Global Transport Secure Page

Implementation Guide

Version 2.1

July 2014

Global Payments Inc.
10 Glenlake Parkway, North Tower
Atlanta, GA 30328-3447

Release July 2014

The Global Transport Secure Page Implementation Guide contains information proprietary to Global Payments. It is intended to be used only in conjunction with the Global Transport Secure Page application.

Global Payments Inc.
10 Glenlake Parkway, North Tower
Atlanta, GA 30328-3447

Table of Contents

Changes and Modifications

The table below lists the changes made to the Global Transport Secure Page Implementation Guide from previous releases:

Version	Changes/Modifications	Pages
1.0	Initial Release.	All
1.1	Added CVVMatch and AVSMatch fields to transaction response values.	20
1.1	Added AVS Result Codes.	47
1.2	Updated Support information.	1
1.2	Added Sandbox Testing information.	10
1.3	Added Global Transport Gateway Response Codes to Error Messages.	44
1.4	Updated Support information.	1
1.4	Updated sandbox testing instructions regarding duplicate transactions.	10
1.4	Added CVV Result Codes.	51
1.5	Updated boarding information with instructions on setting up a separate user account for Global Transport Secure eCommerce.	4
1.5	Added note about Global Transport Virtual Terminal requiring Internet Explorer.	11, 17
1.5	Added a trailing slash to the Transaction Validation Service URL for production use and a note about the requirement of the slash.	35
1.5	Added “Authentication failure.” to Global Transport Secure Page Processing Messages; updated Processing Messages with error codes.	43
1.5	Added ERROR: ((1000)) and ERROR: ((1001)) section.	47
1.6	Updated Payment Request Form POST Values table format and added Page Request Block, Payment Form Options Block, and Order Details Block parameters.	12-17
1.6	Added uID and CRE_Tokenize Payment Request Form POST Values.	12
1.6	Added Diners Club to allowed_types Payment Request Form POST Values.	15
1.6	Updated organization of Sample Merchant HTML Code for Payment Request Form.	18
1.6	Added uID, CRE_Card_Token, and analysis_result to Transaction Success Response Page postback values.	19
1.6	Added new CSS elements used for styling the Merchant Payment Template Page’s payment form.	21
1.6	Added Controlling the ERROR Message Suffix Text to Merchant Payment Template Page.	24
1.6	Added Customizing Fields to Merchant Payment Template Page.	24
1.6	Added Card on File section to Global Transport Secure Direct Services.	28
1.6	Added Repeat Sale section to Global Transport Secure Direct Services.	32
1.6	Updated name of response_type Transaction Validation Service response field.	35

Version	Changes/Modifications	Pages
1.6	Added uID section to Global Transport Secure Direct Services.	37
1.6	Added Transaction Reversal section to Global Transport Secure Direct Services.	41
2.0	Added information regarding PCI compliance to Introduction.	2
2.0	Added Section 508 compliance.	2
2.0	Updated boarding process.	5
2.0	Updated Payment Request Form POST Value allowed_types with JCB value.	15
2.0	Added Payment Request Form POST parameters token_type, token_slug, collect_total_amount, collect_order_id, collectAddress.	13, 16
2.0	Added ACH payments.	14
2.0	Updated description of Payment Request Form POST Value currency_code.	16
2.0	Updated description of Payment Request Form POST Value order_id to include invoice number restrictions.	15
2.0	Added instructions for reversing transactions based on AVS and CVV response values.	20
2.0	Updated Card on File and Repeat Sale tokenization descriptions.	28
2.0	Add instructions for using custom tokens.	33
2.0	Updated description Transaction Reversal service to describe flow for void and refund. Updated description of parameter reversal_type.	41
2.0	Updated transaction response values.	44
2.0	Added troubleshooting information for WordPress.	48
2.1	Added MasterPass™ Implementation section	25
2.1	Added MasterPass Onboarding section	8
2.1	Added New Authorization with a Card on File information	30
2.1	Added Card Verify Transaction information	37
2.1	Added Pre-Auth Complete through Direct Services information	38
2.1	Added link to MasterPass Terms of Use	55
2.1	Added links to QuickStart Secure Page support site	55
2.1	Updated Sandbox support e-mail address.	10
2.1	Added link for online Sandbox Test Account requests	10
2.1	Updated Support information with QuickStart links	1
2.1	Updated PCI Compliance section	52

Support

Global Payments Inc. is committed to providing the highest quality tools and customer support. If you forget your Global Transport Production Gateway password, you must contact the PC Support Desk at (800) 462-6609 to reset your password. If you forget your Sandbox password or cannot access your Global Transport Secure eCommerce Sandbox test account, contact (888) 453-4885. For security purposes, passwords cannot be provided via email.

The Global Transport Secure eCommerce QuickStart website is located at **https://quickstart.hps.controlscan.com/gt/**.

Technical support for questions related to the implementation of Global Transport Secure eCommerce is available by telephone from 8:00 am to 8:00 pm ET (GMT-5) M-F at **(888) 453-4885**. Messages left after 8:00 pm will be responded to the next business day.

Technical support via e-mail is available at **GTSupport@ControlScan.com** with a one business day turn-around.

Support tickets can be submitted online at **http://quickstart.hps.controlscan.com/gt/gt-helper/**

Introduction

Global Transport Secure Page provides a way to perform credit card transactions on your site and remain PCI compliant without implementing expensive security measures on your servers. Global Transport Secure Page maintains the quality of the customer experience by using HTML Clone™ technology to display a secure payment form using your payment template page.

Global Transport Secure Page is Section 508 compliant.

Global Payments is certified as a PCI Compliant Level 1 service provider. The following link shows a list of PCI Compliant service providers:

http://www.visa.com/splisting/

Overview

This document describes the prerequisites for setting up a site using Global Transport Secure Page, then, describes the components of Global Transport Secure Page and how to incorporate them into your site.

Prerequisites

Prerequisites for Global Transport Secure Page fall in to two categories: merchant and technical.

Merchant Prerequisites

Before configuring Global Transport Secure Page, Merchants must meet the following requirements:

- Merchants must already have a Global Payments merchant account
- Merchants must complete the enrollment for Global Transport Secure Page at the following URL:

  http://manage.gtpaysecure.com/

Website Prerequisites

Your site must meet the following requirements to connect to Global Transport Secure Page:

- Accessible via the internet
- Use HTML to generate distinct web pages
- Have an SSL certificate installed (any SSL provider is allowed; most web hosts resell SSL certificates. A 256-bit certificate is recommended; 128-bit certificates are allowed.)

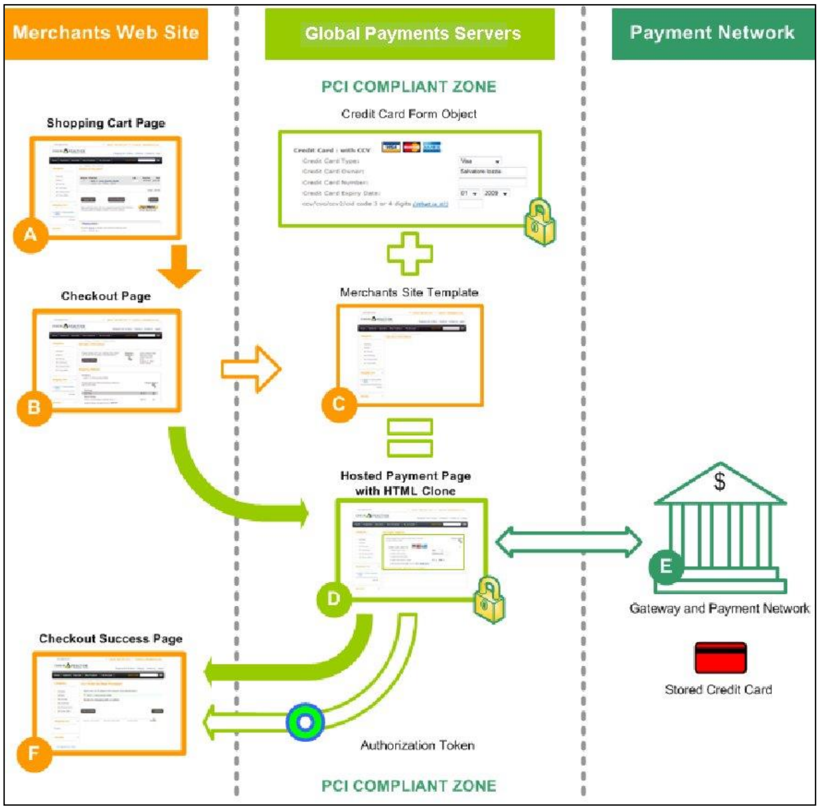
Global Transport Secure Page Site Components

Using Global Transport Secure Page on your site requires the following elements which are described in greater detail in the rest of this document:

- Payment Request Form
- Template Payment Page
- Transaction Success Response Page

System Overview

The following graphic illustrates how Global Transport Secure Page works to help you process credit card transactions and meet PCI requirements:



A. Customers begin by creating orders on your site as normal.

B. They proceed to checkout where the Global Transport Secure Page is integrated to the Payment Request Form. They select the Global Transport Secure Page payment method and choose Checkout.

C. Global Transport Secure Page servers receive the order and payment request. Using a process called HTML Clone™, Global Transport Secure Page reads the Template Payment Page on your site in real time, scrubs it for any malicious code, and then combines it with a secure credit card collection form.

D. Global Transport Secure Page presents customers with a secure hosted payment page that looks just like your site. With HTML Clone™, the customer still has access to navigation of your site because Global Transport Secure Page dynamically matches your unique template design from the Template Payment Page on the merchant site.

E. The cardholder data and payment transaction is processed in our highly secure, PCI-Compliant data center and connects directly with the Global Transport Gateway.

F. Once the payment transaction is complete the customer is sent directly back to your Transaction Success Response page, where the order status is updated. The response includes transaction information and masked card data.

