BE PAYMENT READY

Hosted Vault Merchant Integration Guide

Version 1.1.0 – September 2024 – Canada Only

Includes: Hosted Vault

Please Read Carefully

1. You have a responsibility to protect cardholder and merchant related confidential account information. Under no circumstances should ANY confidential information be sent via email while attempting to diagnose integration or production issues. When sending sample files or code for analysis by Moneris staff, all references to valid card numbers, merchant accounts and transaction tokens should be removed and or obscured. Under no circumstances should live cardholder accounts be used in the test environment.

2. The Transaction Risk Management Tool provides additional information to assist in identifying fraudulent transactions. In order to maximize the benefits from the Transaction Risk Management Tool it is highly recommended that you:
    a. Carefully consider the business logic and processes that you need to implement surrounding handling the response information the Transaction Risk Management Tool provides.
    b. Also implement the other fraud tools available through Moneris Gateway (e.g., AVS, CVD, Verified by Visa and MasterCard SecureCode).

3. When testing the Transaction Risk Management Tool there is specific test data that you will need to use. Please carefully review and follow the testing instructions and data provided in the document.

Getting Help

Moneris has help for you at every stage of the integration process.

Getting Started	During Development	Production
Contact our Client Integration Specialists: clientintegrations@moneris.com Hours: Monday – Friday, 8:30am to 8 pm ET	If you are already working with an integration specialist and need technical development assistance, contact our eProducts Technical Consultants: 1-866-319-7450 eproducts@moneris.com Hours: 8am to 8pm ET	If your application is already live and you need production support, contact Moneris Customer Service: onlinepayments@moneris.com 1-866-319-7450 Available 24/7

For additional support resources, you can also make use of our community forums at

http://community.moneris.com/product-forums/

Table of Contents

Skills and System Requirements

In order to use Hosted Vault your system will need the following:

- A web server capable of sending and receiving an HTML POST/GET

In addition, you will need the following knowledge and/or skill set:

- Knowledge of creating an HTML web page and posting forms.
- Knowledge of iframes
- If you are selling more than one item, you will need some knowledge of a client-side scripting language (JavaScript, PHP, etc.) to calculate a final charge amount.
- If you want to create your own custom receipts and perform transaction verification, you will require knowledge of a server-side scripting language (PHP, Perl, ASP, etc.)

It is important to note that all Merchants and Service Providers that store, process, or transmit cardholder data must comply with PCI DSS and the Card Association Compliance Programs. However, certification requirements vary by business and are contingent upon your "Merchant Level" or "Service Provider Level". Failure to comply with PCI-DSS and the Card Association Compliance Programs may result in a Merchant being subject to fines, fees or assessments and/or termination of processing services. Non-compliant solutions may prevent merchants boarding with Moneris Solutions.

As a Moneris Solutions client or partner using this method of integration, your solution must demonstrate compliance to the Payment Card Industry Data Security Standard (PCI DSS) and/or the Payment Application Data Security Standard (PA DSS). These standards are designed to help the cardholders and merchants in such ways as they ensure credit card numbers are encrypted when transmitted/stored in a database and that merchants have strong access control measures.

For further information on PCI DSS and PA DSS requirements, please visit http://www.pcisecuritystandards.org.

For more information on how to get your application PCI-DSS compliant, please contact our Integration Specialists and visit https://developer.moneris.com to download the PCI-DSS Implementation Guide.

1 Introduction to Moneris Hosted Payment Solutions

Moneris' Hosted Vault Solution allows you as a merchant to securely accept payment information from your customers. This is one of the simplest integration methods to accept payments on your website. A few simple lines of coding will allow you to get started with your online payments.

1.1 Integrating Your Hosted Solution

To integrate a Moneris Gateway Hosted Solution, there are five overall sets of tasks and/or activities that you must complete:

1. **Creating a new configuration profile for the solution**. This is done in the Merchant Resource Center. For more information on this, see "Creating a Hosted Payment Solution Configuration Profile" on page 10
2. **Configuring the solution profile**. Configuration is also done using the Merchant Resource Center's Hosted Vault Configuration Tool. For more information on this, see "Configuring a Hosted Payment Solution Profile" on page 1.
3. **Developing the solution**. For more information on this, see "Developing Your Hosted Solution" on page 15.
4. **Testing the solution**. For more information on this, see "Testing a Hosted Payment Solution" on page 25.
5. **Moving the solution into production**. For more information on this, see "Moving to Production" on page 61

1.2 Hosted Vault Account Registration & Update (HVARU)

The Hosted Vault Account Registration & Update Page (HVARU) was designed as a solution for those merchants that do not wish to handle client's credit card or account information. When a transaction is initiated, the transaction specific information is sent to Moneris Gateway HVARU via an HTTP POST. The cardholder can then securely enter their account information. Upon submission Moneris Gateway will forward the cardholder and the response back to the merchant's site so that further action can be taken by the merchant website. Also, upon receiving the response the merchant can perform a Transaction Verification to ensure that the response is from a legitimate request.

The Hosted Vault Account Registration & Update Page will not send any financial transactions — it is used to register and update account information only. The data returned from the HVARU account registration and update is to be used in conjunction with the Vault API of your choice. The APIs are capable of sending financial transactions, and updating account information. For PCI reasons some merchant accounts may be unable to alter the financial account portions of the account through the API; however, updating all other parts of a registered account is possible.

2 Hosted Payment Page Configuration Tool

The Hosted Vault Configuration Tool, part of the Merchant Resource Center, is where you create and configure a profile for your hosted payment solution. Creating and configuring a hosted payment solution profile are the two first steps in the process of integrating the hosted payment solution with your system. To review the steps for integrating your hosted payment solution, refer to Integrating Your Hosted Solution.

In order to use the Hosted Vault Configuration Tool to create and configure a hosted payment solution profile, you need to log in to the Merchant Resource Center test environment.

To log into the Merchant Resource Center test environment go to

https://esqa.moneris.com/mpg

and use one of the following login IDs.

Table 1 Test IDs for Merchant Resource Center

Store ID	Username	Password
store1	DemoUser	password
store2	DemoUser	password
store3	DemoUser	password
store5	DemoUser	password
moneris	DemoUser	password

Table 2 Test IDs for Merchant Resource Center – INTERAC® Online Payment

Store ID	Username	Password
store3	DemoUser	password

Table 3 Test IDs for Merchant Resource Center – Convenience Fee

Store ID	Username	Password
monca00392	DemoUser	password

2.1 Creating a Hosted Payment Solution Configuration Profile

The first step in the process of integrating your hosted payment solution is creating a configuration profile for it using the Merchant Resource Center Hosted Vault Configuration Tool.

2.1.1 Creating a Hosted Vault Configuration

To create a Hosted Vault Configuration:

1. Log in to the Merchant Resource Center
   - QA: https://esqa.moneris.com/mpg
   - Production: https://www3.moneris.com/mpg
2. Do the required development as outlined in "Hosted Vault" on page 1
3. Click on Vault in the menu
4. Click **Hosted Vault Config**
5. Click the **Generate a New Configuration** button

You will be assigned a Hosted Vault ID (res_id), which is the identifier for this unique configuration. You will also be assigned a Hosted Vault Token (res_key). The Hosted Vault ID and Token are sent as part of the registration/update request to securely identify your store and the specific configuration.

Each Moneris Gateway account may have up to five unique Hosted Vault configurations. Each configuration can have a differing appearance as well as handle responses in varying ways. Because the Moneris Gateway test environment is a shared environment there is no limit to the number of configurations assigned to a specific store account. However, there is a 30 day time limit where a store configuration will be deleted after 30 days, regardless of use. Please do not alter or delete configurations that were not assigned to you.

> **NOTE:** In the production environment, an individual must be granted permission to access and alter the configuration.

2.1.2 Configuring the Hosted Vault Page

Generate new res_key

This allows you to change the Hosted Vault Token (res_key). Both the “res_id” and “res_key” are to be kept secure, though if security were to be compromised, you may generate a new “res_key” without having to create a completely new configuration.

Basic Configuration

Response Method

This determines how the transaction response will be handled.

Sent to your server as a POST: Moneris Gateway will use an HTTP POST to send the transaction responses to your web server so that you can store the data_key and proceed with other processes which may be associated with account creation or updates.

Sent to your server as a GET: Moneris Gateway will redirect the cardholder to a URL on your server and attach the response as a URL encoded query string at the end of the URL so that you can store the data_key and proceed with other processes which may be associated with account creation or updates. Please note that there are limitations imposed by the browser and operating system on the length of a query string.

NOTE: When handling the response (POST or GET), you must be able to dynamically parse the data. In the future, new variables may be added and the order of the response variables may change.

Response URL

You will need to specify the URL where the transaction response will be returned (either in a POST or GET). The URL needs to be complete , for example:

not sufficient URL: www.example.com

proper URL: http://www.example.com/response.php

If a URL is missing or improperly typed it may result in a 404 error or a looping page.

> **NOTE:** Click on the **Save Changes** button to save the existing configuration. If the configuration is not saved the current Hosted Vault ID (res_id) and Token (res_key) will be deleted after a period of time

Hosted Vault Page Appearance

Click on the **Configure Appearance** button to specify what will be displayed on the Hosted Vault.

Hex Colour Chart

All colours in the Colours and Styles section must be input as the standard HTML hex colour value. You may click this button to view a colour chart.

Colours and Styles

Background Colour

This defines the background colour of the page.

Font Style

This defines what font group will be used for the HVARU. We have defined three groups – Arial/Helvetica/SansSerif, Times New Roman/Times/Serif and Courier New/Courier/Mono.

Primary Text Colour

This defines the colour of text on the HVARU. This must be legible on the chosen background colour.

Company Name Colour
This defines the colour that will be used for your company's business/merchant name.

Header & Footer Highlight Colour
The HVARU will contain a header and footer and a colour bar is used to define these sections. This defines the colour of the header and footer bars.

Section Divider Colour
The HVARU may be divided into several sections depending on what is displayed. A colour bar is used to define the information. This defines the colour of the section divider bars.

Section Divider Text Colour
Occasionally the Section Divider Bar will contain text – this defines the colour of the text that will appear in the Section Divider Bar. Please ensure that the text is legible (i.e. Do not pick the same colour for the Section Divider Colour and for the Section Divider Text Colour).

Subsection Divider Colour
The HVARU may be divided into several sub-sections depending on what is displayed. A colour heading highlight is used to define the information. This defines the colour of the sub-section headings.

Subsection Divider Text Colour
Occasionally the sub-section headings will contain text – this defines the colour of the text that will appear in the Subsection Divider. Please ensure that the text is legible (i.e. Do not pick the same colour for the Subsection Divider Colour and for the Subsection Divider Text Colour).

Hosted Vault Page Data Fields

Display customer details (cust_id, email, note, phone . . .)
This field indicates whether the Customer ID ("cust_id") is to be displayed on the HVARU – the Customer ID field is often used for membership #'s, policy #s, student IDs, or invoice #s. It is a searchable field from the Merchant Resource Center. Also, this field will indicate whether the HVARU should display other fields such as the customer's email address ("email"), the phone number ("phone") and the "note" field – the "note" field can contain any special instructions. In order to display this information it is required that the "cust_id", "email", "phone" and "note" fields be sent in the transaction request. Please refer to Required Variables - Adding New Profile to Vault to properly send this data.

Display merchant name
This field indicates whether the Merchant Name should also be displayed on the HVARU. The name that will be displayed is the official Merchant Name that Moneris Solutions has associated with the account and the name that the cardholder will see on their credit card statement. It is mandated by industry regulations that the merchant name be displayed on any checkout pages and receipts, but this field may be omitted if the HVARU will be loaded within a frame that already displays the merchant name. If you choose to load the HVARU within a frame, you are then required to have an SSL certificate.

Hosted Vault Page Input Fields

Display AVS input
This defines whether the HVARU should include the prompt for the Address Verification Service (AVS) details. If these input fields are displayed on the Hosted Paypage it is then mandatory that the cardholder complete this data.

Security Features

Referring URL

By adding a URL, you specify that you would like us to check whether the transaction is coming from a location (URL) that you allow. Only POSTs sent from one of the specified URLs will be processed. (It is possible for the Referring URL to be "spoofed" – this is not a guaranteed method of securing your transactions – but it makes it more difficult).

Add URL

Here you can specify up to ten Referring URLs to a max of 255 characters. Each URL needs to be complete and at a registered domain, for example:

not sufficient URL: www.example.com

proper URL: http://www.example.com/response.php

If a URL is missing or improperly typed it may result in a 404 error or a looping page.

After specifying a URL, click on the **Add URL** button to add it to the Allowed URLs list. Once a URL has been added, the **Remove URL** button will become available.

NOTE: To verify your Referring URL, you may POST to https://esqa.moneris.com/HPPDP/myurl.php which will display the URL you are posting from.

