 12 characters in length	Amount must be exactly 12 characters in length, right-aligned, left-padded with zeros. For example, \$12.00 = 000000001200
1005	Invalid Capture Flag value provided	The CaptureFlag parameter must be set to either "M" for manual capture (authorize only) or "A" for automatic (authorize/capture)

Appendix 3.4 – AVS Response Codes

AVS Codes are returned in the AVSResult field in the Response message of the Operation concerned; one of AuthorizeResponse, TransactionModificationResponse, or TransactionStatusResponse (see main FACPG2 Integration Guide). There are different codes depending on the card type.

Visa

Code	Definition
A	Address matches, Zip code does not match.
B	Street addresses match for international transaction. Postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)
C	Street address and postal code not verified for international transaction due to incompatible formats. (Acquirer sent street address and postal code.)
D	Street addresses and postal codes match for international transaction.
E	Error response for Merchant Category Code.
F	Address does compare and five-digit ZIP codes does compare (UK only)
G	Address information is unavailable for international transaction; non-AVS participant.
I	Address information not verified for international transaction.
M	Street addresses and postal codes match for international transaction.
N	Address and ZIP code do not match.
P	Postal codes match for international transaction. Street address not verified due to incompatible formats. (Acquirer sent street address and postal code.)
R	Retry; system unavailable or timed out.
S	Service not supported by issuer.
U	Address information is unavailable; domestic transactions.
W	Nine-digit ZIP code matches, but address does not match.
X	Exact match, address, and nine-digit ZIP code match.
Y	Address and five-digit ZIP code match.
Z	Five-digit ZIP code matches, but address does not match.
5*	Invalid AVS response (from VISA).
9*	Address Verification Data contains EDIT ERROR.
0	Issuer has chosen not to perform Address Verification for an authorization that was declined.

MasterCard

Code	Definition
A	Address matches, postal code does not.
N	Neither address nor postal code matches.
R	Retry, system unable to process.
S	AVS currently not supported
U	No data from issuer/Authorization System.

W	For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not.
X	For U.S. addresses, nine-digit postal code and address matches; for addresses outside the U.S., postal code and address match.
Y	For U.S. addresses, five-digit postal code and address matches.
Z	For U.S. addresses, five-digit postal code matches, address does not.
5*	Invalid AVS response (from MasterCard)
9*	Address Verification Data contains EDIT ERROR.
0	Issuer has chosen not to perform Address Verification for an authorization that was declined.

Note: For MasterCard, if a 5 digit zip code is sent and a 9 digit zip code is on the cardholder file (and address matches) a response of 'Y' is returned.

Amex

Code	Definition
A	ADDRESS: Address correct, zip code incorrect
N	NO: Address and zip code are no correct.
R	Retry, system unavailable or timeout.
S	Address Verification Service not valid.
U	Address information is unavailable; account number is not US or Canadian.
Y	YES: Address and zip code are correct.
Z	Zip code correct; address incorrect.
5*	Invalid AVS response (from American Express).
9*	Address Verification Data contains EDIT ERROR.

* These responses (5 & 9) for all credit card types are processor-generated responses. Response Code 9 means the record was not sent out for Address Verification. This response will also be returned when address verification has not been requested.

Appendix 3.5 – CVV Response Codes

After checking a CVV2/CVC2, values are returned in the CVV2Result field as follows:

Code	Definition
M	Match
N	No match.
P	Not Processed
S	Should be on card but was not provided. (Visa only)
U	Issuer not participating or certified.

Appendix 7.6 – Fraud Control Response Codes

ResponseCode

Response Code	Description
1	Fraud Check Successful
2	Decline
3	Error

ReasonCode

There are only ReasonCodes for decline and errors (ResponseCode 2 and 3).

Response Code	ReasonCode	Description	Details
2	2020	FraudControl Decline	FraudControl query succeeded without error but the transaction declined, as it did not pass the fraud check rules based on Kount response code.
2	2021	BinCheck Decline	BinCheck was successful but the transaction declined as it did not pass the BinCheck rules based on BIN data.
3	321	BAD_EMAL	The email address does not meet required format or is
3	2001	Merchant Not Enabled	FraudControl is not enabled for this merchant.
3	2002	Invalid Fraud Profile	Merchant settings do not specify a valid fraud profile
3	2003	Missing MerchantId	Could not find fraud-specific MerchantId for this merchant
3	2004	Invalid Fraud Response	Response from Fraud system was invalid
3	2005	FraudCheckOnly Not Supported	FraudCheckOnly transactions are not supported with the current merchant configuration.
3	2006	Simulated Fraud Response	Fraud Response Codes and Score are simulated. For testing only.
3	2007	BinCheck System Error	BinCheck System Error
3	2091	Response Timeout	Timeout waiting for Fraud System Response or communications error
3	2097	Format Error (Various)	Various format errors. Details will be in the description.
3	2096	FraudControl System Error	FraudControl System Exception
3	2099	FraudControl System Error	FraudControl Internal Error