Global Transport Secure eCommerce Boarding

Before configuring Global Transport Secure Page on your merchant site, you must first board on the Global Transport Secure eCommerce Boarding site.

To board your merchant on the Global Transport Secure Page, follow these steps:

1. Add a new user using Global Transport VT that will be used to process transactions through Global Transport Secure eCommerce. See Adding a Global Transport Secure eCommerce User below for instructions.
2. Log in to Global Transport VT using the new user to reset the password.
3. Board the new user you created on Global Transport Secure eCommerce. See Boarding Process on page 5 for instructions.

Adding a Global Transport Secure eCommerce User

Before boarding on the Global Transport Secure eCommerce Boarding site, you must add a new user for this purpose and set your Global Transport Secure eCommerce user to have a password that does not expire.

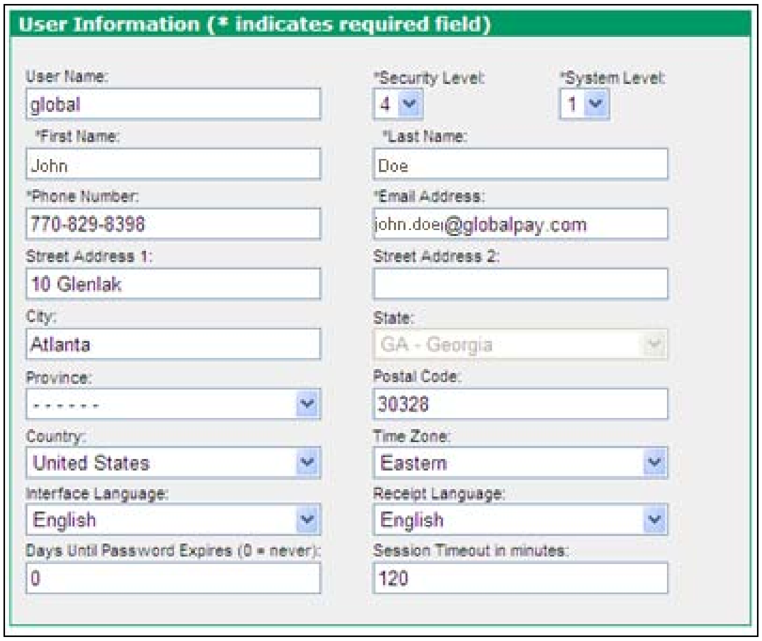
> **Note:** You must set the password for the user to never expire. If you do not, the credentials will expire within 90 days and your website will not be able to process transactions until you reset the password and re-board the merchant on Global Transport Secure eCommerce.

To add a Global Transport Secure eCommerce user, follow these steps:

1. Log in to Global Transport VT using the credentials you received in your welcome email.

   Note: If this is your first time logging in, you will be required to reset your password.

2. From the Main Menu, click **Manage Users**.
3. From the Manage Users menu, click **Add**. The following screen displays:



User Information (* indicates required field)

User Name: global

*Security Level: 4

*System Level: 1

*First Name: John

*Last Name: Doe

*Phone Number: 770-829-8398

*Email Address: john.doe@globalpay.com

Street Address 1: 10 Glenlak

Street Address 2:

City: Atlanta

State: GA - Georgia

Province: - - - - - -

Postal Code: 30328

Country: United States

Time Zone: Eastern

Interface Language: English

Receipt Language: English

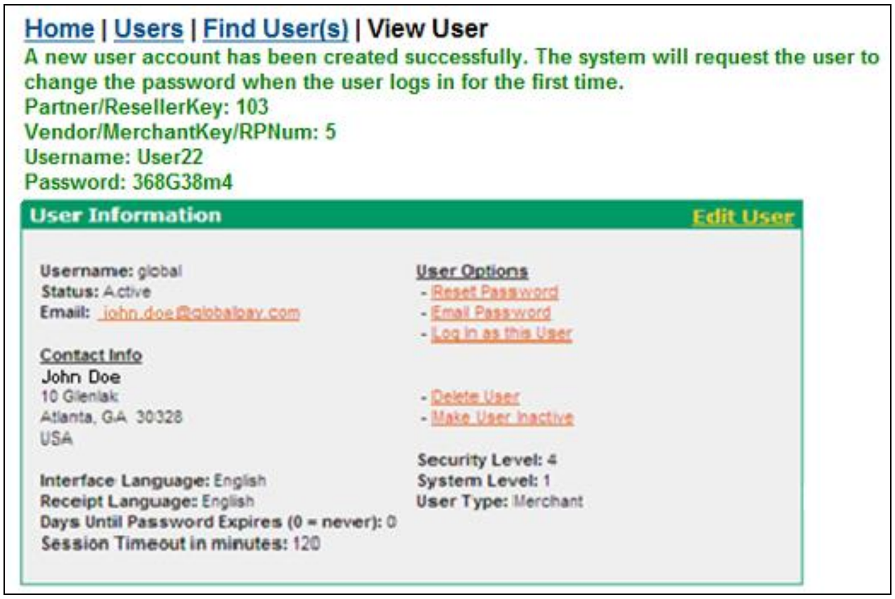
Days Until Password Expires (0 = never): 0

Session Timeout in minutes: 120

Complete the fields on this screen. See the *Global Transport VT User Guide* for complete field descriptions.

In the **Days Until Password Expires** field, enter 0 to set the password to never expire.

4. Click **Save User**. Global Transport VT displays the following message indicating the information about the user account:



A new user account has been created successfully. The system will request the user to change the password when the user logs in for the first time.
Partner/ResellerKey: 103
Vendor/MerchantKey/RPNum: 5
Username: User22
Password: 368G38m4

Username: global
Status: Active
Email: john.doe@globalpay.com

Contact Info
John Doe
10 Glenlak
Atlanta, GA 30328
USA

Interface Language: English
Receipt Language: English
Days Until Password Expires (0 = never): 0
Session Timeout in minutes: 120

Security Level: 4
System Level: 1
User Type: Merchant

To complete the process, log in to Global Transport VT using the newly created user. When you first log in, you must reset the password for the user.

Boarding Process

To board on the Global Transport Secure eCommerce Boarding site, follow these steps:

1. Navigate to the following boarding site URL.

   For production, use the following URL:

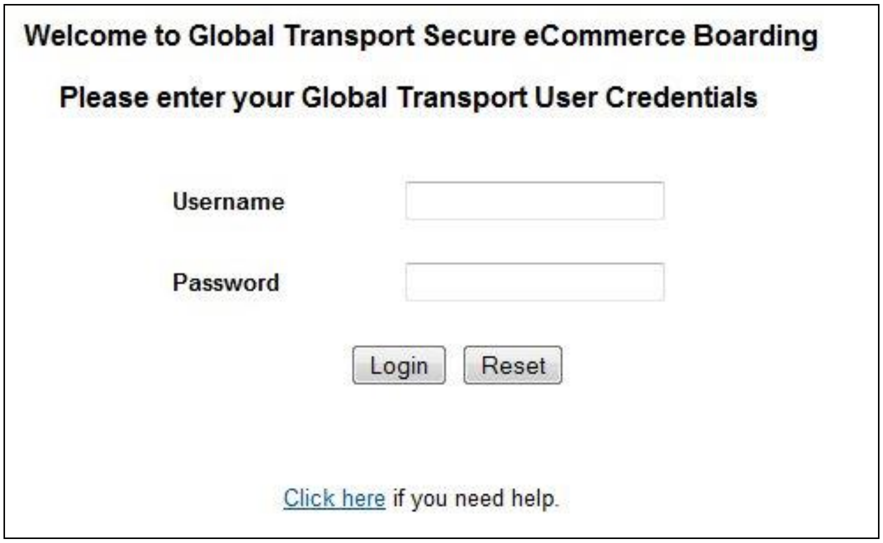
   https://manage.gtpaysecure.com

   For sandbox testing, use the following URL:

   https://manage-sandbox.gtpaysecure.com/

   Note: You must use the username and password you created in the previous section for access to the Production gateway.

The following screen displays:



Welcome to Global Transport Secure eCommerce Boarding

Please enter your Global Transport User Credentials

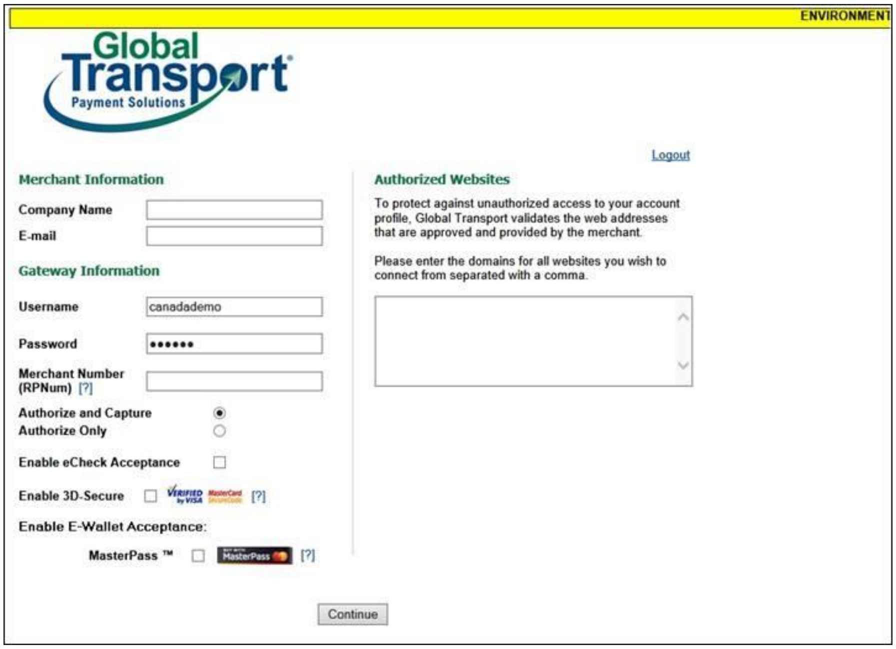
Username

Password

Click here if you need help.