Transaction Verification

NOTE: Click on the **Save Verification Settings** button to apply these chosen additional security features to the Hosted Vault configuration. If the security feature is not saved these fields will be returned to their last known saved configuration.

Enable Transaction Verification

This must be checked for transaction verification to be enabled. When Transaction Verification is enabled the HVARU will return a "transactionKey" in the transaction response. When the response is received the fields should be logged and a transaction verification request is sent to Moneris Gateway. Moneris Gateway then replies with transaction information and whether the transaction was valid or not. Each transaction can only be verified once and it must be verified within 15 minutes of the original transaction being performed. This allows you to ensure that the responses sent to your page are not "spoofed" and that you are only receiving the responses once. If you also intend to check the Referring URL you must ensure that the source of the verification request is in the list of Allowed URLs.

Response Method

This determines how the transaction verification response will be handled.

Displayed as XML on our server: Once the transaction verification has been performed the HVARU will generate a page and display an XML string. This can be used in conjunction with cURL, screen scraping or other such methods.

Displayed as key/value pairs on our server: Once the transaction verification has been performed the HVARU will generate a page and display key value pairs. This can be used in conjunction with cURL, screen scraping or other such methods.

NOTE: When handling the response (POST or GET), you must be able to dynamically parse the data. In the future, new variables may be added and the order of the response variables may change.

Card Verification

Enable Card Verification

This must be checked for card verification to be enabled. This allows our system to perform card verification on the card before adding the card to the vault. If the card verification fails, card is not added to the vault and no data key is returned.

NOTE: Card verification will only be performed for VISA and MasterCard. All other card types are not supported.

Vault Update Settings

This section will allow you to have the update information page locked for a specified number of minutes after a set number of sequential failed key attempts have been made. An email can also be sent when the page is locked.

NOTE: Click on the **Save Vault Update Settings** button to apply these chosen additional security features to the Hosted Vault configuration. If the security feature is not saved these fields will be returned to their last known saved configuration. Next, to continue with your Hosted Vault configuration setup, click the **Return to main configuration** button.

Number of attempts

This is the number of sequential failed attempts that the HVARU will allow before locking and preventing all future attempts for the number of minutes defined under Lock Period. For example, to lock the update functionality for 15 minutes after it has received 4 invalid data keys sequentially, please set the Number of Attempts to 4 and the Lock Period to 15.

Lock Period

This defines the number of minutes the update functionality will be locked. To lock the update functionality indefinitely set Lock Period to '999'.

Email Address

If the HVARU is locked, a notification email will be sent to this address if it is filled in. To receive an email after every invalid data key but to never lock the update feature, configure Number of Attempts to '1' and Lock Period to '0', and fill in Email Address.

NOTE:

DO NOT USE REAL ACCOUNT INFORMATION WHEN TESTING IN THE QA ENVIRONMENT.

Moneris GatewayQA is a shared environment and data sent to it may be accessible to others.

3 Developing Your Hosted Solution

3.1 Adding a new profile to Vault using the Hosted Vault

Following are a series of tables containing all the fields that can be sent in an HVARU request while adding a new profile to the Vault. The first table contains the required variables — these must be sent to properly register a profile. Subsequent tables contain variables that can be sent optionally. The appearance and functionality of the Hosted Vault Page is controlled by the Hosted Vault Configuration Tool located in the outlined above.

3.1.1 Required Variables - Adding New Profile to Vault

Table 1 Required Variables - Adding New Profile to Hosted Vault

	form	https://esqa.moneris.com/HPPDP/index.php - Development https://www3.moneris.com/HPPDP/index.php - Production
res_id	hidden	Provided by Moneris Solutions – Hosted Vault Configuration Tool
res_key	hidden	Provided by Moneris Solutions – Hosted Vault Configuration Tool
cc_crypt_type	hidden	Electronic Commerce Indicator (ECI) consists of 1 digit. Possible values are: 1 - Mail Order/Telephone Order - Single 2 - Mail Order/Telephone Order - Recurring

		3 - Mail Order/Telephone Order - Instalment 7 - Electronic Transaction with SSL

Table 2 Required Variables for Adding Vault Profile - ACH

Variable name	Type	Description
ach_sec	hidden	SEC code – possible values are : web – Internet Initiated Entry ccd – Cash Concentration or Disbursement ppd – Prearranged Payment and Deposit Your Moneris Gateway merchant account must be properly configured to accept each of the SEC code types that are used.

Below is a sample of the HVARU add account request using only the required variables.

Sample Add Profile to Vault - Required Variables

```
<FORM METHOD="POST" ACTION="https://esqa.moneris.com/HPPDP/index.php" >
<INPUT TYPE="HIDDEN" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="HIDDEN" NAME="res_key" VALUE="resTTJYGTDLNB">
<INPUT TYPE="HIDDEN" NAME="cc_crypt_type" VALUE="7">
<!--MORE OPTIONAL VARIABLES CAN BE DEFINED HERE -->
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
<FORM METHOD="POST" ACTION="https://esplusqa.moneris.com/DPHPP/index.php" >
<INPUT TYPE="HIDDEN" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="HIDDEN" NAME="res_key" VALUE="resTTJYGTDLNB">
<INPUT TYPE="HIDDEN" NAME="cc_crypt_type" VALUE="7">
<INPUT TYPE="HIDDEN" NAME="ach_sec" VALUE="web">
<INPUT TYPE="HIDDEN" NAME="pd_p_account_number" VALUE="1234567">
<INPUT TYPE="HIDDEN" NAME="pd_presentation_type" VALUE="W">
<!--MORE OPTIONAL VARIABLES CAN BE DEFINED HERE -->
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
```

3.1.2 Optional Variables - Adding a New Profile to Vault

Table 1 Optional Variables - Adding New Profile to Hosted Vault

Variable name	Type	Description
lang	hidden	This defines what language the Hosted Vault Page will be in: en-ca = English fr-ca = French If the tag is not included the Hosted Vault Page will default to English.
cust_id	50 alphanumeric	This is an ID field that can be used to identify the client, commonly used for student #s, policy #s, client name or invoice #s. Cannot be more than 50 characters. IT IS STRONGLY RECOMMENDED TO ALWAYS SEND A CUST_ID TO UNIQUELY IDENTIFY YOUR CLIENTS.
phone	20 alphanumeric	This is the cardholder's phone number
email	100 alphanumeric	This is where you would include the cardholder's email address should you wish to have an email receipt sent to them. Can not be more than 50 characters.
note	100 alphanumeric	This is any special instructions that you or the cardholder might like to store. Can not be more than 50 characters.

Table 2 Optional Variables - Adding New Profile to Vault - ACH Transactions

Variable name	Type	Description
ach_cust_first_name	50-character alphanumeric	Client's first name

Variable name	Type	Description
ach_cust_last_name	50-character alphanumeric	Client's last name
ach_cust_address1	50-character alphanumeric	Client's address
ach_cust_address2	50-character alphanumeric	Client's extra address information
ach_cust_city	50-character alphanumeric	Client's city
ach_cust_state	20-character alphanumeric	Client's state
ach_cust_zip	10-character alphanumeric	Client's ZIP code

NOTE: Request fields allow the following characters: a-z A-Z 0-9 _ - : . @ $ = /

The code below will set the optional fields. These are details that will identify the customer's profile.

Sample Add Profile to Vault - Optional Variables

```
<INPUT TYPE="HIDDEN" NAME="cust_id" VALUE="invoice: 123456-12-1">
<INPUT TYPE="HIDDEN" NAME="phone" VALUE ="416 555 1212">
<INPUT TYPE="TEXT" NAME="email" VALUE="john.smith@moneris.com">
<INPUT TYPE="TEXT" NAME="note" VALUE="All deliveries go to back door">
<INPUT TYPE="HIDDEN" NAME="lang" VALUE="fr-ca">
<INPUT TYPE="HIDDEN" NAME="cust_id" VALUE="invoice: 123456-12-1">
<INPUT TYPE="HIDDEN" NAME="phone" VALUE ="416 555 1212">
<INPUT TYPE="TEXT" NAME="email" VALUE="john.smith@moneris.com">
<INPUT TYPE="TEXT" NAME="note" VALUE="All deliveries go to back door">
```

3.1.3 Optional 'rvar' Variables

Things to Consider:

Things to Know:

- Where n is an alphanumeric value less than 10 characters long, unique to each rvar variable.
- The data sent in the rvar variables will NOT be stored in the Merchant Resource Center. These fields will be echoed backin the transaction response – in a GET or POST method.

- They may also be sent in the email receipt to the merchant if **Include 'rvar' in merchant email** is selected in the Email Receipt Configuration.

Table 1 Optional Variables - rvar

Variable name	Type	Description
rvarn	hidden	If these extra variables are sent in the request, they will be echoed back in the response (if GET or POST have been selected for the Response Method). Commonly used for session IDs. These variables must begin with “rvar” and then contain any alphanumeric string (i.e. rvar1, rvarname, rvarMyVariable).

The code below will send 3 rvar’s in the request so that they may be returned in the response or displayed on the merchant’s email receipt.

Sample Optional rvar request - Add Vault Profile

```
<INPUT TYPE="HIDDEN" NAME="rvar1" VALUE="TWO">
<INPUT TYPE="HIDDEN" NAME="rvar_monkey" VALUE="monkeys are funny">
<INPUT TYPE="HIDDEN" NAME="rvar_123" VALUE="abc">
```

3.2 Updating a Vault Profile Using the Hosted Vault

Below are a series of tables containing all the fields that can be sent in an HVARU request while updating an existing Vault profile. The first table contains the required variables – these must be sent to properly update the profile. Subsequent tables contain variables that can be sent optionally. The appearance and functionality of the Hosted Vault Page is controlled by the Hosted Vault Configuration Tool located in the Merchant Resource Center outlined above.

3.2.1 Required Variables - Updating Vault Profile

Table 1 Required Variables - Adding New Profile to Hosted Vault

Variable name	Type	Description
	form	Testing:https://esqa.-moneris.com/HPPDP/index.php

Variable name	Type	Description
		Production: https://www3.moneris.com/HPPDP/index.php
res_id	hidden	Provided by Moneris Solutions – Hosted Vault Configuration Tool
res_key	hidden	Provided by Moneris Solutions – Hosted Vault Configuration Tool
data_key	Hidden	Provided by Moneris Solutions in the response to a Vault Add Profile request. Identifies the unique Vault profile to be updated.
cc_crypt_type	hidden	Electronic Commerce Indicator (ECI) consists of 1 digit. Possible values are: 1 - Mail Order/Telephone Order - Single 2 - Mail Order/Telephone Order - Recurring 3 - Mail Order/Telephone Order - Instalment 7 - Electronic Transaction with SSL

Below is a sample of the HVARU update request using only the required variables.

Sample Add Profile to Vault - Required Variables

```
<FORM METHOD="POST" ACTION="https://esqa.moneris.com/HPPDP/index.php" >
<INPUT TYPE="HIDDEN" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="HIDDEN" NAME="res_key" VALUE="resTTJYGTDLNB">
<INPUT TYPE="HIDDEN" NAME="data_key" VALUE="123QWERTY123qwerty">
<INPUT TYPE="HIDDEN" NAME="cc_crypt_type" VALUE="7">
<!--MORE OPTIONAL VARIABLES CAN BE DEFINED HERE -->
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
<FORM METHOD="POST" ACTION="https://esplusqa.moneris.com/DPHPP/index.php" >
<INPUT TYPE="HIDDEN" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="HIDDEN" NAME="res_key" VALUE="resTTJYGTDLNB">
<INPUT TYPE="HIDDEN" NAME="data_key" VALUE="123QWERTY123qwerty">
<INPUT TYPE="HIDDEN" NAME="cc_crypt_type" VALUE="7">
<INPUT TYPE="HIDDEN" NAME="ach_sec" VALUE="web">
<INPUT TYPE="HIDDEN" NAME="pd_p_account_number" VALUE="1234567">
<INPUT TYPE="HIDDEN" NAME="pd_presentation_type" VALUE="w">
<!--MORE OPTIONAL VARIABLES CAN BE DEFINED HERE -->
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
```

NOTE: In the update transaction only the financial details (e.g. card number, expiry date) can be altered through the Hosted Vault Registration page. All other account details must be updated through an API.

3.2.2 Optional 'rvar' Variables - Updating Vault Profile

Things to Consider:

Things to Know:

- Where n is an alphanumeric value less than 10 characters long, unique to each rvar variable.
- The data sent in the rvar variables will NOT be stored in the Merchant Resource Center. These fields will be echoed backin the transaction response – in a GET or POST method.
- They may also be sent in the email receipt to the merchant if **Include 'rvar' in merchant email** is selected in the Email Receipt Configuration.

Table 1 Optional Variables - rvar

Variable name	Type	Description
rvarn	hidden	If these extra variables are sent in the request, they will be echoed back in the response (if GET or POST have been selected for the Response Method). Commonly used for session IDs. These variables must begin with “rvar” and then contain any alphanumeric string (i.e. rvar1, rvarname, rvarMyVariable).