* - ResponseCode 1 has no ReasonCode or ReasonCodeDesc

HPP Error Codes

Description	Response Code	Original Response Code	Reason Code	ReasonCode Description
HPP Token Expired	3	91	3000	Security Token Expired
Invalid or very old token	3	12	3001	Invalid Security Token
CardHolderResponseURL missing	3	97	3002	Missing CardHolderResponseUrl
Insufficient number of fields	3	97	3003	Missing parameters
PageSet or PageName missing	3	97	3004	Missing PageName or PageSet
Hosted Page not found in file system (or db in future)	3	97	3005	Hosted Page not found
Hosted Page validation error	3	97	3006	Hosted Page validation error
Hosted Page results not available	3	12	3007	Hosted Page Results Unavailable
General HPP system error	3	99	3090	Hosted Page System Error

FraudResponseCode (OriginalResponseCode)

These are only if you are subscribed to FAC's fraud service which includes Kount. These are the actual response codes returned by the Fraud System (third party)

Code	System	Description
A	Kount	Authorize
D	Kount	Decline
R	Kount	Review
E	Kount	Escalate
[Various]	PayTrue	See PayTrue Documentation
B	BinCheck	BinCheck decline based on merchant rules and BinCheck data
91	All	Timeout
12	All	Invalid transaction - FraudControl is not enabled for merchant (FOnly)
99	All	Error

Appendix 4 - Glossary of Terms

3D Secure

3D Secure encompasses both Visa's *Verified by Visa* and MasterCard's *SecureCode* security solutions for online e-commerce transactions. These solutions use personal passwords to help protect cardholders' card numbers against unauthorized use.

Authentication

The process of authenticating is used in 3D Secure transactions to verify that the person attempting a transaction with a given credit card number is the actual cardholder by requiring them to enter a personal password they set up when enrolling in the 3D Secure program (either *Verify by Visa* or *SecureCode*).

Authorization

The process of checking that the credit card being used in a transaction contains sufficient funds to cover the amount of the transaction. Note that if sufficient funds are found, the amount is held for a given period of time, waiting to be withdrawn when settlement occurs (the period of time varies based on the issuing bank of the credit card).

Authorization/Capture

An Authorize/Capture not only checks that the credit card being used in a transaction contains sufficient funds to cover the amount of the transaction, it also flags the transaction as captured meaning it is to be sent for settlement in the next settlement period.

AVS (Address Verification System)

AVS is used as an extra level of security for online credit card transactions that takes the first line of the billing address and the zip/postal code of the cardholder and checks if they are valid as compared to what is stored on file for the given credit card number.

CID (Card Identification Digits)

The 4-digit code found on the front of AMEX cards, the CID is used as an extra security step to help to verify that the person using the credit card is the actual cardholder.

CVC2 (Card Verification Code)

The 3-digit code found on the back of MasterCard cards, the CVC2 is used as an extra security step to help to verify that the person using the credit card is the actual cardholder.

CVV2 (Card Verification Value)

The 3-digit code found on the back of Visa cards, the CVV2 is used as an extra security step to help to verify that the person using the credit card is the actual cardholder.

Capture

When a capture is performed (in either an Authorize/Capture or Capture only transaction), it is the process of flagging an already authorized transaction to be settled in the next settlement period.

Hosted Page

A payment page hosted on the servers at FAC.

One-Pass Transaction

A one-pass transaction (also called an authorize/capture transaction in this document) is a transaction that is both authorized and captured (flagged for settlement) at the same time, in a single transaction request.

FACPG and FACPG2

The First Atlantic Commerce Payment Gateway Services. These services support and enable the FAC products [cGate® Secure Real-Time](#) and [cGate® Secure Verify](#).

Refund

A refund is the process of refunding a previously settled transaction. This will appear as a credit on the cardholder's credit card statement.

Reversal

A reversal is the process of reversing a previously captured, but not yet settled, transaction. It means that the transaction will never appear on the cardholder's credit card statement.

Settle/Settled/Settlement

The process of settling a transaction is when the money is taken from the cardholder's account and put into the merchant's account. Once a transaction is settled, it will appear as a charge on the cardholder's credit card statement.

SHA1

Secure Hash Algorithm 1. A message digest (hash) function defined in RFC 3174.

Single-Use Token

A token used to identify a transaction without revealing the details of that transaction and can only be used during the transaction time frame itself. After that, the token is unusable and meaningless.

Used in conjunction with shared secret validation it ensures a safe transaction is performed on a Hosted Page.

Transaction

A transaction is any e-commerce request made by you, the merchant, to FAC. This includes Authorizations (both 3D and Non-3D Secure), Authorization & Captures (both 3D and Non-3D Secure), Captures only, Reversals, Refunds, 3D Secure Authentication Only transactions and AVS Verification Only transactions.

Two-Pass Transaction

A two-pass transaction is a transaction that is processed in two separate transaction requests. The first transaction is the authorization only request and the second transaction (which can come seconds, minutes, hours or even days after the first transaction) captures this transaction and flags it for settlement.