2. Enter the user name and password created in the previous section and click **Login**.

   The following screen displays:



Merchant Information

Company Name

E-mail

Gateway Information

Username canadademo

Password ••••••

Merchant Number (RPNum) [?]

Authorize and Capture ●

Authorize Only ○

Enable eCheck Acceptance □

Enable 3D-Secure □ [?]

Enable E-Wallet Acceptance:

MasterPass ™ □ [?]

Authorized Websites

To protect against unauthorized access to your account profile, Global Transport validates the web addresses that are approved and provided by the merchant.

Please enter the domains for all websites you wish to connect from separated with a comma.

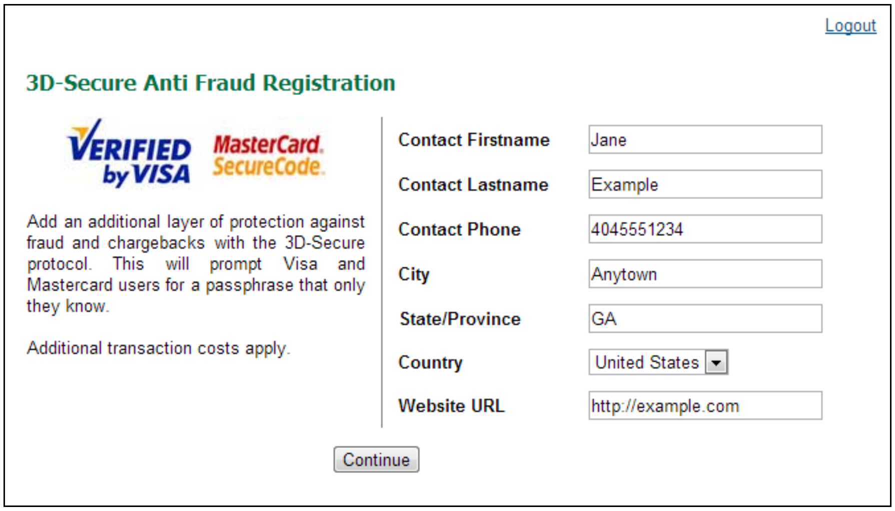
3. Use the following table to complete this screen:

Field	***Description***
Company Name	Enter the name of your company.
Email	Enter your business email address.
Username	Enter the gateway username created in the previous section.
Password	Enter the gateway password created in the previous section.

Field	*Description*
Authorize and Capture **Authorize Only**	Select **Authorize and Capture** to capture transactions in a batch for processing. Select **Authorize Only** if you will use another service to capture transactions.
Enable eCheck Acceptance	Select to enable check processing through Global Transport Secure Page.
Enable 3D-Secure	Select to enable 3D-Secure security to reduce fraud and chargebacks. Additional transaction fees apply.
Enable E-Wallet Acceptance: MasterPass	Select to enable MasterPass e-wallet payments
Authorized Websites	Enter a list of domain names for each website you will use to connect to Global Transport Secure Page. Any domain hosting your CSS, payment template page, and response page must be listed here. If you are connecting more than one domain, list all domains here separated by commas.

4. Click **Continue**.

   If you select Enable 3D-Secure, the following screen displays (otherwise continue to step 6):



3D-Secure Anti Fraud Registration

Add an additional layer of protection against fraud and chargebacks with the 3D-Secure protocol. This will prompt Visa and Mastercard users for a passphrase that only they know.

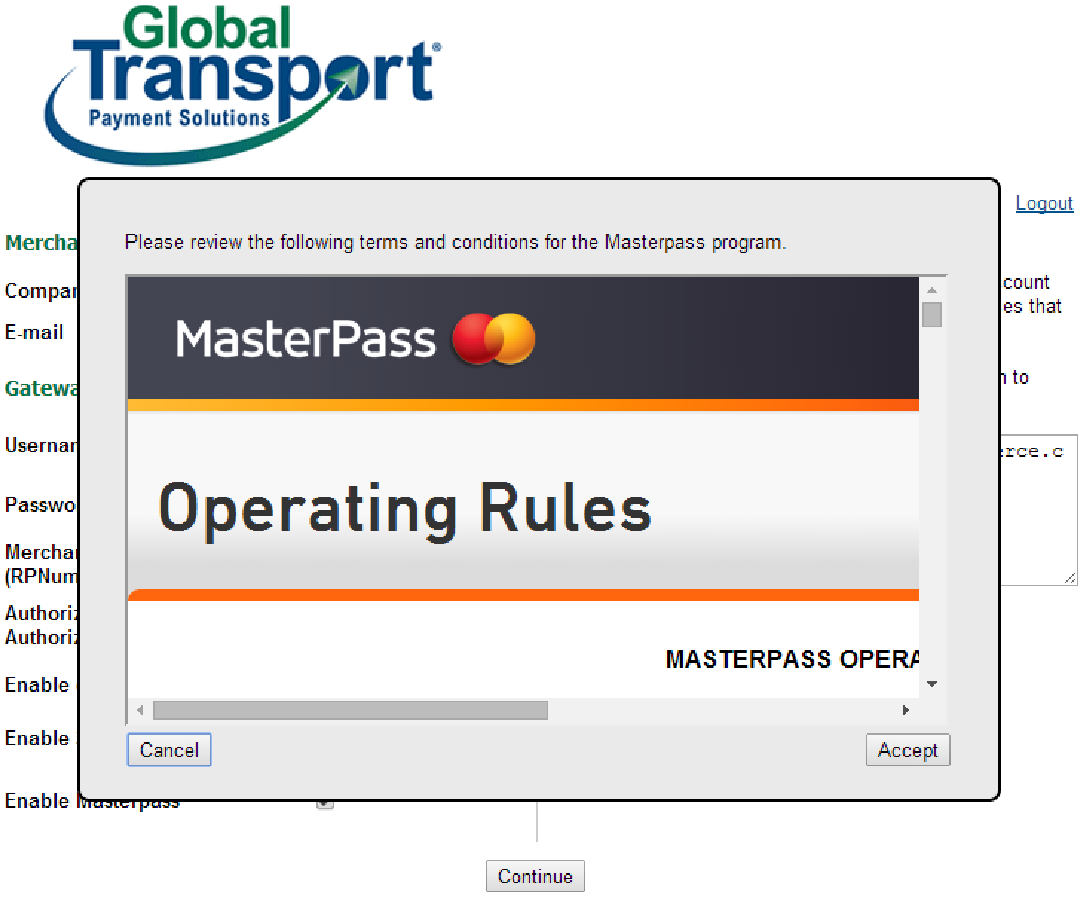
Additional transaction costs apply.

Contact Firstname	Jane
Contact Lastname	Example
Contact Phone	4045551234
City	Anytown
State/Province	GA
Country	United States
Website URL	http://example.com

5. Enter your business contact information for 3D-Secure processing.

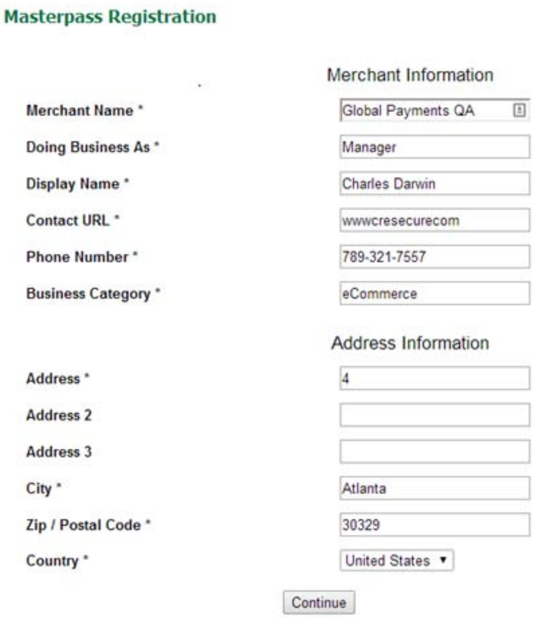
6. Click **Continue**.

   The following screen displays:



Please review the following terms and conditions for the Masterpass program.

7. Click **Accept** if you want to review the MasterPass Terms of Use and enable MasterPass. You will be presented with the MasterPass Registration page:



Masterpass Registration

Merchant Information

Merchant Name *	Global Payments QA
Doing Business As *	Manager
Display Name *	Charles Darwin
Contact URL *	wwwcresecurecom
Phone Number *	789-321-7557
Business Category *	eCommerce

Address Information

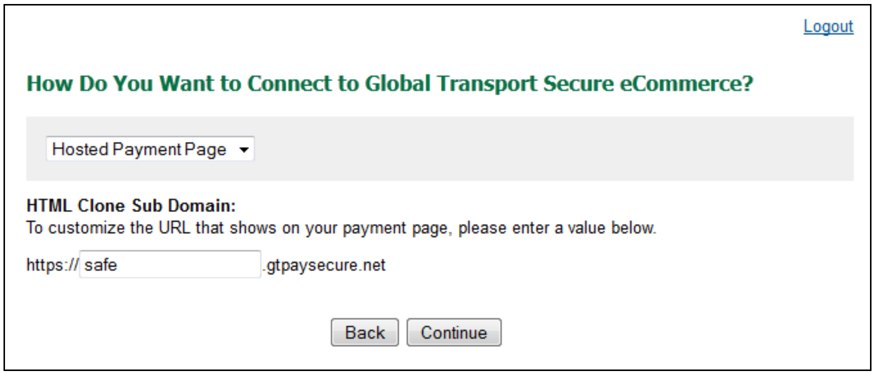
Address *	4
Address 2	
Address 3	
City *	Atlanta
Zip / Postal Code *	30329
Country *	United States ▾

Enter your business contact information for MasterPass processing and click **Continue**.