Sample Update Vault Profile with rvar Variables

```
<INPUT TYPE="HIDDEN" NAME="rvar1" VALUE="TWO">
<INPUT TYPE="HIDDEN" NAME="rvar_monkey" VALUE="monkeys are funny">
<INPUT TYPE="HIDDEN" NAME="rvar_123" VALUE="abc">
```

3.3 Transaction Verification via Hosted Vault

- "Sending a Transaction Verification Request Via Hosted Vault" on the next page

3.3.1 Sending a Transaction Verification Request Via Hosted Vault

In order to perform a Transaction Verification it is essential that you configure the Hosted Vault configuration accordingly. If the Hosted Vault is properly configured you will receive a variable in a GET or POST response called “transactionKey”.

It is advised that you log the initial transaction response and then compare the Transaction Verification response to ensure authenticity. The transaction verification request should be performed using server to server communication rather than sending the request through the browser.

Transaction Verification can only be performed once on a given transaction, and it can only be performed within 15 minutes of the original transaction.

The transaction verification **must** be performed using a server to server request. The verification should not be sent through the browser.

Table 1 Variables for Transaction Verification - Hosted Vault

Variable name	Type	Description
	form	https://esqa.moneris.com/HPPDP/index.php - Development https://www3.moneris.com/HPPDP/index.php- Production
res_id	hidden	Provided by Moneris Solutions – Hosted Vault Configuration Tool
res_key	hidden	Provided by Moneris Solutions – Hosted Vault Configuration Tool
transactionKey	Hidden	This is returned in the transaction response.

Following is a sample of the Transaction Verification Request. This is just a sample for quick testing; the verification should be performed as a server to server request.

Sample Transaction Verification Request - Hosted Vault

```
<FORM NAME=VERIFY ACTION="https://esqa.moneris.com/HPPDP/verifyTxn.php">
<INPUT TYPE="HIDDEN" NAME="ps_store_id" VALUE="qampg">
<INPUT TYPE="HIDDEN" NAME="hpp_key" VALUE="hpPu7yr4Hn5k">
<INPUT TYPE="HIDDEN" NAME="transactionKey" VALUE="SDGJSGI4ujwrlsfGSGsjhlfhs5lsffs4h">
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to perform verification">
</FORM>
<FORM ACTION="https://esplusqa.moneris.com/DPHPP/index.php" method="POST">
<INPUT TYPE="hidden" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="hidden" NAME="res_key" VALUE="resTTJYGTDLNB">
<INPUT TYPE="hidden" NAME="verify_key" VALUE="SADF98AF78ADSFUASDF987">
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to perform verification">
</FORM>
```

Once Moneris Gateway receives the transaction verification request we match the key, then verify and log the request. A transaction verification response is then returned with the transaction information and a status. This response is created in the format defined in the "Security Features" portion of the Hosted Vault configuration. Please see the following table for a list of possible Transaction Verification statuses.

Table 2 Response Fields - Transaction Verification Request - Hosted Vault

Variable name	Type	Description
data_key	50-character alphanumeric	data_key of the original transaction
response_code	3-character alphanumeric	Transaction Response Code from the original transaction < 50: Transaction approved >= 50: Transaction declined NULL: Incomplete registration - Profile registration was not attempted
transactionKey	100-character alphanumeric	The transactionKey from the request
status	alphanumeric	This is the value to check to see if the transaction has been properly validated. Below is a list of possible replies and their meaning. Valid-Registered: The account add/update was successfully validated Invalid-Reconfirmed: The transactionKey provided has already been validated Invalid: Unable to validate request Invalid referrer URL - ??: Invalid referrer URL

Table 3 Error Codes - Transaction Verification

Code	Message/Description
991	Invalid referrer URL - <referrer url>: Referring URL does not match what is listed in the "Security Features" portion of the Hosted Vault configuration, validation failed. The source URL will be returned.
994	Invalid – Reconfirmed: The transaction has already been confirmed, validation failed.
995	Invalid: Not a valid confirmation request. Either the transaction doesn't exist or the request is older than 15 minutes, validation failed.

Below are samples of valid and invalid Transaction Verification Responses displayed on our server in XML format:

Sample Transaction Verification Response for Hosted Vault - Valid	Sample Transaction Verification Response for Hosted Vault - Invalid
<?xml version="1.0" standalone="yes"?> <response> <data_key>123QWER123QWER123</data_key> <response_code>1</response_code> <status>Valid - Registered</status> <transactionKey>SADF98AF78ADSFUASDF987</transactionKey> </response> <?xml version="1.0" standalone="yes"?> <response> <data_key>123QWER123QWER123</data_key> <response_code>1</response_code> <msg>Valid - Registered</msg > </response>	<?xml version="1.0" standalone="yes"?> <response> <response_code>995</response_code> <status>Invalid</status > <transactionKey>SADF98AF78ADSFUASDF987</transactionKey> </response> <?xml version="1.0" standalone="yes"?> <response> <response_code>995</response_code> <message>Invalid</message > </response>

4 Testing a Hosted Payment Solution

4.1 How Do I Test My Solution?

A testing environment is available for you to connect to while you are integrating your site to our payment gateway. The test environment is available 24/7; however since it is a development environment we cannot guarantee 100% availability. Also, please be aware that other merchants are using the testing environment so you may see transactions, user IDs, and Hosted Vault configurations that you did not create.

As a courtesy to others that are testing we ask that when you are processing refunds, changing passwords and/or trying other functions that you use only the transactions/users/configurations that you created.

Using the logins in Hosted Payment Page Configuration Tool , you can create your own Hosted Vault Configuration ID and Token. You can use these to send transactions to our test environment and configure your Hosted Vault. Your Configuration ID and Token will be valid for 30 days. You may test as often as required.

The test environment has been designed to replicate our production environment as closely as possible. One major difference is that we are unable to send test transactions onto the production authorization network and thus issuer responses are simulated. Additionally, the requirement to emulate approval, decline and error situations dictates that we use certain transaction variables to initiate various response and error situations.

The test environment will approve and decline transactions based on the penny value of the amount field.

> **EXAMPLE:** a transaction made for the amount of $9.00 or $1.00 will approve since the .00 penny value is set to approve in the test environment. Transactions in the test environment should not exceed $10.00. This limit does not exist in the production environment. For a list of all current test environment responses for various penny values, please see the Test Environment Penny Response table as well as the Test Environment eFraud Response table, available for download at https://developer.moneris.com

When testing you may use the following test credit card numbers with any future expiry date.

NOTE: These responses may change without notice. Moneris Solutions recommends you regularly refer to our website to check for possible changes.

Table 1 Test Card Numbers

Card Plan	Card Number
MasterCard	5454545454545454
Visa	4242424242424242 or 4005554444444403
Amex	373599005095005
Diners	36462462742008

Table 2 INTERAC® Online Payment Test Card Numbers

Card Plan	Card Number
INTERAC Online Track2	3728024906540591206=01121122334455000 5268051119993326=01121122334455000000 453781122255=011211223344550000000000

NOTE:

When testing INTERAC® Online Payment you will be forwarded to the INTERAC® Online Payment merchant testing tool. A screen will appear where certain fields need to be completed.

For an approved response you will need to enter the following data in to the fields, do not alter any of the other fields:

IDEBIT_TRACK2:3728024906540591206=01121122334455000

IDEBIT_ISSNAME:RBC

IDEBIT_ISSCONF:123456

For a declined response leave the fields blank.

Click **Post to Merchant**. Do **not** click **Validate Data** — it will return validation errors.

When testing ACH transactions you may use the following test bank account details:

Table 3 Test Account Details - ACH

Financial Institution	Routing Number	Account Number	Check Number
FEDERAL RESERVE BANK	011000015	Any number between 5-22 digits	Any number

Gift Card Test Card Numbers

For Gift Card test credentials please contact our Integration Support team at onlinepayments@moneris.com.

4.2 What Information Will I Get As a Response to My Transaction Request?

For each transaction you will receive a response message. The fields that will be included in the response are indicated in the table below.

The Receipt can be handled in two ways depending on how the "Response Method" has been configured.

1. Moneris Gateway can generate a receipt on your behalf and present it to the client. The receipt will be relatively generic in appearance and will be based on the settings from the Hosted Vault Configuration in the Merchant Resource Center. Please refer to What Do I Need to Include in the Receipt? to configure the receipt.
2. The receipt values will be sent back to the URL specified in the Hosted Vault Configuration settings from the Merchant Resource Center. You can then create a custom receipt or use it to initiate a secondary process. These values can be passed back appended to the URL in a query string format or as an HTTP POST.

4.2.1 Response Fields for Transaction Request

Table 1 Response Fields - Transaction Request

Variable name	Size/Type	Description
response_order_id	50-character alphanumeric	order_id specified in request or generated by Hosted Vault
response_code	3-character alphanumeric	Transaction Response Code

Variable name	Size/Type	Description
		< 50: Transaction approved >= 50: Transaction declined NULL: Transaction was not sent for authorization If you would like further details on the response codes that are returned please see the Response Codes document available for download at: https://developer.moneris.com
date_stamp	yyyy-mm-dd	Processing host date stamp
time_stamp	##:##:##	Processing host time stamp
bank_approval_code	8-character alphanumeric	Authorization code returned from the issuing institution
result	1-character numeric	1 = approved , 0 = declined, incomplete
trans_name	alphanumeric	Type of transaction that was performed purchase: cardholder was billed immediately preauth: funds were locked on the card – a capture will need to be performed to have the funds deposited into merchant's account (see Merchant Resource Centre User's Guide). A PreAuth transaction **must** be reversed if it is not to be captured. To reverse the full amount of the PreAuth, please use the Capture transaction with a dollar amount of "0.00". achdebit: bank account information is collected and funds are debited from this account cavv_purchase: similar to purchase but a VbV/MCSC authentication attempt was made. cavv_preauth: similar to preauth but a

Variable name	Size/Type	Description
		VbV/MCSC authentication attempt was made. idebit_purchase: similar to purchase but the transaction was performed using INTERAC® Online Payment
cardholder	40-character alphanumeric	Cardholder's name
charge_total	9-character decimal. Up to 7-character numeric + 2-character numeric after the decimal point **EXAMPLE:** 1234567.89	Amount of the transaction
card	2-character alphanumeric	Credit Card Type M = Mastercard V = Visa AX = American Express DC = Diners Card NO = Novus / Discover C = JCB SE = Sears P = INTERAC® Online Payment CQ = ACH (Online Check)
f4l4	####***#### ***####	First 4 and last 4 digits of the card # Last 4 digits of the bank account number (ACH/Online Check)
exp_month	2-character numeric	2 digit month (ex. 01, 02...). Will return expiry month entered on the Hosted Vault (Credit Card only)
exp_year	2-character numeric	2 digit year (ex. 01, 02...). Will return

Variable name	Size/Type	Description
		expiry year entered on the Hosted Vault (Credit Card only)
message	100-character alphanumeric	Response description returned from issuing institution or from Moneris Gateway if there is a system error.
CfStatus	2-character alphanumeric	Indicates the status of the merchant and convenience fee transactions. The CfStatus field provides details about the transaction behavior and should be referenced when contacting Moneris Customer Support. Possible values are: 1 or 1F = Completed 1st purchase transaction 2 or 2F = Completed 2nd purchase transaction 3 = Completed void transaction 4A or 4D = Completed refund transaction 7 or 7F = Completed merchant independent refund transaction 8 or 8F = Completed merchant refund transaction 9 or 9F = Completed 1st void transaction 10 or 10F = Completed 2nd void transaction 11A or 11D = Completed refund transaction
iso_code	2-character numeric	ISO response code
bank_transaction_id	18-character numeric	The reference number is an 18-character string that references the terminal used to process the transaction as well as the shift, batch and sequence number.

Variable name	Size/Type	Description
		This data is typically used to reference transactions on the host systems and must be displayed on any receipt presented to the customer. This information should be stored by the merchant. **EXAMPLE:** The following illustrates the breakdown of this field where "660123450010690030" is the reference number returned in the message, "66012345" is the terminal id, "001" is the shift number, "069" is the batch number and "003" is the transaction number within the batch.
transactionKey	100-character alphanumeric (optional)	This is an encrypted string that is returned when using the transaction verification feature. There is no need to decrypt the string. It needs to be passed back to Moneris Gateway to verify the authenticity of the transaction. **NOTE:** This variable applies only when using transaction verification functionality.
ticket	alphanumeric	The value returned from the preload data request. **NOTE:** This variable applies only when using data preload functionality.
rvarn	optional	These extra variables can be sent in the request and will be echoed back in the

<table>
<tr><th>Variable name</th><th>Size/Type</th><th>Description</th></tr>
<tr><td></td><td></td><td>response. These variables must begin with “rvar” and then contain any alpha-numeric string (i.e. rvar1, rvarname, rvarMyVariable). If they are not posted in the request, they will not be included in the response.</td></tr>
<tr><td>eci</td><td>1-character numeric</td><td>Electronic Commerce Indicator that was sent with the transaction.