8. Click **Cancel** if you do not want to enable MasterPass.

9. Click **Continue**.

   The following screen displays:



How Do You Want to Connect to Global Transport Secure eCommerce?

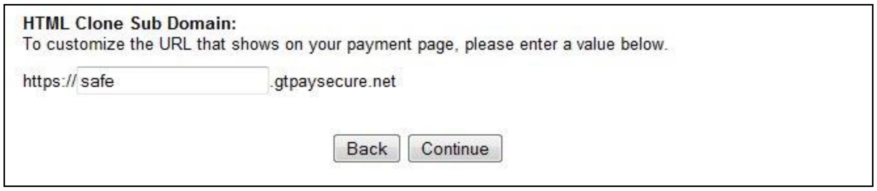
Hosted Payment Page

HTML Clone Sub Domain:
To customize the URL that shows on your payment page, please enter a value below.

https:// safe .gtpaysecure.net

10. Select Hosted Payment Page.

    The following option displays:



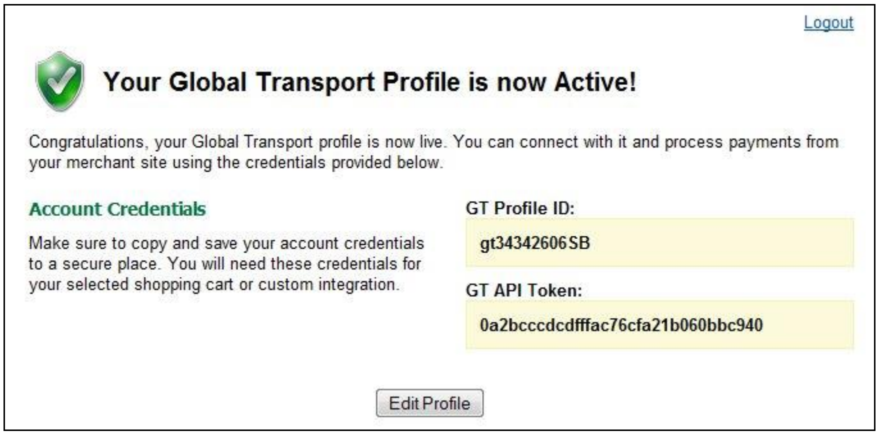
HTML Clone Sub Domain:
To customize the URL that shows on your payment page, please enter a value below.

https:// safe .gtpaysecure.net

You can customize the gtpaysecure.net sub-domain URL for your payment page, for example to reflect the domain name of your website.

11. After setting the options for your connection type, click **Continue**.

    The following screen displays.



Your Global Transport Profile is now Active!

Congratulations, your Global Transport profile is now live. You can connect with it and process payments from your merchant site using the credentials provided below.

Account Credentials

Make sure to copy and save your account credentials to a secure place. You will need these credentials for your selected shopping cart or custom integration.

GT Profile ID: gt34342606SB

GT API Token: 0a2bcccdcdfffac76cfa21b060bbc940

Copy and save your account credentials in a secure place. The GT Profile ID and GT API Token values are used to connect to the Global Transport Secure Page.

Testing

Production Testing

Global Payments suggests using the production environment (safe.gtpaysecure.net) for testing Global Transport Secure Page integrations. Use the following test card information to verify that your integration is properly submitting purchase transactions

Note: You will be charged a per transaction fee for test transactions submitted into production, even when Declined.

Credit Card	*Card Number*	*Exp. Date*	*CVV/CID*	*AVS*
Visa	4788250000028291	Dec. 2015 (1215)	123	Street: 10 Glenlake Parkway ZIP: 30328
MasterCard	5454545454545454		123	

The card issuer will return a response of Declined – INVLD ACCT. This response validates that your integration is connecting successfully to the Global Transport gateway and is communicating with the card associations.

Sandbox Credentials

If you wish to perform more extensive testing of your integration, please request a test account on the development sandbox. Follow the steps below to use the sandbox environment:

1. Request a Global Transport Secure eCommerce test account online at **http://quickstart.hps.controlscan.com/gt/gt-test-account-request-form/**
2. Or, send an e-mail to **GTSupport@ControlScan.com** requesting a Global Transport Secure eCommerce test account. You will be e-mailed a Test Account Request Form. Please complete the form and return it to **GTSupport@ControlScan.com**.

   You will receive special Global Transport Secure Page Sandbox credentials for your test applications. You will also receive the Global Transport Secure eCommerce sandbox URL and instructions regarding connecting your application to the sandbox.
3. When you are ready to go live, update your application to use the production endpoints defined in this document.

Sandbox Testing

Use the following test card information to verify that your integration is properly submitting purchase transactions

Credit Card	*Card Number*	*Exp. Date*	*CVV/CID*	*AVS*
Visa	4003000123456781	Dec. 2015 (1215)	123	Street: 10 Glenlake Parkway ZIP: 30328
MasterCard	5499990123456781		123	

Transactions submitted for less than $11.00 will receive an Approved response. Transactions submitted for amounts greater than $11.00 will receive a Declined response.

Vary the amounts when testing (i.e., $1.01, $1.02, etc.) Multiple transactions submitted into the open batch for the same card number and amount indicate a Duplicate Transaction to the test host. The host returns a Decline (12) response for those transactions.

Note: Do NOT use the above test card numbers in a batch of live transactions on Production. The presence of those test card numbers will cause the host to drop the entire batch, which cannot be recovered.

If you wish to test into production and receive Approval responses, please use a valid credit card. You can use the Global Transport Virtual Terminal account provided when you board your integrated application to void or refund any live card transactions submitted into Production.

Note: To log into the Global Transport Virtual Terminal, open Internet Explorer, go to **https://vt.globalpay.com/admin/login.aspx**, and log in with the provided account credentials. You must use Internet Explorer.

Note: Please contact Global Payments at **GTSupport@ControlScan.com** before attempting any stress or load testing.

Payment Request Form

When a customer selects a payment method supported by Global Transport Secure Page from the payment request form, send an HTTPS POST to the Global Transport Secure Page server to initiate the payment process. Send the post to the following URL:

- Production
  https://safe.gtpaysecure.net/securepayments/a1/cc_collection.php
- Development and testing
  https://safe.sandbox-gtpaysecure.net/securepayments/a1/cc_collection.php

Note: See Production Testing on page 10 for testing instructions and test credit card numbers.

Note: The payment request forms are posted to the **safe.gtpaysecure.net** URL. The **manage.gtpaysecure.com** URL is only used for the boarding site.

IMPORTANT! Your website must use SSL. Posting to Global Transport Secure Page from a non-SSL URL will result in a 404 error because Global Transport Secure Page only accepts secure connections.

The following sections describe the payment request form post values and provide sample HTML code for posting to the Global Transport Secure Page server.

Payment Request Form POST Values

The following table describes the payment request form POST values:

Note: The optional customer and order information fields do not display on the Secure Page. If the merchant provides data in these fields, the data is echoed back in the response message for processing by the merchant.

POST Value	*Required*	*Description*
uID	Optional	A unique identifier used to pass transaction information between your servers and Global Transport without sending it through the customer's browser. Send the uID instead of the other values in this table to perform a Payment Form Request. See uID on page 39 for information on obtaining and using a uID. Alphanumeric.
Page Request Block		
CRESecureID	Required	The GT Profile ID you received from the Global Transport Secure eCommerce Boarding site. Unique account number for Global Transport Secure Page.

POST Value	***Required***	***Description***
return_url	Required	The HTTPS URL on the merchant site where the customer is returned along with the values from a successful transaction. **Note:** If a customer remains on the payment form page for more than 15 minutes, Global Transport Secure Page returns the customer to the return_url with the action parameter value “cancel”.
content_template_url	Required for HTML Clone™	The HTTPS URL where the merchant template resides. If omitted the page will render without a template, for use in pop up integrations.
cancel_url	Optional	The HTTPS URL to display if a customer clicks “Cancel” on the payment form. If not defined, HPP returns the customer to the URL set by the return_url post value.
CRE_Tokenize	Optional	Invokes the card-storing capability described in Card on File on page 28. The customer’s card information will be stored on file at the Global Transport Gateway vault without authorizing a payment amount. The value for this parameter is: **store_only**
token_type	Optional	Specifies the custom token format. See Requesting a Custom/Legacy Token Format on page 33 for more details. This parameter takes the following values: • **custom** – Uses 12 leading digits provided by the merchant and the last four digits of the credit card number. • **mod10a** – Preserves the last four digits and the first two digits of the credit card number. The four middle digits ensure that the token is not a valid card number. The full token value is mod10 validated.
token_slug	Optional	For custom tokens, this is the first 12 digits of the token. See Requesting a Custom/Legacy Token Format on page 33 for more details. 12 digits, numeric, unique from other submitted values.
sess_id	Optional	The unique session identifier for the customer user on the merchant site. Minimum 8 characters.
sess_name	Optional	The session name for the customer user on the merchant site. Default = osCsid

POST Value	***Required***	***Description***
analysis	Optional	Checks the card number against BIN ranges provided by the processor to determine the card type and the card level. Card analysis is only as accurate as the BIN ranges provided by the processor. Valid values are: • **card_type** – checks debit or credit • **card_level** – checks consumer or purchase card • **card_type|card_level** – checks both type and level
trans_type	Optional	Sets the transaction type. Valid values are: • **auth_capture** – sets the transaction type to Sale • **auth_only** – sets the transaction type to Auth Only • **auth_complete –** sets the transaction type to PreAuth Complete The default for this parameter is set in the Merchant Profile.
multi_trans_profile_id	Optional	Alphanumeric GT Profile ID of an affiliated merchant. Generates multiple tokens when a single customer transaction actually generates multiple transactions. The GT Profile ID value determines the merchant that receives the second token. **Note:** This feature requires authorization by Global Transport before it can be used, and the ID of the affiliate merchant must be listed on your Global Payments Merchant Profile as an authorized ID.
Payment Form Options Block		
payment_type	Optional	Sets the payment acceptance type. Valid values are: • **Credit_Card** – credit card (default) • **ACH** – ACH/check

POST Value	*Required*	*Description*
allowed_types	Optional	The card types to display on the payment form. Text separated by PIPE delimiter. For example: Visa|MasterCard|American Express Valid values are: • **Visa** • **MasterCard** • **American Express** • **Discover** • **Diners Club** • **JCB** To enable all card types, send the following string as the value: Visa|MasterCard|American Express|Discover|Diners Club|JCB Default value is Visa|MasterCard
form	Optional	Changes the displayed payment form. Valid values are: • **osc** – table-based form based on osCommerce wide HTML format (default) • **mage** – table-less form based on Magento tall HTML format
required	Optional	Changes the form validation and requirements. Valid values are: • **minimum** – Name on Card: optional; Card Number: required; Expiration Date: required; CVV: optional (default) • **all** – all fields required
Order Details Block		
total_amt	Required if CRE_Tokenize is not used	The amount to authorize or capture in the transaction. Numeric, 2 decimal places.
total_weight	Optional	The total weight of the order. Determines if physical or digital goods. A value of 0 indicates digital goods. Default = 0
order_desc	Optional	Text description of the purchase. Minimum 1 character.
order_id	Optional	System value of the order or payment (gets trimmed). Maximum length for American Express cards is 16 characters. Maximum length for all other cards is 25 characters. Minimum 1 character.
customer_id	Optional	The customer identification number. Minimum 1 character.
ip_address	Optional	The IP address of the customer. Must be in valid IP address format.

POST Value	***Required***	***Description***
currency_code	Optional	The 3 letter ISO currency of the transaction. Must be valid ISO currency code. • **USD** – U.S. dollars • **CAD** – Canadian dollars Default value is USD.
lang	Optional	The language of the text displayed on the payment page. Valid values are: • **en_US** – English (default) • **fr_CA** – French
collect_total_amount	Optional	Determines whether to collect the total value for the transaction on the payment page. The default value is 0. Valid values are: • 0 – Do not collect total amount on payment page • 1 – Display total amount as read only field • 2 – Collect total amount with editable field
collect_order_id	Optional	Determines whether to collect the order ID for the transaction on the payment page. The default value is 0. Valid values are: • 0 – Do not collect order ID on payment page • 1 – Display order ID as read only field • 2 – Collect order ID with editable field
collectAddress	Optional	Determines whether to collect the customer's address for the transaction on the payment page. The default value is 0. Valid values are: • 0 – Do not collect address on payment page • 1 – Collect address with editable field • 2 – Collect address including country with editable field
Customer Info Block – Billable Address for AVS		
customer_company	Optional	Customer's company name. Minimum 1 character.
customer_firstname	Optional	Customer's first name. Minimum 1 character.
customer_lastname	Optional	Customer's last name. Minimum 1 character.
customer_address	Optional	The billing address street number and name. Required for AVS by most gateways. Minimum 1 character.

POST Value	***Required***	***Description***
customer_address2	Optional	The second line of the billing address. Required for AVS by most gateways. Minimum 1 character.
customer_email	Optional	Customer email for the billing address. Must be valid email format.
customer_phone	Optional	Phone number for the billing address. Numeric. Minimum 10 characters.
customer_city	Optional	The billing address city. Minimum 1 character.
customer_state	Optional	The billing address state or province. 2 letter abbreviation.
customer_postal_code	Optional	The billing address ZIP or postal code. Required for AVS by most gateways. Minimum 5 characters.
customer_country	Optional	The billing address country. 3 letter ISO. Default = USA
Customer Delivery Block – Shipping Address		
delivery_company	Optional	Ship-to company name. Minimum 1 character.
delivery_firstname	Optional	Ship-to first name. Minimum 1 character.
delivery_lastname	Optional	Ship-to last name. Minimum 1 character.
delivery_address	Optional	The delivery address street number and name. Required for AVS by most gateways. Minimum 1 character.
delivery_address2	Optional	The second line of the delivery address. Required for AVS by most gateways. Minimum 1 character.
delivery_email	Optional	Ship-to email for the delivery address. Must be valid email format.
delivery_phone	Optional	Phone number for the delivery address. Numeric. Minimum 10 characters.
delivery_city	Optional	The delivery address city. Minimum 1 character.
delivery_state	Optional	The delivery address state or province. 2 letter abbreviation.
delivery_postal_code	Optional	The delivery address ZIP or postal code. Minimum 5 characters.
delivery_country	Optional	The delivery address country. 3 letter abbreviation. Default = USA

Sample Merchant HTML Code for Payment Request Form

The following code is an example of the form data that must be sent to the Global Transport Secure Page server to initiate the payment process:

```
<form name="form1" method="post" action="https://safe.sandbox-
gtpaysecure.net/securepayments/a1/cc_collection.php">

  <input type="hidden" name="CRESecureID"  value="XXXXXXXXXXXX" />

  <input type="hidden" name="return_url"
         value="https://mydomain.com/return.aspx" />

  <input type="hidden" name="content_template_url"
value="https://mydomain.com/content_template.aspx" />

  <input type="hidden" name="sess_id" value="e91dd8af53j35k072s0bubjtn7" />

  <input type="hidden" name="sess_name" value="session" />

  <input type="hidden" name="allowed_types"
         value="Visa|MasterCard|American Express" />

  <p>
    <label>Order Amount:
    <input type="text" name="total_amt" value="123.00" />
    </label>
  </p>

  <p>
    <label>Total Weight
    <input type="text" name="total_weight" value="7" />
    </label>
  </p>

  <p>
    <label>Order  ID:
    <input type="text" name="order_id" value="336" />
    </label>
  </p>

  <input type="hidden" name="lang" value="en_US" />

  <p>
    <label>Street Address:
    <input type="text" name="customer_address" value="1000 1st Av" />
    </label>
  </p>

  <p>
    <label>Email Address:
    <input type="text" name="customer_email" value="chuck@test.com” />
    </label>
  </p>

  <p>
    <label>Phone Number:
    <input type="text" name="customer_phone" value="1234567890"/>
    </label>
  </p>

  <p>
    <label>Postal Code:
    <input type="text" name="customer_postal_code" value="10101" />
    </label>
  </p>

  <p>
    <label>
    <input type="submit" name="submit" value="Submit" />
    </label>
  </p>

</form>
```

Transaction Success Response Page

Global Transport Secure Page returns the transaction response to the supplied return URL as name/value pairs in an HTTP $_GET (postback).

The following URL is an example of a postback from Global Transport Secure Page:

```
https://mydomain.com/return.aspx?order_id=6&code=000&msg=Success&error=&mPAN
=XXXXXXXXXXXX3801&name=Salvatore%20F%20Iozzia&type=Visa&exp=1012&ApprovalCod
e=012345&TxnGUID=1234567890&ProcTxnID=ABCDEFG&osCsid=ddc2e76644e8dde7308d426
06f7f7e74
```

The following table describes the values returned in the postback:

POST Value	*Description*
uID	Returned if it was used in the iFrame request. If used, the only parameters that will be returned are uID, code, error, and msg. The uID can be used to obtain all the values listed in this table by using the uID GET service. See uID on page 39 for more details.
action	Used to indicate the transaction was not completed. Possible values are: • **cancel –** the transaction has been canceled by the customer or has timed out • **duplicate –** the transaction is a duplicate of a previous transaction in the last 48 hours, based on order_id and total_amt values (when the action value is duplicate, Global Transport Secure Page also returns the transaction details from the original transaction.
order_id	Order number or ID.
code	Success or failure code. 000 = success.
error	Returns ‘true’ if there is an error.
msg	The error message if error is true. If error is false, value = Success
mPAN	Masked credit card number to be stored in the orders table.
name	Cardholder name to be stored in the orders table.
type	Credit card type (brand) to be stored in the orders table; detected based on the starting number or BIN range
exp	Credit card expiration date to be stored in the orders table.
osCsid	Unique session identifier from the merchant site. This is session_name sent in the POST data.

POST Value	*Description*
card_brand_selected	Selected credit card brand value.
CVVMatch	The value indicating whether the submitted CVV value matches the CVV value associated with the cardholder's account. The merchant application can examine CVVMatch results and determine whether to decline issuer-approved transactions if the CVV value does not match. If you choose not to accept an approved transaction due to the CVVMatch value, you must display the Declined page to the cardholder and immediately void the transaction using the reversal service. See Transaction Reversal on page 41 for information on using this service. See CVV Result Codes on page 51 for a list of result codes.
AVSMatch	The value indicating whether the submitted address matches the address associated with the cardholder's account. See on AVS Result Codes page 47 for values. The merchant application can examine AVSMatch results and determine whether to decline issuer-approved transactions if the AVS value does not match. If you choose not to accept an approved transaction due to the AVSMatch value, you must display the Declined page to the cardholder and immediately void the transaction using the reversal service. See Transaction Reversal on page 41 for information on using this service. See AVS Result Codes on page 49 for a list of result codes.
ApprovalCode	Approval code for the transaction.
TxnGUID	PNRef number identifying the transaction from the Global Transport Gateway.
ProcTxnID	Optional Diagnostic ID for transactions on specific gateway integrations.
CRE_Card_Token	A permanent card token for a stored credit card.
analysis_result	credit|CI

Note: You do not need to handle failed transactions. Global Transport Secure Page only responds to your merchant system when a payment is successful. In the event of a failed transaction, the customer is shown the payment page again with an error message. The customer can either retry the transaction or leave the page. To cancel the transaction, the customer clicks 'Cancel' or any other link in your template HTML.

Merchant Payment Template Page

Overview

The merchant payment template page contains all the template information and user session logic used for the presentation of the page. The page contains the value [[FORM INSERT]] at the location in the template that the HTML Clone™ technology inserts the credit card payment form. Pass the URL for your merchant payment template page to Global Transport Secure Page using the content_template_url post variable described in the section Payment Request Form on page 12.