Possible values are:

<table>
<tr><th>Crypt Type</th><th>TVisa/MCSC Definitions</th></tr>
<tr><td>5</td><td>- Fully authenticated

- There is a liability shift and the merchant is pro-tected from chargebacks.</td></tr>
<tr><td>6</td><td>- VbV/MCSC has been attempted

- VbV -There is a liability shift and the merchant is protected from chargebacks

-MCSV –No liability shift and the merchant is not protected from chargebacks.</td></tr>
<tr><td>7</td><td>- Non-VbV/MCSC trans-action

- Merchant is no longer protected from chargebacks</td></tr>
</table>
</td></tr>
<tr><td>txn_num</td><td>20-character alphanumeric</td><td>Gateway Transaction identifier. This value is required if merchant decides to send automated captures, voids or refunds through an API.</td></tr>
</table>

Variable name	Size/Type	Description
recur_result	true	Indicates the Recurring Billing result. true: The Recurring Billing transaction was successfully registered. Any response other than “true” indicates that the recurring billing transaction was not properly registered.
avs_response_code	1-character alphanumeric	Indicates the address verification result. Refer to Appendix A Transaction Request Examples for further details. To test AVS you must create a configuration in “store5” and use that configuration for testing.
cvd_response_code	1-character alphanumeric	Indicates the CVD validation result. Refer to Appendix A Transaction Request Examples for further details. To test CVD you must create a configuration in “store5” and use that configuration for testing.
cavv_result_code	1-character alphanumeric	The Cardholder Authentication Verification Value (CAVV) is a value that allows VisaNet to validate the integrity of the VbV transaction data. These values are passed back from the issuer to the merchant after the VbV/SecureCode authentication has taken place. **EXAMPLE** If the eci returned is a “6” and the result code is a "B", it becomes liable for chargeback. Please see CAVV Result Codes - Verified by Visa for the CAVV result codes table
is_visa_debit	boolean	A value of ‘true’ or ‘false’ is sent back which indicates if the card provided by the cardholder was a Visa Debit card.

Variable name	Size/Type	Description

Table 2 Response Fields - INTERAC® Online Payment

Variable name	Size/Type	Description
Trans_name	alphanumeric	Type of transaction that was performed idebit_purchase: similar to purchase but the transaction was performed using INTERAC® Online Payment
ISSNAME	1-30 characters alphanumeric	Returned for an INTERAC® Online Payment transaction. This field identifies the name of the card issuer. This data must be displayed on a receipt.
INVOICE	1-20 characters alphanumeric	Returned for an INTERAC® Online Payment transaction. This field contains the invoice number used to identify the transaction. This data must be displayed on the receipt.
ISSCONF	1-15-character alphanumeric	Returned for an INTERAC® Online Payment transaction. This field is the confirmation number returned by the issuing bank. This data must be displayed on the receipt.

Table 3 Response Fields - Gift Card Transactions

Variable name	Size/Type	Description
gift_charge_total	9-character numeric	This is the total amount of the Purchase transaction. This must contain 3 digits with two penny values. The minimum value passed can be 0.01 and the maximum 9999999.99

Variable name	Size/Type	Description
rem_balance	9-character numeric	This is the remaining balance on the card after Deactivation. The balance will be in pennies.
display_text	82-character alphanumeric	This is the remaining balance on the card after Deactivation. The balance will be in pennies.
receipt_text	122-character alphanumeric	This is a message that, if present, is to be printed on the receipt
voucher_text	255-character alphanumeric	If the VoucherType field is non-zero, the text from this field should be printed in the body of the voucher.
ref_num	10-character numeric	This is the unique number that was assigned by the Moneris system to identify the transaction. The maximum value of this parameter is 0xFFFFFFFF (4294967295). The host can not return reference numbers greater than this value. If this field is present, it is to be included on the receipt.
terminal_id	8-character numeric	Identifies the Terminal Identifier which was used to process the transaction.
txn_num	30-character alphanumeric	Gateway Transaction identifier. This value is required if merchant decides to send automated void/refund through an API.

NOTE: Multiple gift cards may be used to cover the full amount of the transaction. If two gift cards are submitted for processing, then there will be two sets of the above <gift_card> response fields within the response XML.

Table 4 Response Fields - Convenience Fee Transactions

Variable name	Size/Type	Description
convenience_fee	9-character decimal. Up to 7-character numeric + 2-character numeric after the decimal point **EXAMPLE:** 1234567.89	Charge the convenience fee amount. Please note the 'convenience_fee' must be less than the 'charge_total'.
cf_fee_rate	9-character decimal	The convenience fee rate that has been defined on the merchant's profile. For example: 1.00 – a fixed amount or 10.0 - a percentage amount
cf_fee_type	AMT / PCT	The type of convenience fee that has been defined on the merchant's profile. Available options are: AMT – fixed amount PCT – percentage
cf_success	true/false	Indicates whether the Convenience Fee transaction processed successfully.

Table 5 Response Fields - Transaction Risk Management Tool Transactions

Variable name	Size/Type	Description
risk_policy_score		The sum of all the risks weights from triggered rules within the selected policy in the range [-100…+100].
risk_request_result		success – ThreatMetrix was able to process the request successfully fail_access – ThreatMetrix was

Variable name	Size/Type	Description
		unable to process the request due to API verification failing fail_verification – API query limit reached fail_incomplete – ThreatMetrix was unable to process the request due to incomplete or incorrect input data fail_internal_error – ThreatMetrix encountered an error while processing the request fail_temporarily_unavailable – the request fail because the service is temporarily unavailable fail_invalid_email_address – the format of the supplied email address was invalid fail_invalid_telephone_number – the format of the supplied telephone number was invalid fail_invalid_device_id – the format of the supplied device_id was invalid fail_invalid_ip_address_parameter – the format of a supplied ip_address parameter was invalid
risk_reason_code		The codes of the rules verified from the selected policy that have triggered. Each rule code is returned as a separate name/value pair.
risk_reason_name		The names of rules verified from the selected policy that have triggered. Each rule name is returned as a separate name/value pair.
risk_reason_message_en		An English message description

Variable name	Size/Type	Description
		of the rule returned.
risk_reason_message_fr		A French message description of the rule returned.

Table 6 Response Fields - Loyalty Card Transactions

Variable name	Type	Description
request_amount	9-character decimal. Up to 7-character numeric + 2-character numeric after the decimal point **EXAMPLE:** 1234567.89	Identifies the amount for which loyalty points are to be awarded. This amount may be equal to or less than the total amount of the transaction.
transaction_points	9-character numeric	Amount processed on this loyalty card transaction. This value will be displayed in the number of points.
transaction_amount	9-character decimal. Up to 7-character numeric + 2-character numeric after the decimal point **EXAMPLE:** 1234567.89	Amount processed on this loyalty card transaction. This value will be displayed in the number of points.
current_balance	9-character numeric	This is the current balance for the card in points. If this field is present, it is to be printed on the receipt. If this field is not present, no balance information is to be printed on the receipt
lifetime_balance	9-character numeric	This is the lifetime balance for the card in points. If this field is present, it is to be printed on the receipt. If this field is not

Variable name	Type	Description
		present, no balance information is to be printed on the receipt.

Table 7 Response Fields - Hosted Vault Transactions

Variable name	Type	Description
data_key	max 50-character alpha-numeric	The unique key to identify the client. This is the ID that will be used for subsequent transactions for the account, such as an update.
payment_type	alphanumeric	This identifies what type of payment was registered. Possible values are:
res_success	4-character alphanumeric	True: Card registered False: Card failed registration Null: Incomplete registration

NOTE: To determine if a transaction is approved, the response_code will have a value of less than 50. If it is declined the response_code will be 50 or greater. A value of NULL means the transaction was incomplete.

4.2.2 Special Error Codes for Hosted Solutions

The Hosted Vault is designed to generate special error codes when certain data is incorrect and/or the transaction couldn't be processed. The table below contains the information regarding the error codes. Each error will be accompanied by a message describing the problem.

Table 1 Special Error Codes

Code	Message/Description
914	Transaction cancelled by cardholder – The response code indicates that the cardholder pressed the <cancel> transaction button – This response is only returned if the enhanced cancel button functionality is enabled within the Hosted Vault configuration.
991	Invalid referrer URL - <referrer url> – If the Hosted Vault solution is configured to check the referring URL and it is incorrect this error will occur. The source URL will be included in the error. Please refer to the "Security Features" portion of the Hosted Vault configuration for a list of all Allowed Referring URLs.
992	VbV / Secure Code authentication failed – This error will occur if your merchant account is configured for VbV/MCSC and the cardholder failed to enter the proper PIN during the authentication process.
993	Data error - unable to store data – This error will occur if too much request data was passed in the transaction request or if the database failed to store the request. This may occur if unsupported characters were included in one of the posted fields.
N/A	Invalid store credentials – There is no code generated and a blank page is loaded with the above information. The ps_store_id and/or hpp_key did not match an existing store.
N/A	Card Issuer returned corrupt data. Unable to proceed with the transaction. Please return to the site where you initiated the transaction and try again. Your card has not been charged. – There is no code generated and a blank page is loaded with the above information. This error will occur if the cardholder's issuing bank did not return the correct data in the VbV/MCSC authentication process.

Table 2 Error Codes - Convenience Fee Responses

Code	Message/Description
973	Unable to locate merchant CF details

Code	Message/Description
977	Invalid amount
978	Failed CF transaction
984	Data error: (optional: field name)
987	Invalid transaction
Null	Error: Malformed XML

4.3 Understanding the Fraud Prevention Tools

4.3.1 Address Verification Service (AVS)

The Address Verification Service (AVS) value refers to the cardholder's street number, street name and zip/postal code as it would appear on their statement. When participating in this security feature the Hosted Vault will prompt the cardholder for the AVS information.

4.3.2 Card Validation Digit (CVD)

The Card Validation Digit (CVD) value refers to the numbers appearing on the back of the credit card which are not imprinted on the front. The exception to this is with American Express card where this value is indeed printed on the front. When participating in this security feature the Hosted Vault will prompt the cardholder to enter CVD value.

4.3.3 Verified by Visa (VbV)

Verified by Visa (VbV) is a program offered by Visa. Before approving a transaction Moneris Gateway and the Bank that issues the credit cards will attempt to authenticate the cardholder through the use of a password, similar to a debit PIN. Merchants who have enrolled in these programs with Moneris will be able to offer their customers added protection against unauthorized credit card use, as well as protect themselves from fraud-related chargebacks.

If you have enrolled in Verified by Visa (VbV) with Moneris, the Hosted Vault will automatically attempt to perform the VbV authentications.

4.3.4 MasterCard SecureCode (MCSC)

MasterCard SecureCode (MCSC) is a new feature offered by MasterCard. Merchants who have enrolled in this program with Moneris and Moneris Gateway will be able to offer their customers added protection against unauthorized credit card use, as well as protect themselves from fraud-related chargebacks. Cardholders that have applied for SecureCode with their issuing bank will be able to use this password similar to a debit PIN number for online transactions with participating online merchants.

Before approving a transaction, Moneris Gateway and the Bank that issued the MasterCard will authenticate the cardholder through the use of this password. For merchants who have enrolled in

SecureCode, the Hosted Vaultsolution will automatically attempt to perform SecureCode verification on every MasterCard transaction.

4.3.5 Transaction Risk Management Tool

The Transaction Risk Management Tool provides additional information to assist in identifying fraudulent transactions. For merchants who have enrolled in the Transaction Risk Management Tool, the Hosted Paypage can be configured to obtain a risk assessment for every transaction and return the results along with the transaction response information.

4.3.6 How Do I Handle the eFraud Response Information?

When reviewing the response information and determining how to handle the transaction, it is recommended that you (either manually or through automated logic on your site) use the following pieces of information:

1. The risk score
2. The rules triggered (e.g. Rule Codes, Rule Names, Rule Messages) Results obtained from Verified by Visa, MasterCard Secure Code, AVS, CVD and the financial transaction authorization
3. Automated processes will also need to include the response codes for the Transaction Risk Management Transaction

4.3.6.1 Card Validation Digits (CVD) and Address Verification Service (AVS)

Card Validation Digits (CVD)

The Card Validation Digits (CVD) value refers to the numbers appearing on the **back** of the credit card. The exception to this is with American Express cards where this value is printed on the front

Address Verification Service (AVS)

The Address Verification Service (AVS) value refers to the cardholder's street number, street name and zip/postal code as it would appear on their statement.

Additional Information for CVD and AVS

The responses that are received from CVD and AVS verifications are intended to provide added security and fraud prevention, but the response itself will not affect the issuer's approval of a transaction. Upon receiving a response, the choice to proceed with a transaction is left entirely to the merchant.