To create a payment template page follow the steps below:

1. Create a page in your application, either by creating a new physical page or using your applications built-in page manager.
2. Specify the page title and any text you want to appear above and/or below the payment form.
3. Place [[FORM INSERT]] where ever you want the credit card form to appear on the page.

The merchant payment template page must meet these requirements:

- The URL of the payment template page can be any URL in your site.
- The URL for the payment template page must be accessible over HTTPS protocol.
- The URL for the payment template page must be directly accessible on the Internet.
- The payment template page must have the BASE tag with the URL of your HTTPS domain or use absolute URLs for CSS and image SRC values.

  Note: Safari on Mac requires absolute URLs.
- The CSS and images must be accessible via your HTTPS domain
- The payment template page must allow for the user session to be set via the URL.
- The payment template page should render using your application template logic and preferences.
- Your payment template page must render correctly without <script> and <iframe> tags. The HTML Clone™ will sanitize the HTML output from your payment template page and remove these tags.

Global Transport Secure Page uses the following classes, id's, and tags to style the payment form:

- **H2 –** Form title, for example Pay With Credit Card.
- **TABLE –** A table that creates the page layout and look. For example, background color and layout spacing.
- **TR –** Indicates a table row.
- **TD.main –** Field labels, for example Cardholder Name.
- **SPAN.main –** Indicates a group of elements on the page.
- **INPUT –** Input fields, for example the Cardholder Name input field.
- **SELECT –** Input fields with drop-down menus, for example the Card Type input field.
- **#submit –** Submit button.
  - **class=”disabled” –** Hides the submit button after it has been pressed.
- **#error_message –** DIV containing the error message.
- **SPAN.error_message –** Surrounds the error message text.

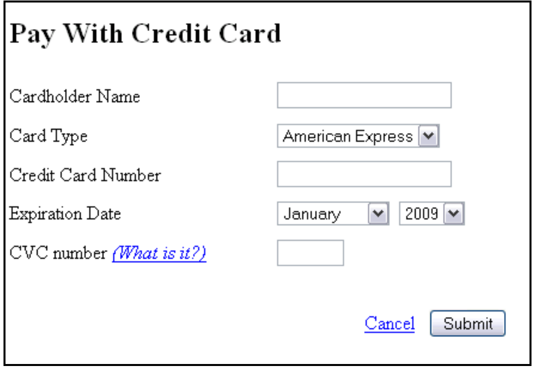
Sample Payment Template Form CSS

The following shows an example of CSS used to style the payment form:

```
<style type="text/css">
U{
    text-decoration:none;
}
TABLE TD{
    background-color:#333;
    padding-left:15px;
}
.main{
    color:#AAA;
    font-family:Arial, Helvetica, sans-serif;
}
.main a{
    color:#999;
    text-decoration:none;
}
.main a:hover{
    text-decoration:underline;
}
.main H2{
    color:#999;
}
.main input, .main select {
    border:2px solid #CCC;
    background-color:#777;
    padding:3px;
    color:#FFF;
    font-weight:bold;
}
.main select{
    cursor:pointer;
}
.main #submit{
    border:none;
    cursor:pointer;
}
</style>
```

The following images show the unstyled payment form and an example of a styled payment form:

Unstyled Payment Form



Pay With Credit Card

Cardholder Name

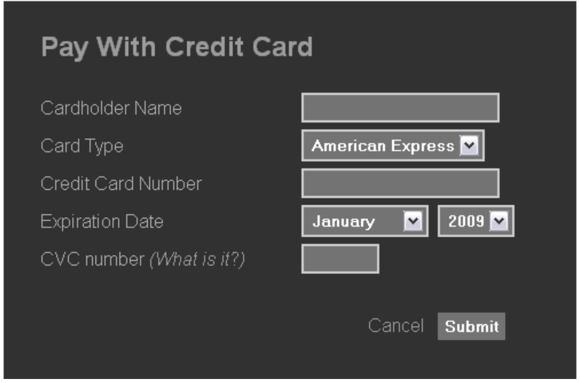
Card Type: American Express

Credit Card Number

Expiration Date: January 2009

CVC number (What is it?)

Styled Payment Form



Pay With Credit Card

Cardholder Name

Card Type: American Express

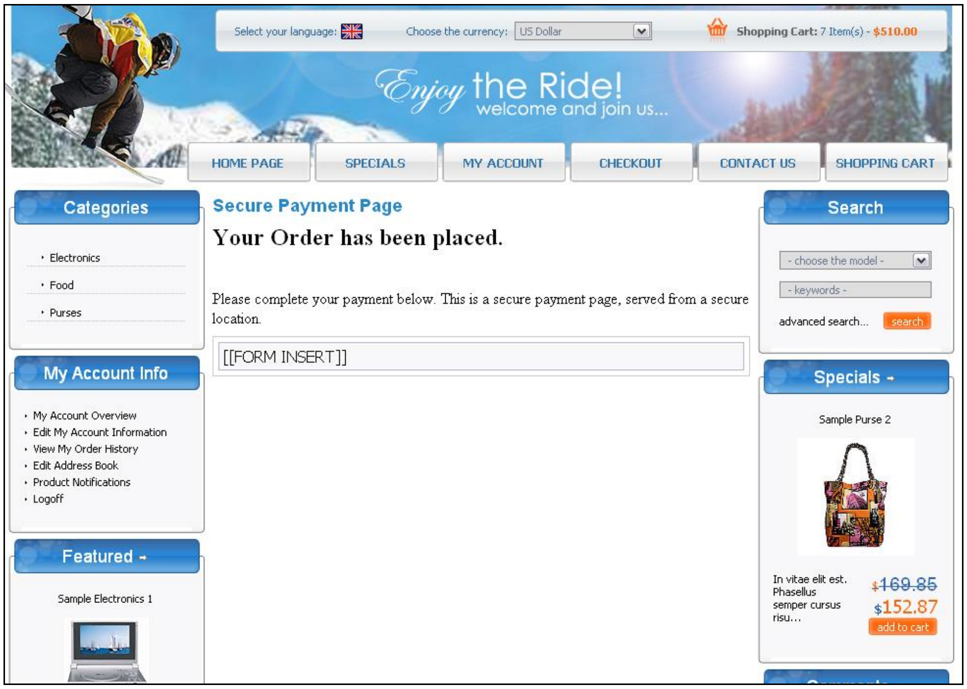
Credit Card Number

Expiration Date: January 2009

CVC number (What is it?)

Global Transport Secure Sample Page

The following images show the merchant payment template page.



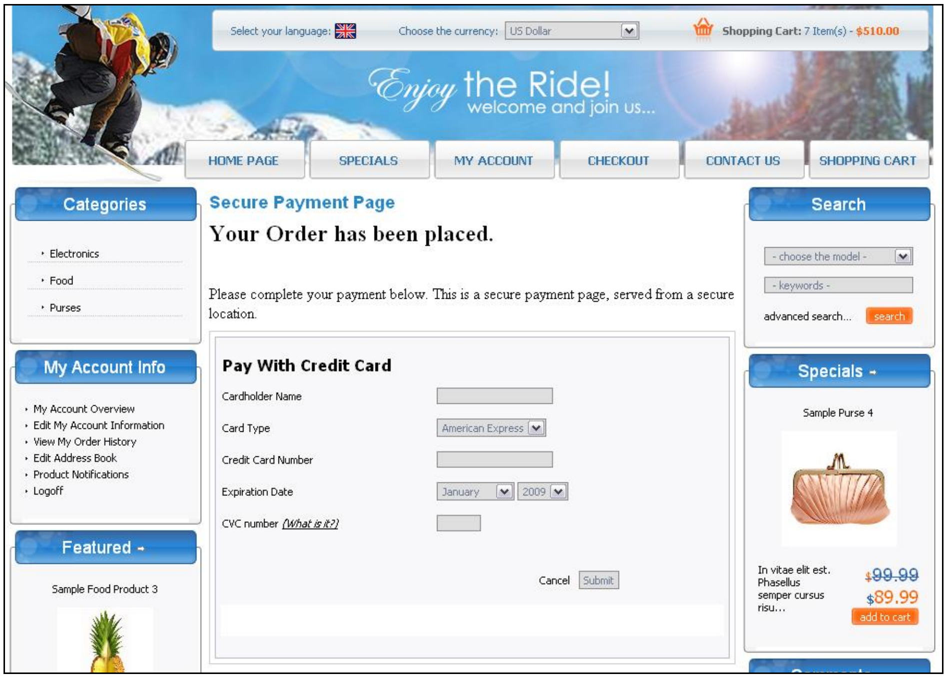
Secure Payment Page

Your Order has been placed.

Please complete your payment below. This is a secure payment page, served from a secure location.

[[FORM INSERT]]

The Global Transport Secure Page after it has been created using HTML Clone™:



Secure Payment Page

Your Order has been placed.

Please complete your payment below. This is a secure payment page, served from a secure location.

Pay With Credit Card

Cardholder Name	
Card Type	American Express
Credit Card Number	
Expiration Date	January 2009
CVC number (What is it?)	

Controlling the ERROR Message Suffix Text

If there is an error in the payment form submission, such as an invalid card number, the payment page displays an error. To customize the error message text, set a hidden DIV in your Payment Page Template HTML as shown below:

```
<div id=”errorMessageSuffix” style=”display:none;”>Please try again.</div>
```

Changing the content of the DIV changes the second sentence displayed when a transaction error occurs.

Customizing Fields

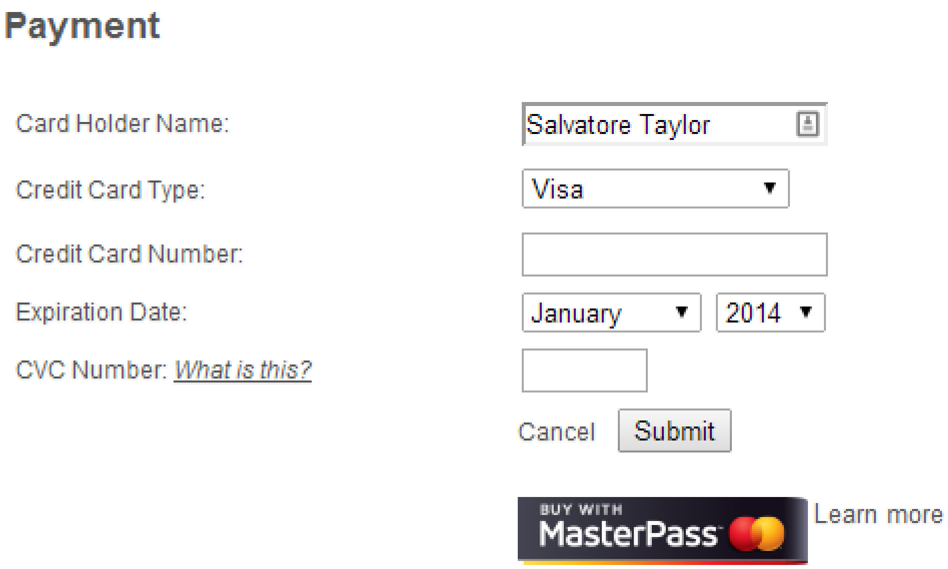
To prevent a field from appearing on the payment form for certain customers, you may supply a css_url override parameter that points to an alternative CSS file. For example, your page may use an alternative CSS file that hides the State field for customers in countries where it is not applicable. Do not hide any required fields, including those that you have set as required (see required on page 15).

Alternatively, you may also collect information that does not require secure processing through a separate form on your website and pass along the necessary fields in the transaction request.

MasterPass™ Implementation

Global Transport Secure Page provides merchants with the ability to add MasterPass as a payment option on their Global Transport Secure Page payment page.

Secure Page with MasterPass enabled:



Payment

Card Holder Name: Salvatore Taylor

Credit Card Type: Visa

Credit Card Number:

Expiration Date: January 2014

CVC Number: What is this?

If a payment card is successfully selected via the MasterPass process then Secure Page will submit the transaction to Global Transport. If the MasterPass process results in an error the user will be represented with the Secure Page payment page.

About MasterPass™

MasterPass is a free service that is a fast, simple and safe way to check out online. It cuts down on the time and effort it takes to buy the things you want and need. And because it's from MasterCard, you can trust that it's secure.

For additional information please go to:

http://www.mastercard.com/mc_us/wallet/learnmore/en/

MasterPass On-Boarding

To enable MasterPass, select the feature option as detailed in the Boarding Process section of this document. A merchant will be enabled for the service within one to two business days.

Once a merchant is enabled for MasterPass the payment option will appear on the payment form for all transactions.

MasterPass Shopping Cart Information

A feature of MasterPass is the presentation of a shopping cart to the end user. Secure Page will provide a default shopping cart if one is not provided as part of the initial request.

Default Shopping Cart Data

If the merchant does not provide shopping cart data then Secure Page will create a default cart with one item to be displayed on the MasterPass site.

If the order_desc parameter is present in the request that value will be utilized as the item description. If the order_desc parameter is not present then the item description is defaulted to "MasterPass Item".

Merchant Defined Shopping Cart Data

The merchant can optionally send the cart_data_url parameter in the Secure Page request that defines the location of a XML file on that contains the shopping cart data for the transaction. The XML file must be properly formed otherwise Secure Page will create a default shopping cart for the transaction.

The XML file must adhere to the MasterPass defined format and structure. A sample file is provided below.

Sample Shopping Cart XML File

```
<?xml version="1.0" ?>
<ShoppingCartRequest>
                <OAuthToken>TO BE INSERTED BY SECURE PAGE</OAuthToken>
        <ShoppingCart>
                <CurrencyCode>USD</CurrencyCode>
                <Subtotal>11900</Subtotal>
        <ShoppingCartItem>
                <Description>This is one item</Description>
                <Quantity>1</Quantity>
                <Value>1900</Value>
        </ShoppingCartItem>
        <ShoppingCartItem>
                <Description>Five items</Description>
                <Quantity>5</Quantity>
                <Value>10000</Value>
                <ImageURL>http://somemerchant.com/someimage</ImageURL>
        </ShoppingCartItem>
        </ShoppingCart>
</ShoppingCartRequest>
```

MasterPass Feature Interaction

The MasterPass feature is not compatible with the following Secure Page features:

- 3D Secure
- Tokenization

Cardholder Name and Billing Address

MasterPass returns cardholder name and billing address information after a user has selected a payment card. Secure Page will utilize the name returned by MasterPass in the transaction sent to Global Transport.

If the merchant passed the collect_address parameter in the request then Secure Page will send the billing address data returned by MasterPass in the transaction to Global Transport.

If the merchant did not pass the collect_address parameter but sent address data in the request then Secure Page will send the address data from the merchant in the transaction to Global Transport. In this case the address data from MasterPass is not sent.

Additional Notes

MasterPass Branding

It is the responsibility of the merchant to adhere to MasterPass branding guidelines when enabling the feature. These guidelines include the display of MasterPass Acceptance Mark on the merchant website as well as the acceptable contrast of the page background (e.g. the Secure Page Template Page) and the Buy with MasterPass checkout button.

MasterPass branding guidelines can be found at:

http://www.mastercard.com/mc_us/wallet/img/PayPass_Wallet_Services_Branding_Standards_v1.0_51712.pdf

Return to Merchant Links

The MasterPass page provides “return to merchant” links to the user. If these links are selected Secure Page will redirect the user back to the merchant’s website as if the user selected “cancel” on the payment page. See the descriptions for return_url and cancel_url parameters for details on this flow.

MasterPass Button CSS

Within the Secure Page form the MasterPass button is wrapped in a <div> with a CSS class name of “`masterpassButtonContainer`”. Using CSS in the template page the merchant can CSS styles and position the element.

Tokenization

Card on File

The Card on File service allows merchants to store a customer's card information at the Global Transport Gateway vault without performing a payment transaction. After storing, merchants may use this information to perform payment transactions using a corresponding PNRef or token number. The following steps describe how to use the Card on File service:

1. To store a card on file, send an HTTP POST as described in Payment Request Form on page 12. In the request, the CRE_Tokenize parameter must be given a value of **store_only** and the total_amt parameter must be left empty. This stores the card's information at the Global Transport Gateway vault without authorizing a payment.
2. In the response to the card-storing transaction, the value returned for the TxnGUID parameter is the PNRef number for this transaction. The value returned for the CRE_Card_Token parameter is a card token that can be used to authorize transactions. You can use either the PNRef or token number as the token to authorize payment transactions with the stored card.
3. To authorize a card-on-file payment transaction, send an HTTP POST to one of the following endpoints:
   - Production
     https://direct.gtpaysecure.net/direct/services/authorize/
   - Development and testing
     https://direct.sandbox-gtpaysecure.net/direct/services/authorize/

   Note: See Production Testing on page 10 for testing instructions and test credit card numbers.

   The following URL is an example of a card-on-file payment authorization request:

   ```
   https://direct.gtpaysecure.net/direct/services/authorize/?CRESecureID
   =XXXXX&CRESecureAPIToken=XXXXXX&total_amt=XXXXXX&CRE_Card_Token=
   XXXXXX&customer_id=XXXXXX&customer_zip_code=XXXXXX&ip_address=XXXXXX&
   order_desc=XXXXXX&orderId=XXXXXX&total_weight=XXXXXX&currency_code=
   XXXXXX&pass_thru=true
   ```

   The following table describes the parameters to send in order to request a card-on-file payment authorization:

Parameter Name	*Required*	*Description*
CRESecureID	Required	The GT Profile ID you received from the Global Transport Secure eCommerce Boarding site. Unique account number for Global Transport Secure Page.
CRESecureAPIToken	Required	The GT API Token you received from the Global Transport Secure eCommerce Boarding site.
total_amt	Required	The transaction amount to authorize or capture. Numeric, 2 decimal places.

Parameter Name	*Required*	*Description*
CRE_Card_Token	Required	The card token to authorize the transaction using the stored card. This value can be either: • The Global Transport Gateway PNRef number identifying the card on file (returned in the TxnGUID parameter of the card-storing transaction response). • The card token (returned in the CRE_Card_Token parameter of the card-storing transaction response). Use this value when requesting a custom format. The Global Transport Gateway uses the card information from the card-storing transaction to authorize payment.
customer_id	Optional	The customer identification number. 1 character minimum.
customer_zip_code	Optional	The billing address ZIP or postal code. 5 characters minimum.
ip_address	Optional	The customer's IP address.
order_desc	Optional	Text description of the purchase. 1 character minimum.
order_id	Optional	System value of the order or payment number. 1 character minimum.
total_weight	Optional	The total weight of the order. Determines if physical or digital goods. If no value is set, default is 0.
currency_code	Optional	The three-letter ISO currency code for the transaction. If no value is set, default is USD.
pass_thru	Required	Enables the ability to send the PNRef or token number directly to the Global Transport Gateway. This parameter takes the following value: **true**

The following is an example of a repeat sale authorization response in name-value pair format:

```
code=000&message=Success&TxnGUID=4CAE3ED05D7F1EBE51DECD9ACD6999604306
5422&ApprovalCode=098209
```

The following table describes the response parameters:

POST Value	*Description*
code	The response code. 000 indicates success.
message	The response message. For example, "success" or "error description".
TxnGUID	The transaction ID from the gateway.
ApprovalCode	The approval code from the gateway.
ERROR	Indicates that there was an error processing your request.