Please note that all responses coming back from these verification methods are not direct indicators of whether a merchant should complete any particular transaction. The responses should not be used as a strict guideline of which transaction will approve or decline.

NOTE:

CVD verification is only applicable towards Visa, MasterCard and American Express transactions.

Also, please note that AVS verification is only applicable towards Visa, MasterCard, Discover and American Express transactions. This verification method is not applicable towards any other card type.

*For additional information on how to handle these responses, please refer to the eFraud (CVD & AVS) Result Codes document which is available at https://developer.moneris.com

Below is a sample of the AVS and CVD response displayed on our server in XML format.

Sample AVS and CVD Response - Valid

```
<?xml version="1.0" standalone="yes"?>
<response>
      <order_id>mhp2250927670</order_id>
<response_code>27</response_code>
<amount>10.10</amount>
<txn_num>135172-0_77</txn_num>
<avs_response_code>A</avs_response_code>
<cvd_response_code>M</avs_response_code>
</response>
```

4.3.6.2 CAVV and Crypt Types

The Cardholder Authentication Verification Value (CAVV) is a value that allows validation of the integrity of Verified by Visa (VbV), MasterCard SecureCode (MCSC) and American Express SafeKeyVerified by Visa (VbV) and MasterCard SecureCode (MCSC) authentication data. This value is passed from the Issuer to the merchant after the authentication has taken place. The Hosted Vault then integrates the CAVV value into the financial authorization request to the Issuer.

The crypt type is derived by Moneris Gateway using the CAVV returned during authentication using VbV, MCSC or SafeKeyVbV or MCSC. Below are the possible values returned.

Crypt Type	Visa, MasterCard and AmericanExpress Definition
5	- Fully authenticated - There is a liability shift and the merchant is protected from chargebacks
6	- VbV/MCSC/SafeKey has been attempted - There is a liability shift and the Merchant is protected from chargebacks of certain types
7	- Non-VbV/MCSC/SafeKey transaction - No liability shift - Merchant is no longer protected from chargebacks

CAVV Result Codes - Verified by Visa

> **NOTE:** This information applies to Verified by Visa transactions only. It does not apply to MCSC or SafeKey transactions.

The Cardholder Authentication Verification Value (CAVV) is a value that allows VisaNet to validate the integrity of the VbV authentication data. This value is passed from the Issuer to the merchant after the VbV authentication has taken place. The Hosted Vault then integrates the CAVV value into the financial authorization request to the Issuer.

Once the VbV authentication is completed and the financial authorization transaction (Purchase or Auth) has been authorized, the CAVV Result Code value may be returned in the financial transaction response to provide the merchant with additional details pertaining to the integrity of the VbV validation.

The following table describes the content of the CAVV Result Code response data and what it means to the merchant.

Table 1 CAVV Result Codes

Result Code	Message	What this means to you as a merchant…
0	CAVV authentication results invalid.	For this transaction you may not receive protection from chargebacks as a result of using VbV as the CAVV was considered invalid at the time the financial transaction was processed. Please check that you are following the VbV process correctly and passing the correct data in our transactions.
1	CAVV failed validation; authentication	Provided that you have implemented the VbV process correctly the liability for this transaction should remain with the Issuer for chargeback reason codes covered by Verified by Visa.
2	CAVV passed validation; authentication	The CAVV was confirmed as part of the financial transaction. This transaction is a fully authenticated VbV transaction (ECI 5)
3	CAVV passed validation; attempt	The CAVV was confirmed as part of the financial transaction. This transaction is an attempted VbV transaction (ECI 6)
4	CAVV failed validation; attempt	Provided that you have implemented the VbV process correctly the liability for this transaction should remain with the Issuer for chargeback reason codes covered by Verified by Visa.

Result Code	Message	What this means to you as a merchant…
7	CAVV failed validation; attempt (US issued cards only)	Please check that you are following the VbV process correctly and passing the correct data in our transactions. Provided that you have implemented the VbV process correctly the liability for this transaction should be the same as an attempted transaction (ECI 6)
8	CAVV passed validation; attempt (US issued cards only	The CAVV was confirmed as part of the financial transaction. This transaction is an attempted VbV transaction (ECI 6)
9	CAVV failed validation; attempt (US issued cards only)	Please check that you are following the VbV process correctly and passing the correct data in our transactions. Provided that you have implemented the VbV process correctly the liability for this transaction should be the same as an attempted transaction (ECI 6)
A	CAVV passed validation; attempt (US issued cards only)	The CAVV was confirmed as part of the financial transaction. This transaction is an attempted VbV transaction (ECI 6)
B	CAVV passed validation	The CAVV was confirmed as part of the financial transaction. However, this transaction doesn't qualify for the liability shift. Treat this transaction the same as an ECI 7.

4.3.6.3 Transaction Risk Management Tool Responses

The responses that are received from CVD and AVS verifications are intended to provide added security and fraud prevention, but the response itself will not affect the completion of a transaction. Upon receiving a response, the choice to proceed with a transaction is left entirely to the merchant.

The responses that are received from the Transaction Risk Management Tool are intended to provide added security and fraud prevention, but the response itself will not affect the completion of a transaction. Upon receiving a response, the choice to proceed with a transaction is left entirely to the merchant.

Below is a sample of the Transaction Risk Management Tool response displayed on our server in XML format.

Sample Transaction Risk Management Tool Response - XML

```
<?xml version="1.0" standalone="yes"?>
<response>
      <order_id>mhp2250927670</order_id>
<response_code>27</response_code>
<amount>5.00</amount>
<txn_num>135172-0_77</txn_num>
      <risk_policy_score>-15</risk_policy_score>
<risk_request_result>success</risk_request_result>
<risk_reason_code>UN001,UN001</risk_reason_code>
<risk_reason_name> 3DevciePerAccountNumberWeek,3DevciePerCreditCardWeek</risk_reason_name>
<risk_reason_message_en> Unknown Rule,Unknown Rule</risk_reason_message_en>
<risk_reason_message_fr> Regle Inconnus,Regle Inconnus<risk_reason_message_fr>
</response>
```

Understanding the Risk Score

For each transaction through the Hosted Vault with the Transaction Risk Management Tool configured, a score with a value between -100 and +100 will be returned based on the rules that were triggered for the transaction. Below is a table defining the different possible risk scores ranges.

Table 1 Risk Score Definitions

Risk Score	Visa Definition
[-100 … -1]	The lowest score that can be reached is -100. The more negative the number (ie closer to -100) the more likely the transaction is fraudulent.
0	A risk score of 0 indicates a neutral transaction

Risk Score	Visa Definition
[1 … +100]	The highest score that can be reached is +100. The more positive the number (ie closer to +100) the lower the risk that the transaction is fraudulent. **NOTE:** All e-commerce transactions have some level of risk associated with them and as a result it is rare to see transactions with a risk score in the high positive values.

When evaluating the risk of a transaction, the risk score will give you an initial indicator of the potential risk level that the transaction is or isn't fraudulent. The more negative the score, the higher the probability is that the transaction is fraudulent. Since some of the rules that are evaluated on each transaction may/may not be as relevant in your business scenario, you should also review the rules that were triggered for the transaction before determining how to handle the transaction.

Understanding the Rule Codes, Rule Names and Rule Messages

The rule codes, rule names and rule messages provide details on what rules were trigged during the assessment of the information provided in Transaction Risk Management Tool. Each Rule Code has a Rule Name and Message. The Rule Name and Rule Message will typically be very similar to the table inTransaction Risk Management Tool Rules & Codes

When evaluating the risk of a transaction, it is recommended that you review the rules that were triggered for the transaction and assess the relevancy of it to your business (e.g. how it relates to the typical buying habits of your customer base).

If you are automating some or all of the decision making process related to handling the responses, you may want to use the Rule Codes. If you are documenting manual processes you may want to refer to the more user friendly Rule Name and/or Rule Message.

Transaction Risk Management Tool Rules & Codes

The following is a list of all possible responses of Rule Names once a Query has been performed.

Table 1 Rule Number and Rule Description

Rule Name	Rule Number	Message/Description	Rule Explanation
White lists			
DeviceWhitelisted	WL001	Device White Listed	Device is on the white list. This indicates that the device has been flagged as always "ok". NOTE: This rule is currently not in use.
IPWhitelisted	WL002	IP White Listed	IP Address is on the white list. This indicates the device has been flagged as always "ok". NOTE: This rule is currently not in use.
EmailWhitelisted	WL003	Email White Listed	Email address is on the white list. This indicates that the device has been flagged as always "ok". NOTE: This rule is currently not in use.
Event Velocity			
2DevicePayment	EV003	2 Device Payment Velocity	Multiple payments were detected from this device in the past 24 hours.
2IPPaymentVelocity	EV006	2 IP Payment Velocity	Multiple payments were detected from this IP within the past 24 hours.
2ProxyPaymentVelocity	EV008	2 Proxy Payment Velocity	The device has used 3 or more different proxies during a 24 hour period. This could be a risk or it could be someone using a legitimate corporate proxy.

Rule Name	Rule Number	Message/Description	Rule Explanation
Email			
3EmailPerDeviceDay	EM001	3 Emails for the Device ID in 1 Day	This device has presented 3 different email ids within the past 24 hours.
3EmailPerDeviceWeek	EM002	3 emails for the Device ID in 1 week	This device has presented 3 different email ids within the past week.
3DevciePerEmailDay	EM003	3 Device Ids for email address in 1 day	This email has been presented from three different devices in the past 24 hours.
3DevciePerEmailWeek	EM004	3 Device Ids for email address in 1 week	This email has been presented from three different devices in the past week.
EmailDistanceTravelled	EM005	Email Distance Travelled	This email address has been associated with different physical locations in a short period of time.
3EmailPerSmartIDHour	EM006	3 Emails for SmartID in 1 Hour	The SmartID for this device has been associated with 3 different email addresses in 1 hour.
GlobalEMailOverOneMonth	EM007	Global Email over 1 month	The e-mail address involved in the transaction over 30 days ago. This generally indicates that the transaction is less risky. Note: This rule is currently set currently set so it does not impact the policy score or risk rating.
ComputerGeneratedEmailAddress	EM008	Computer Generated Email Address	This transaction used a computer generated email address.

Rule Name	Rule Number	Message/Description	Rule Explanation
Account Number			
3AccountNumberPerDeviceDay	AN001	3 Account Numbers for device in 1 day	This device has presented 3 different user accounts within the past 24 hours.
3AccountNumberPerDeviceWeek	AN002	3 Account Numbers for device in 1 week	This device has presented 3 different user accounts within the past week.
3DevciePerAccountNumberDay	AN003	3 Device IDs for account number in 1 day	This user account been used from three different devices in the past 24 hours.
3DevciePerAccountNumberWeek	AN004	3 Device IDs for account number in 1 week	This card number has been used from three different devices in the past week.
AccountNumberDistanceTravelled	AN005	Account Number distance travelled	This card number has been used from a number of physically different locations in a short period of time.
Credit Card / Payments			
3CreditCardPerDeviceDay	CP001	3 credit cards for device in 1 day	This device has used three credit cards within 24 hours.
3CreditCardPerDeviceWeek	CP002	3 credit cards for device in 1 week	This device has used three credit cards within 1 week.
3DevicePerCreditCardDay	CP003	3 device ids for credit card in 1 day	This credit card has been used on three different devices in 24 hours.
3DevciePerCreditCardWeek	CP004	3 device ids for credit card in 1 week	This credit card has been used on three different devices in 1 week.

Rule Name	Rule Number	Message/Description	Rule Explanation
CredtCardDistanceTravelled	CP005	Credit Card has travelled	The credit card has been used at a number of physically different locations in a short period of time.
CreditCardShipAddressGeoMismatch	CP006	Credit Card and Ship Address do not match	The credit card was issued in a region different from the Ship To Address information provided.
CreditCardBillAddressGeoMismatch	CP007	Credit Card and Billing Address do not match	The credit card was issued in a region different from the Billing Address information provided.
CreditCardDeviceGeoMismatch	CP008	Credit Card and device location do not match	The device is located in a region different from where the card was issued.
CreditCardBINShipAddressGeoMismatch	CP009	Credit Card issuing location and Shipping address do not match	The credit card was issued in a region different from the Ship To Address information provided.
CreditCardBINBillAddressGeoMismatch	CP010	Credit Card issuing location and Billing address do not match	The credit card was issued in a region different from the Billing Address information provided.
CreditCardBINDeviceGeoMismatch	CP011	Credit Card issuing location and location of the device do not match	The device is located in a region different from where the card was issued.
TransactionValueDay	CP012	Daily Transaction Value Threshold	The transaction value exceeds the daily threshold.
TransactionValueWeek	CP013	Weekly Transaction Value Threshold	The transaction value exceeds the weekly threshold.
Proxy Rules			

Rule Name	Rule Number	Message/Description	Rule Explanation
3ProxyPerDeviceDay	PX001	3 Proxy Ips in 1 day	This device has used three different proxy servers in the past 24 hours.
AnonymousProxy	PX002	Anonymous Proxy IP	This device is using an anonymous proxy
UnusualProxyAttributes	PX003	Unusual Proxy Attributes	This transaction is coming from a source with unusual proxy attributes.
AnonymousProxy	PX004	Anonymous Proxy	This device is connecting through an anonymous proxy connection.
HiddenProxy	PX005	Hidden Proxy	This device is connecting via a hidden proxy server.
OpenProxy	PX006	Open Proxy	This transaction is coming from a source that is using an open proxy.
TransparentProxy	PX007	Transparent Proxy	This transaction is coming from a source that is using a transparent proxy.
DeviceProxyGeoMismatch	PX008	Proxy and True GEO Match	This device is connecting through a proxy server that didn’t match the devices geolocation.
ProxyTrueISPMismatch	PX009	Proxy and True ISP Match	This device is connecting through a proxy server that doesn’t match the true IP address of the device.
ProxyTrueOrganizationMismatch	PX010	Proxy and True Org Match	The Proxy information and True ISP information for this source do not match.

Rule Name	Rule Number	Message/Description	Rule Explanation
DeviceProxyRegionMismatch	PX011	Proxy and True Region Match	The proxy and device region location information do not match.
ProxyNegativeReputation	PX012	Proxy IP Flagged Risky in Reputation Network	This device is connecting from a proxy server with a known negative reputation.
SatelliteProxyISP	PX013	Satellite Proxy	This transaction is coming from a source that is using a satellite proxy.
GEO			
DeviceCountriesNotAllowed	GE001	True GEO in Countries Not Allowed blacklist	This device is connecting from a high-risk geographic location.
DeviceCountriesNotAllowed	GE002	True GEO in Countries Not Allowed (negative whitelist)	The device is from a region that is not on the whitelist of regions that are accepted.
DeviceProxyGeoMismatch	GE003	True GEO different from Proxy GEO	The true geographical location of this device is different from the proxy geographical location.
DeviceAccountGeoMismatch	GE004	Account Address different from True GEO	This device has presented an account billing address that doesn't match the devices geolocation.
DeviceShipGeoMismatch	GE005	Device and Ship Geo mismatch	The location of the device and the shipping address do not match.
DeviceShipGeoMismatch	GE006	Device and Ship Geo mismatch	The location of the device and the shipping address do not match.
Device			

Rule Name	Rule Number	Message/Description	Rule Explanation
SatelliteISP	DV001	Satellite ISP	This transaction is from a source that is using a satellite ISP.
MidsessionChange	DV002	Session Changed Mid-session	This device changed session details and identifiers in the middle of a session.
LanguageMismatch	DV003	Language Mismatch	The language of the user does not match the primary language spoken in the location where the True IP is registered.
NoDeviceID	DV004	No Device ID	No device ID was available for this transaction.
Dial-upConnection	DV005	Dial-up connection	This device uses a less identifiable dial-up connection.
DeviceNegativeReputation	DV006	Device Blacklisted in Reputational Network	This device has a known negative reputation as reported to the fraud network.
DeviceGlobalBlacklist	DV007	Device on the Global Black List	This device has been flagged on the global blacklist of known problem devices.
DeviceCompromisedDay	DV008	Device compromised in last day	This device has been reported as compromised in the last 24 hours.
DeviceCompromisedHour	DV009	Device compromised in last hour	This device has been reported as compromised in the last hour.
FlashImagesCookiesDisabled	DV010	Flash Images Cookies Disabled	Key browser functions/identifiers have been disabled on this device.

Rule Name	Rule Number	Message/Description	Rule Explanation
FlashCookiesDisabled	DV011	Flash Cookies Disabled	Key browser functions/identifiers have been disabled on this device.
FlashDisabled	DV012	Flash Disabled	Key browser functions/identifiers have been disabled on this device.
ImagesDisabled	DV013	Images Disabled	Key browser functions/identifiers have been disabled on this device.
CookiesDisabled	DV014	Cookies Disabled	Key browser functions/identifiers have been disabled on this device.
DeviceDistanceTravelled	DV015	Device Distance Travelled	The device has been used from multiple physical locations in a short period of time.
PossibleCookieWiping	DV016	Cookie Wiping	This device appears to be deleting cookies after each session.
PossibleCookieCopying	DV017	Possible Cookie Copying	This device appears to be copying cookies.
PossibleVPNConnection	DV018	Possibly using a VPN Connection	This device may be using a VPN connection

Pulling All the Information Together to Make a Decision

Depending on your business policies and processes, you will use the information obtained from the Fraud Tools (e.g. AVS, CVD, VbV/SecureCode and Transaction Risk Management) to make an informed decision on whether you want to accept the transaction or consider it to be a potential fraudulent transaction that you do not want to continue to process.

If you do not want to continue with a transaction because it appears too risky and is likely fraudulent, you will need to:

- Let the customer know that you will not be proceeding with their order.
- Cancel the financial transaction if you have received an approved authorization. To do this you will need to send a Void/Refund for a purchase transaction or a $0.00 Capture transaction if the original transaction was a pre-authorization.

4.4 What Do I Need to Include in the Receipt?

Visa and MasterCard expect certain variables be returned to the cardholder and presented as a receipt when a transaction is approved. If the Hosted Vault is configured to return the response to your web-server it is imperative that you display the information listed below. These required fields are listed below and includes the corresponding variable name as returned by the Hosted Vault or a proper description in brackets.

1. Amount - (charge_total)
2. Transaction Type - (trans_name)
3. Convenience Fee Amount – (convenience_fee – required only for Convenience Fee)
4. Date and Time - (date_stamp & time_stamp)
5. Authorisation Code - (bank_approval_code)
6. ResponseCode - (response_code)
7. ISO Code - (iso_code)
8. Response Message - (message)
9. Reference Number - (bank_transaction_id)
10. Goods and Services Order - (description of the products / services ordered)
11. Merchant Name - (Your Business Name – should be same as what you registered with Moneris Solutions)
12. Merchant URL - (Your business website)
13. Cardholder Name - (cardholder)
14. Return Policy (only a requirement for e-commerce transactions)

The following are required for INTERAC® Online Payment **only**:

1. Issuer Name (ISSNAME)
2. Issuer Confirmation (ISSCONF)
3. Invoice Number (INVOICE)

5 Moving to Production

Once you have completed the necessary steps of creating a profile for your solution, configuring the solution profile, developing and testing the solution, you are ready to move your solution into production.

5.1 How Do I Activate My Store?

Once you have received your activation letter/fax go to https://www3.moneris.com/connect/en/activate/index.php https://esplus.moneris.com/usmpg/activate as instructed in the letter/fax. You will need to input your store ID and merchant ID then click on **Activate**. Once this is confirmed you will need to create an administrator account that you will use to log into the Merchant Resource Center to access and administer your Moneris Gateway store.

> **NOTE:** The API TOKEN that you receive during Activation is NOT the token that you require for the Hosted Vault request.

5.2 How Do I Configure My Store for Production?

Once you have activated your store, the next step is to point your store to the production host.

To point your store to the production host:

1. In your HTML FORM POST, change the <FORM METHOD="POST" ACTION=https://esqa.moneris.com/HPPDP/index.php> to contain the production URL: <FORM METHOD="POST" ACTION=https://www3.moneris.com/HPPDP/index.php>.
2. Change the ps_store_id and hpp_key to reflect your production store configuration.

Once you are in production you will access the Merchant Resource Center at https://www3.moneris.com/mpg. You can use the store administrator ID you created during the activation process and then create additional users as needed.

For INTERAC® Online Payment Solution:

Third-party Service/Shopping-cart Provider

In your product documentation, please ensure that the clients are properly instructed to create the Production HPP configuration as outlined above. They should also be instructed to provide Moneris Solutions with screen-shots of their check-out process showing examples of approved and declined transactions using the INTERAC® Online Payment service and provide the completed Merchant Checklist of Appendix B. Detailed descriptions of the requirements for the checklist can be found in the INTERAC

Online Merchant Guidelines document. Once completed, they can be faxed or emailed to the Moneris Gateway Integration Support group for review.

When you are ready to move into production please contact the Integration Support Team at eproducts@moneris.com.

Appendix A Transaction Request Examples

Transaction Requests

The example below will send both shipping and billing address information as well as item information, and initiate a recurring charge.

```
<FORM ACTION="https://esqa.moneris.com/HPPDP/index.php" method=post>
<!-- Store Settings-->
<INPUT TYPE="HIDDEN" NAME="ps_store_id" VALUE="qampg">
<INPUT TYPE="HIDDEN" NAME="hpp_key" VALUE="hpPu7yr4Hn5k">
<!------- DEFINE CHARGE TOTAL HERE --->
Amount:<INPUT TYPE="text" NAME="charge_total" VALUE="300.00"><br><br>
<!-- Unique Order ID -->
<INPUT TYPE="hidden" NAME="order_id" VALUE="hpp_mr_test_1">

<!-- Additional Optional Details -->
<input type="hidden" name="cust_id" value="customer num">
<input type="hidden" name="email" value="">
<input type="hidden" name="note" value="these are special instructions">
<!-- Item Information -->
<input type="hidden" name="quantity1" value="3">
<input type="hidden" name="description1" value="qunat 3">
<input type="hidden" name="id1" value="sku123">
<input type="hidden" name="price1" value="4.00">
<input type="hidden" name="subtotal1" value="12.00">
<input type="hidden" name="quantity2" value="2">
<input type="hidden" name="description2" value="qunat 2">
<input type="hidden" name="id2" value="2sku123">
<input type="hidden" name="price2" value="24.00">
<input type="hidden" name="subtotal2" value="212.00">
<input type="hidden" name="gst" value="3.03">
<input type="hidden" name="shipping_cost" value="4.03">
<!-- rvar Information -->
<input type="hidden" name="rvar1" value="1_rvar">
<input type="hidden" name="rvar2" value="2_rvar">
<input type="hidden" name="rvar3" value="3_rvar">
<input type="hidden" name="rvar4" value="4_rvar">
<!-- Shipping information -->
<input type="hidden" name="ship_first_name" value="sfn">
<input type="hidden" name="ship_last_name" value="sln">
<input type="hidden" name="ship_company_name" value="scn">
<input type="hidden" name="ship_address_one" value="sao">
<input type="hidden" name="ship_city" value="sc">
<input type="hidden" name="ship_state_or_province" value="ssop">
<input type="hidden" name="ship_postal_code" value="spc">
<input type="hidden" name="ship_country" value="scount">
<input type="hidden" name="ship_phone" value="sp">
<input type="hidden" name="ship_fax" value="sf">
<!-- Billing Information -->
<input type="hidden" name="bill_first_name" value="bfn">
<input type="hidden" name="bill_last_name" value="bln">
<input type="hidden" name="bill_company_name" value="bcn">
<input type="hidden" name="bill_address_one" value="bao">
<input type="hidden" name="bill_city" value="bc">
<input type="hidden" name="bill_state_or_province" value="bsop">
<input type="hidden" name="bill_postal_code" value="bpc">
<input type="hidden" name="bill_country" value="bcount">
<input type="hidden" name="bill_phone" value="bp">
<input type="hidden" name="bill_fax" value="bf">
```

```
<!-- Recurring Information -->
<input type="hidden" name="doRecur" value ="1">
<input type="hidden" name="recurUnit" value ="day">
<input type="hidden" name="recurStartDate" value="2006/06/01">
<input type="hidden" name="recurNum" value="99">
<input type="hidden" name="recurStartNow" value="true">
<input type="hidden" name="recurPeriod" value="4">
<input type="hidden" name="recurAmount" value="4.00">
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
<FORM ACTION="https://esplusqa.moneris.com/DPHPP/index.php" METHOD="POST">
<!-- Mandatory Fields -->
<INPUT TYPE="hidden" NAME="hpp_id" VALUE="QRZX9qa002">
<INPUT TYPE="hidden" NAME="hpp_key" VALUE="hpTTJYGTDLNB">
<INPUT TYPE="hidden" NAME="amount" VALUE="9.00">
<!-- Unique Order ID -->
<INPUT TYPE="hidden" NAME="order_no" VALUE="hpp_mr_test_1">
<!-- Additional Optional Details -->
<INPUT TYPE="hidden" NAME="client_email" VALUE="john.smith@moneris.com">
<INPUT TYPE="hidden" NAME="note" VALUE="This is a note.">
<INPUT TYPE="hidden" NAME="cust_id" VALUE="Some Customer Number">

<!-- rvar Information -->
<INPUT TYPE="hidden" NAME="rvar_1" VALUE="1">
<INPUT TYPE="hidden" NAME="rvar_monkey" VALUE="monkeys are funny">
<INPUT TYPE="hidden" NAME="rvar_123abc" VALUE="123abc">
<!-- Item Information-->
<INPUT TYPE="hidden" NAME="li_quantity1" VALUE="1">
<INPUT TYPE="hidden" NAME="li_description1" VALUE="Blue Suede Shoes">
<INPUT TYPE="hidden" NAME="li_id1" VALUE="1sku123">
<INPUT TYPE="hidden" NAME="li_price1" VALUE="2.00">
<INPUT TYPE="hidden" NAME="li_quantity2" VALUE="2">
<INPUT TYPE="hidden" NAME="li_description2" VALUE="Red Mary-Janes">
<INPUT TYPE="hidden" NAME="li_id2" VALUE="2sku123">
<INPUT TYPE="hidden" NAME="li_price2" VALUE="1.00">
<INPUT TYPE="hidden" NAME="li_shipping" VALUE="4.00">
<INPUT TYPE="hidden" NAME="li_taxes" VALUE="1.00">
<!-- Billing Information -->
<INPUT TYPE="hidden" NAME="od_bill_firstname" VALUE="John">
<INPUT TYPE="hidden" NAME="od_bill_lastname" VALUE="Smith">
<INPUT TYPE="hidden" NAME="od_bill_company" VALUE="Moneris">
<INPUT TYPE="hidden" NAME="od_bill_address" VALUE="101 Main St">
<INPUT TYPE="hidden" NAME="od_bill_city" VALUE="Springfield">
<INPUT TYPE="hidden" NAME="od_bill_state" VALUE="IL">
<INPUT TYPE="hidden" NAME="od_bill_zipcode" VALUE="123456">
<INPUT TYPE="hidden" NAME="od_bill_country" VALUE="USA">
<INPUT TYPE="hidden" NAME="od_bill_phone" VALUE="555-555-5555">
<INPUT TYPE="hidden" NAME="od_bill_fax" VALUE="555-555-5566">
<!-- Shipping information -->
<INPUT TYPE="hidden" NAME="od_ship_firstname" VALUE="Mary">
<INPUT TYPE="hidden" NAME="od_ship_lastname" VALUE="Smith">
<INPUT TYPE="hidden" NAME="od_ship_company" VALUE="Moneris">
<INPUT TYPE="hidden" NAME="od_ship_address" VALUE="222 Lakeshore Blvd">
<INPUT TYPE="hidden" NAME="od_ship_city" VALUE="New York">
<INPUT TYPE="hidden" NAME="od_ship_state" VALUE="NY">
<INPUT TYPE="hidden" NAME="od_ship_zipcode" VALUE="234567">
<INPUT TYPE="hidden" NAME="od_ship_country" VALUE="USA">
<INPUT TYPE="hidden" NAME="od_ship_phone" VALUE="666-555-6666">
<INPUT TYPE="hidden" NAME="od_ship_fax" VALUE="666-555-6655">
<!-- Recurring Information -->
<INPUT TYPE="hidden" NAME="recur_initiate" VALUE="1">
<INPUT TYPE="hidden" NAME="recur_unit" VALUE="week">
<INPUT TYPE="hidden" NAME="recur_period" VALUE="1">
<INPUT TYPE="hidden" NAME="recur_num" VALUE="4">
<INPUT TYPE="hidden" NAME="recur_start_now" VALUE="true">
<INPUT TYPE="hidden" NAME="recur_amount" VALUE="3.00">
```

```
<INPUT TYPE="hidden" NAME="recur_start_date" VALUE="2006/12/01">
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
```

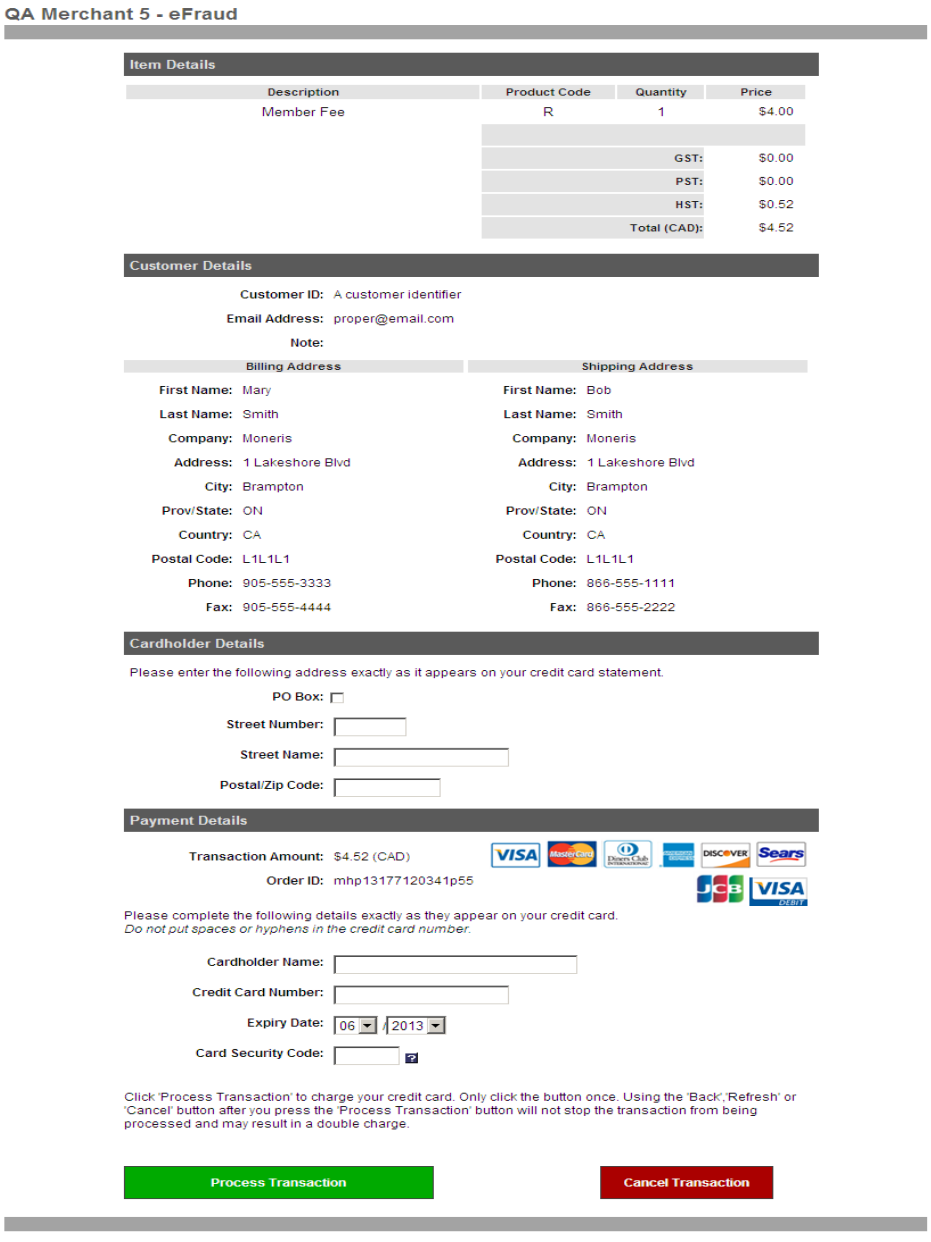
Hosted Vault Transaction Request

```
<FORM ACTION="https://esqa.moneris.com/HPPDP/index.php" METHOD="POST">
<!-- Mandatory Fields -->
<INPUT TYPE="hidden" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="hidden" NAME="res_key" VALUE="reTTJYGTDLNB">
<!-- Mandatory for update ONLY, not used in this example -->
<!-- <INPUT TYPE="hidden" NAME="data_key" VALUE="58t203kF71u9dm6g75P2hA1">-->
<!-- Additional Optional Details -->
<INPUT TYPE="hidden" NAME="email" VALUE="john.smith@example.com">
<INPUT TYPE="hidden" NAME="note" VALUE="This is a note.">
<INPUT TYPE="hidden" NAME="cust_id" VALUE="Some Customer Number">
<INPUT TYPE="hidden" NAME="phone" VALUE="416 555 1212">
<INPUT TYPE="HIDDEN" NAME="lang" VALUE="fr-ca">
<!—- Payment Type information -->
<INPUT TYPE="hidden" NAME="cc_crypt_type" VALUE="7">

<!-- rvar Information -->
<INPUT TYPE="hidden" NAME="rvar_1" VALUE="1">
<INPUT TYPE="hidden" NAME="rvar_monkey" VALUE="monkeys are funny">
<INPUT TYPE="hidden" NAME="rvar_123abc" VALUE="123abc">
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
<FORM ACTION="https://esplusqa.moneris.com/DPHPP/index.php" METHOD="POST">
<!-- Mandatory Fields -->
<INPUT TYPE="hidden" NAME="res_id" VALUE="QRZX9qa002">
<INPUT TYPE="hidden" NAME="res_key" VALUE="reTTJYGTDLNB">
<!-- Additional Optional Details -->
<INPUT TYPE="hidden" NAME="email" VALUE="john.smith@example.com">
<INPUT TYPE="hidden" NAME="note" VALUE="This is a note.">
<INPUT TYPE="hidden" NAME="cust_id" VALUE="Some Customer Number">
<INPUT TYPE="hidden" NAME="phone" VALUE="416 555 1212">
<!—Payment Type information -->
<INPUT TYPE="hidden" NAME="cc_crypt_type" VALUE="7">
<INPUT TYPE="hidden" NAME="ach_sec" VALUE="web">
<INPUT TYPE="hidden" NAME="pd_p_account_number" VALUE="123invoicenumber">
<INPUT TYPE="hidden" NAME="pd_presentation_type" VALUE="W">
<!-- rvar Information -->
<INPUT TYPE="hidden" NAME="rvar_1" VALUE="1">
<INPUT TYPE="hidden" NAME="rvar_monkey" VALUE="monkeys are funny">
<INPUT TYPE="hidden" NAME="rvar_123abc" VALUE="123abc">
<INPUT TYPE="SUBMIT" NAME="SUBMIT" VALUE="Click to proceed to Secure Page">
</FORM>
```

Appendix B Sample Hosted Payment Page Layout

The sample below displays the layout of the Hosted Vault. The sections and sub-sections displayed, as well as the colour and style of the page, are determined by the settings chosen in the Hosted Vault Configuration. Please refer to Configuring the Hosted Payment Page (see page 1) for further information.



QA Merchant 5 - eFraud

Item Details

Description	Product Code	Quantity	Price
Member Fee	R	1	$4.00
		GST:	$0.00
		PST:	$0.00
		HST:	$0.52
		Total (CAD):	$4.52

Customer Details

Customer ID: A customer identifier
Email Address: proper@email.com
Note:

Billing Address		Shipping Address	
First Name:	Mary	First Name:	Bob
Last Name:	Smith	Last Name:	Smith
Company:	Moneris	Company:	Moneris
Address:	1 Lakeshore Blvd	Address:	1 Lakeshore Blvd
City:	Brampton	City:	Brampton
Prov/State:	ON	Prov/State:	ON
Country:	CA	Country:	CA
Postal Code:	L1L1L1	Postal Code:	L1L1L1
Phone:	905-555-3333	Phone:	866-555-1111
Fax:	905-555-4444	Fax:	866-555-2222

Cardholder Details

Please enter the following address exactly as it appears on your credit card statement.

PO Box:
Street Number:
Street Name:
Postal/Zip Code:

Payment Details

Transaction Amount: $4.52 (CAD)
Order ID: mhp13177120341p55

Please complete the following details exactly as they appear on your credit card.
Do not put spaces or hyphens in the credit card number.

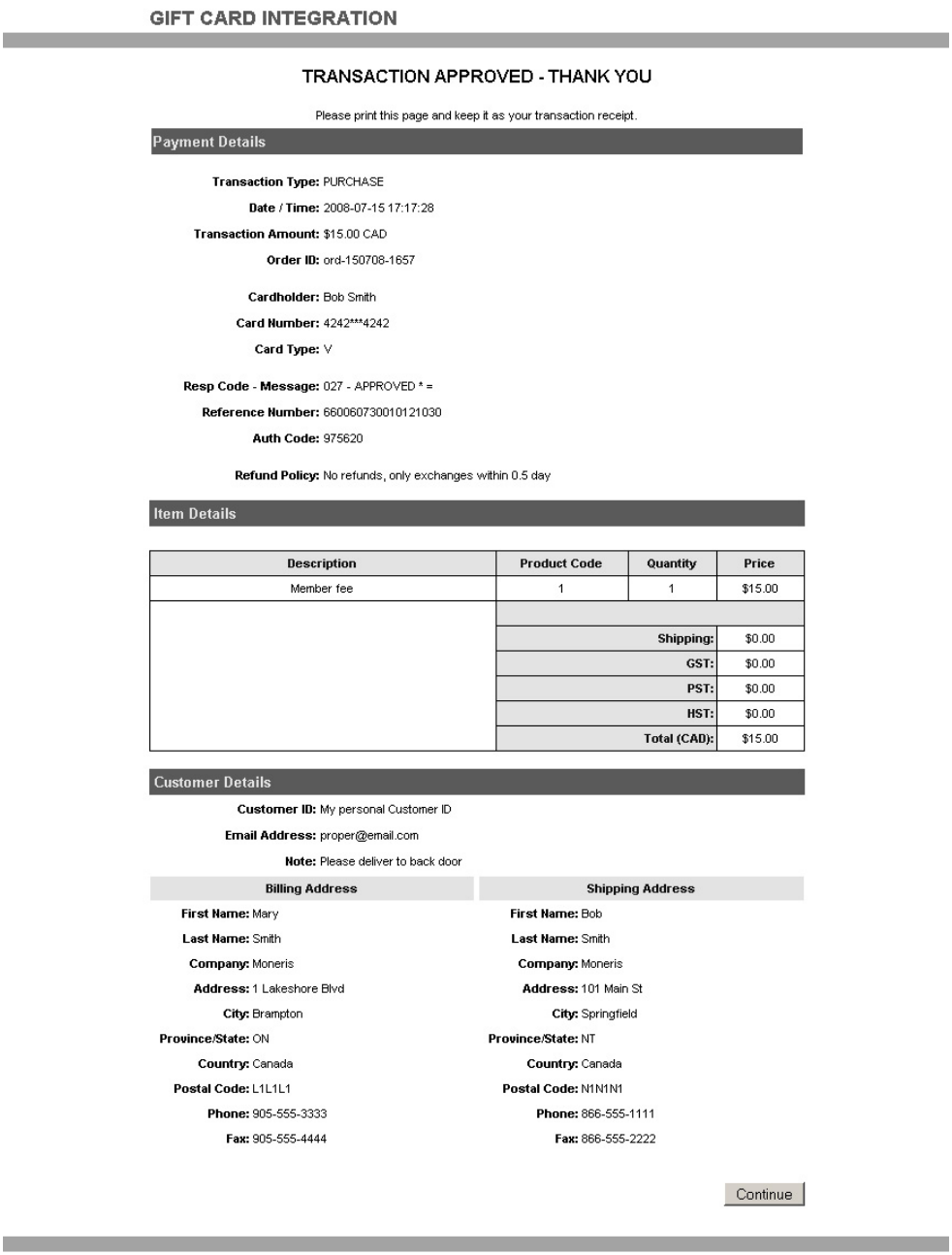
Cardholder Name:
Credit Card Number:
Expiry Date: 06 / 2013
Card Security Code:

Click 'Process Transaction' to charge your credit card. Only click the button once. Using the 'Back','Refresh' or 'Cancel' button after you press the 'Process Transaction' button will not stop the transaction from being processed and may result in a double charge.

Process Transaction Cancel Transaction

Appendix C Sample Receipt

The sample below displays the layout of the response receipt. This receipt is only displayed if the Response Method is set to **Moneris Gateway will generate a receipt** in the Hosted Vault configuration. The sections and subsections displayed, as well as the colour and style of the receipt, are determined by the settings chosen in the Hosted Vault configuration. Please refer to "Configuring the Hosted Payment Page" (page 1) for further information.



GIFT CARD INTEGRATION

TRANSACTION APPROVED - THANK YOU

Please print this page and keep it as your transaction receipt.

Payment Details

Transaction Type: PURCHASE
Date / Time: 2008-07-15 17:17:28
Transaction Amount: $15.00 CAD
Order ID: ord-150708-1657

Cardholder: Bob Smith
Card Number: 4242***4242
Card Type: V

Resp Code - Message: 027 - APPROVED * =
Reference Number: 660060730010121030
Auth Code: 975620

Refund Policy: No refunds, only exchanges within 0.5 day

Item Details

Description	Product Code	Quantity	Price
Member fee	1	1	$15.00
		Shipping:	$0.00
		GST:	$0.00
		PST:	$0.00
		HST:	$0.00
		Total (CAD):	$15.00

Customer Details

Customer ID: My personal Customer ID
Email Address: proper@email.com
Note: Please deliver to back door

Billing Address	Shipping Address
First Name: Mary	**First Name:** Bob
Last Name: Smith	**Last Name:** Smith
Company: Moneris	**Company:** Moneris
Address: 1 Lakeshore Blvd	**Address:** 101 Main St
City: Brampton	**City:** Springfield
Province/State: ON	**Province/State:** NT
Country: Canada	**Country:** Canada
Postal Code: L1L1L1	**Postal Code:** N1N1N1
Phone: 905-555-3333	**Phone:** 866-555-1111
Fax: 905-555-4444	**Fax:** 866-555-2222

Continue

Appendix D XML POST Response for Financial Transaction

The XML is returned in a field called xml_response. A sample of the XML is below. Fields in blue are returned optionally or based on the transaction type performed. The XML should be parsed dynamically to ensure that if and when fields are added in the future the transaction responses are handled properly. Field definitions are the same as indicated in the standard response format tables. Gift card response fields are defined below. The gift_card tag may appear once or twice depending on the number of gift cards used during the transaction. The item tag will appear for every item that was posted in the request with a quantity greater than 0.

NOTE: The XML may not be returned formatted in the manner below. It may be returned as a single line or with line breaks. Your XML parser should be able to handle these variations.

```
<?xml version='1.0' standalone='yes'?>
<response>
<response_order_id>mhp1573006623</response_order_id>
<bank_transaction_id>660035520011120030</bank_transaction_id>
<response_code>027</response_code>
<iso_code>01</iso_code>
<bank_approval_code>608681</bank_approval_code>
<time_stamp>18:53:27</time_stamp>
<date_stamp>2008-07-10</date_stamp>
<trans_name>purchase</trans_name>
<message>APPROVED * =</message>
<charge_total>1.00</charge_total>
<cardholder>Bill Smith</cardholder>
<card_num>4510***5010</card_num>
<card>V</card>
<expiry_date>0807</expiry_date>
<result>1</result>
<convenience_fee>1.00</convenience_fee>
<eci>7</eci>
<txn_num>829-0_22</txn_num>
<rvar1>1_rvar</rvar1>
<rvar2>2_rvar</rvar2>
<transactionKey>uJv2RGGasX4Kd3Tlz3eujRAY5wUCd1</transactionKey>
<recur_result> </recur_result>
<gift_card>
<order_no>mhp1573006623_g1</order_no>
<txn_num>9041-1215730102475-00035540_21</txn_num>
<response_code>000</response_code>
<ref_num>37286815</ref_num>
<terminal_id>00035540</terminal_id>
<txn_type>purchase</txn_type>
<card_num>0211***0222</card_num>
<card_desc>Gift Fixed Reloadabl</card_desc>
<date_time>Jul 10 2008 06:53PM</date_time>
<gift_charge_total>99.50</gift_charge_total>
<rem_balance>0.00</rem_balance>
<display_text>Approved</display_text>
<receipt_text>En
NHLJ: Jul 10, 2008
NHC: 07/10/2008
```

```
NHRJ: 10-07-2008
DHLJ: 10 Jul 2008D
DHC: Jul 10, 2008
DHRJ: End Of Text
</receipt_text>
<voucher_text> </voucher_text>
<result>1</result>
</gift_card>
<item>
<quantity>3</quantity>
<description>qunat 3</description>
<id>sku123</id>
<price>4.00</price>
</item>
<item>
<quantity>2</quantity>
<description>qunat 2</description>
<id>2sku123</id>
<price>24.00</price>
</item>
<item_misc>
<shipping_cost>4.03</shipping_cost>
<hst></hst>
<pst></pst>
<gst>3.03</gst>
</item_misc>
<shipping>
<ship_first_name>sfn</ship_first_name>
<ship_last_name>sln</ship_last_name>
<ship_company_name>scn</ship_company_name>
<ship_address_one>sao</ship_address_one>
<ship_state_or_province>ssop</ship_state_or_province>
<ship_postal_code>spc</ship_postal_code>
<ship_country>scount</ship_country>
<ship_phone>sp</ship_phone>
<ship_fax>sf</ship_fax>
</shipping>
<billing>
<bill_first_name>bfn</bill_first_name>
<bill_last_name>bln</bill_last_name>
<bill_company_name>bcn</bill_company_name>
<bill_address_one>bao</bill_address_one>
<bill_state_or_province>bsop</bill_state_or_province>
<bill_postal_code>bpc</bill_postal_code>
<bill_country>bcount</bill_country>
<bill_phone></bill_phone>
<bill_fax></bill_fax>
</billing>
<od_other>
<email>bill.smith@example.com</email>
<cust_id>customer num</cust_id>
<note>these are special instructions</note>
</od_other>
</response>
```

Appendix E Internet Explorer 7 Compatibility

The example code in 1 Getting a Temporary Token on page 1 does not support Internet Explorer 7, so if compatibility with Internet Explorer is required then the below code should be used instead.

The example below will work once you add your Hosted Tokenization ID along with your own URL.

```
<html>
<head>
<script type="text/javascript">
function doMonerisSubmit()
{
var frame_ref;

if(navigator.userAgent.indexOf("Safari") != -1)
{
frame_ref = frames["monerisFrame"];
}
else
{
frame_ref = document.getElementById("monerisFrame").contentWindow;
}
frame_ref.location = "https://esqa.moneris.com/HPPtoken/index.php?id=<YOUR HPP TOKEN
ID>&poll=true&css_body=background:green;border:2px dotted purple;&css_textbox=border:1px
solid blue; &css_textbox_pan=width:140px;&enable_exp=1&css_textbox_exp=width:40px;&enable_
cvd=1&css_textbox_cvd=width:40px;&parent=<THE URL OF PARENT WINDOW> " + "#submitResForm" +
(new Date()).getTime();
}
var post_data = "";

function checkForMessages()
{
if(location.hash != post_data)
{
post_data = location.hash;
var raw_json = decodeURIComponent(post_data.substr(1));
var respData = eval("(" + raw_json + ")");
document.getElementById("monerisResponse").innerHTML = " SENT " + " - " +
respData.responseCode + " " + respData.dataKey + " - bin: " + respData.bin;
document.getElementById("monerisFrame").style.display = 'none';
}
}
setInterval("checkForMessages()", 200);
</script>
</head>
<body style=background:#E3E3E3>
<div>This is the outer page!!</div>
<div id=monerisResponse></div>
<iframe id=monerisFrame src="https://esqa.moneris.com/HPPtoken/index.php?id=<YOUR HPP TOKEN
ID>&poll=true&css_body=background:green;border:2px dotted purple;&css_textbox=border:1px
solid blue &css_textbox_pan=width:140px;&enable_exp=1&css_textbox_exp=width:40px;&enable_
cvd=1&css_textbox_cvd=width:40px;&parent=<THE URL OF PARENT WINDOW>" frameborder='0'
width="200px" height="30px"></iframe>
<input type=button onClick=doMonerisSubmit() value="go go">
</html>
```

Appendix F How to Identify Visa Debit Cards

Visa Debit transactions can be indentified by checking the value of the visaDebit member of the response object.

The example below demonstrates how to do this in bold.

> **NOTE:** the response value for this field will be either True or undefined, the field will not return false, so the best way to handle this is to check if the response is equal to the string value of “true”.

```
<html>
<head>
<title> Outer Frame - Merchant Page</title>
<script>
    function doMonerisSubmit()
    {
        var monFrameRef = document.getElementById('monerisFrame').contentWindow;
        monFrameRef.postMessage('','https://esqa.moneris.com/HPPtoken/index.php');
        return false;
    }

    var respMsg = function(e)
    {
        var respData = eval("(" + e.data + ")");

        document.getElementById("monerisResponse").innerHTML = e.origin + " SENT " + " |
Response Code: "
+ respData.responseCode + " | "Temporary Token: " + respData.dataKey + " | Error Message: "
+ respData.errorMessage + " | Visa Debit: " + respData.visaDebit;
        document.getElementById("monerisFrame").style.display = 'none';
        //Correct what to check for a Visa Debit card
        if(respData.visaDebit == "true")
        {
            alert("This is a Visa Debit Card");
        }
    }

    window.onload = function()
    {
        if (window.addEventListener)
        {
            window.addEventListener ("message", respMsg, false);
        }
        else
        {
            if (window.attachEvent)
            {
                window.attachEvent("onmessage", respMsg);
            }
        }
    }
</script>
</head>

<body>
```

```
    <div>This is the outer page!!</div>
    <div id=monerisResponse></div>
    <iframe id=monerisFrame src="https://esqa.moneris.com/HPPtoken/index.php?id=<YOUR HPP
TOKEN ID>&poll=true&css_body=background:green;border:2px dotted purple;&css_
textbox=border:1px solid blue &css_textbox_pan=width:140px;&enable_exp=1&css_textbox_
exp=width:40px;&enable_cvd=1&css_textbox_cvd=width:40px;&parent=<THE URL OF PARENT WINDOW>"
frameborder='0' width="200px" height="30px"></iframe>

    <input type=button onClick=doMonerisSubmit() value="go go">

</html>
```