New Authorization with a Card on File

Once you have completed a Card Verify transaction with the Web Services you can send the CRE_Card_Token via a web service call to request new authorizations (charges) against the Card on File that the Token represents. Send the HTTP POST to the following endpoint:

https://direct.cresecure.net/direct/services/authorize/

For Sandbox, use the following endpoint:

https://direct.sandbox-cresecure.net/direct/services/authorize/

The POST uses the following parameters:

Post Value	***Type***	***Requirements***	***Description***
CRESecureID	Required	Provided by Global Transport	Unique Account Number for Web Services
CRESecureAPIToken	Required	Provided by Global Transport	API Token as part of the authentication chain
total_amt	Required	Numeric, Decimal 2 places	The amount to authorize or capture in the transaction
CRE_Card_Token	Required	Authorization	The PRNref# that was returned with your initial transaction
customer_id	Optional	Authorization/ Generation	ID of the customer
customer_zip_code	Optional	Authorization/ Generation	The ZIP/Postal code of the customer
ip_address	Optional	Authorization	The IP Address of the customer
order_desc	Optional	Authorization	A text overview of the order contents
order_id	Optional	Authorization	The ID or Number of the order in the merchant system
total_weight	Optional	Authorization	The weight of the order
currency_code	Optional	Authorization	The Currency Identifier, as specified from the gateway.
pass_thru	Optional	Authorization	No value or True Sets the pass thru ability to send the token directly to the gateway. Works only with the gateway's token.

For instance, a new token authorization might look like:

https://direct.cresecure.net/direct/services/authorize/?CRESecureID=XXXXX&CRESecureAPIToken=XXXXXX&total_amt=XXXXXX&CRE_Card_Token=XXXXXX&customer_id=XXXXXX&customer_zip_code=XXXXXX&ip_address=XXXXXX&order_desc=XXXXXX&order_id=XXXXXX&total_weight=XXXXXX&currency_code=XXXXXX

And the response might look like:

code=000&message=Success&TxnGUID=4CAE3ED05D7F1EBE51DECD9ACD69996043065422&ApprovalCode=098209

The response can include the following parameters:

Parameter	***Description***
code	000 for success
message	Message for transaction (example ”success” or “error description”)
TxnGUID	The transaction ID from the gateway
ApprovalCode	The approval code from the gateway
ERROR	Indication that there was an error processing your request

Repeat Sale

The Repeat Sale service allows merchants to process a sale transaction for a repeat customer without reentering the customer's card information. To obtain the card information, the Global Transport Gateway uses the PNRef or token number from a previous transaction you processed with the customer's card. Before attempting a repeat sale transaction, locate the previous transaction's PNRef number (returned in the TxnGUID parameter of the response) or token (returned in the CRE_Card_Token parameter of the response).

To authorize a repeat sale transaction, send an HTTP POST to one of the following endpoints:

- Production
  https://direct.gtpaysecure.net/direct/services/authorize/
- Development and testing
  https://direct.sandbox-gtpaysecure.net/direct/services/authorize/

  Note: See Production Testing on page 10 for testing instructions and test credit card numbers.

The following URL is an example of a repeat sale authorization request:

```
https://direct.gtpaysecure.net/direct/services/authorize/?CRESecureID=
XXXXX&CRESecureAPIToken=XXXXXX&total_amt=XXXXXX&CRE_Card_Token=XXXXXX&
customer_id=XXXXXX&customer_zip_code=XXXXXX&ip_address=XXXXXX&order_desc=XXX
XXX&orderId=XXXXXX&total_weight=XXXXXX&currency_code=XXXXXX&pass_thru=true
```

The following table describes the parameters to send in order to request a repeat sale authorization:

Parameter Name	***Required***	***Description***
CRESecureID	Required	The GT Profile ID you received from the Global Transport Secure eCommerce Boarding site. Unique account number for Global Transport Secure Form.
CRESecureAPIToken	Required	The GT API Token you received from the Global Transport Secure eCommerce Boarding site.
total_amt	Required	The transaction amount to authorize or capture. Numeric, 2 decimal places.
CRE_Card_Token	Required	The card token to authorize the transaction using the stored card. This value can be either: • The Global Transport Gateway PNRef number identifying the card on file (returned in the TxnGUID parameter of the card-storing transaction response). • The card token (returned in the CRE_Card_Token parameter of the card-storing transaction response). Use this value when requesting a custom format. The Global Transport Gateway uses the card information from the card-storing transaction to authorize payment.
customer_id	Optional	The customer identification number. 1 character minimum.
customer_zip_code	Optional	The billing address ZIP or postal code. 5 characters minimum.
ip_address	Optional	The customer's IP address.

Parameter Name	*Required*	*Description*
order_desc	Optional	Text description of the purchase. 1 character minimum.
order_id	Optional	System value of the order or payment number. 1 character minimum.
total_weight	Optional	The total weight of the order. Determines if physical or digital goods. If no value is set, default is 0.
currency_code	Optional	The three-letter ISO currency code for the transaction. If no value is set, default is USD.
pass_thru	Required	Enables the ability to send the PNRef or token number directly to the Global Transport Gateway. This parameter takes the following value: **true**

The following is an example of a repeat sale authorization response in name-value pair format:

```
code=000&message=Success&TxnGUID=4CAE3ED05D7F1EBE51DECD9ACD69996043065422&Ap
provalCode=098209
```

The following table describes the response parameters:

POST Value	*Description*
code	The response code. 000 indicates success.
message	The response message. For example, “success” or “error description”.
TxnGUID	The transaction ID from the gateway.
ApprovalCode	The approval code from the gateway.
ERROR	Indicates that there was an error processing your request.

Requesting a Custom/Legacy Token Format

Note: When requesting a custom/legacy token format, you must use the CRE_Card_Token value as the token. You cannot use the PNRef number when requesting a custom/legacy token format.

Depending on your token requirements, you can request one of the following custom token types:

- **custom** – Preserves the last four digits of the card number. The leading 12 digits are provided by the merchant.
- **mod10** – Preserves the last four digits and the first two digits of the card number. The middle four digits ensure that the token is not a valid card number. The token is mod10 validated.

Custom

For merchants with systems that cannot be altered to work with a new token value format, Global Transport Secure Page can return a custom 16-digit, numeric token. The custom token preserves the last four numbers of the card collected.

Global Transport Secure Page appends the last four digits of the card number to a 12-digit numeric string you provide. By using digits you supply, you can specify the format and leading numbers so that the tokens can be processed the same as existing tokens on your system.

For example, you post the number 000012345678 as a token slug. On your system, the four leading zeroes could indicate that the value is not an actual credit card number. Global Transport Secure Page adds the last four digits of the card number and returns the custom token 0000123456785454.

To request a custom token send the following additional values in the payment request along with the CRE_Tokenize parameter:

Parameter Name	***Required***	***Description***
token_type	Required for custom token	Send the following value to request a custom token: • custom – Sets the token format to custom.
token_slug	Required for custom token	The leading 12 digits of the custom token. 12 digits, numeric. Must be unique from other submitted values.

Mod10

Note: The mod10 token format will be implemented in a future release.

The mod10 token format provides a card token that preserves the last four and the first two digits of the credit card number. The middle four digits ensure that the token is not a valid card number. The entire token value is mod10 validated.

To request a mod10 token send the following values in the payment request along with the CRE_Tokenize parameter:

Parameter Name	***Required***	***Description***
token_type	Required for Mod10 token	Send the following value to request a mod10 token: • mod10a – Sets the token format to mod10.
customer_id	Required for Mod10 token	Send a unique customer ID for each customer.

The mod10 token request returns a card token in the transaction response in name value pair format, tokenId=371-4199995849941111-0113.

The returned token strings are delimited using - characters into the following three values:

- **Customer ID** – The first value is the customer ID that was submitted with the token request.
- **Mod10 String** – The second value is the mod10 string. The first two digits and the last four digits correspond to the original card number.
- **Expiration Date** – The third value is the expiration date of the tokenized card.

Global Transport Secure eCommerce Direct Services

Global Transport Secure eCommerce provides multiple direct services for merchants to conduct repeat transactions, validate transactions, reverse transactions, and send merchant and transaction data securely. Direct services are used for your application to communicate with our platform. Direct services do not present any customer facing web content.

Transaction Validation

The Transaction Validation service allows you to query Global Transport to verify that a payment was successfully processed. This enables you to automate verification of orders marked as paid to prevent payment spoofing. To validate a transaction, send an HTTP POST to one of the following endpoints:

- Production
  https://direct.gtpaysecure.net/direct/services/validation/
- Development and testing
  https://direct.sandbox-gtpaysecure.net/direct/services/validation

Note: The production URL requires a trailing slash, but the development and testing URL does not.

Note: See Production Testing on page 10 for testing instructions and test credit card numbers.

The following URL is an example of a transaction validation request:

```
https://direct.gtpaysecure.net/direct/services/validation/?CRESecureID=XXXX&
CRESecureAPIToken=XXXX&order_id=XXXX&total_amt=XX.XX
```

The following table describes the parameters used to validate transactions:

POST Value	*Required*	*Description*
CRESecureID	Required	The GT Profile ID you received from the Global Transport Secure eCommerce Boarding site. Unique account number for Global Transport Secure Page.
CRESecureAPIToken	Required	The GT API Token you received from the Global Transport Secure eCommerce Boarding site. API Token as part of the authentication chain.
order_id	Required	System value of the order or payment. Minimum 1 character.
total_amt	Required	The amount authorized or captured in the transaction to validate. Numeric, 2 decimal places.
trans_id	Optional	PNRef number from the Global Transport Gateway identifying the transaction you want to validate. Alphanumeric.
response_type	Optional	Sets the format for the response. Valid values are: • **nvp** – name value pair (default) • **xml** – XML format • **json** – json format

An example of a transaction validation response is shown below in name-value pair format:

```
order_id=XXXX&order_id_match=YES&total_amt=30.4&total_amt_match=YES&trans_id
=&trans_id_match=NO&status=success
```

The following table describes the parameters of the transaction validation request response:

POST Value	***Description***
order_id	Order ID sent to the service.
order_id_match	Result of match query for the order ID. Possible values are: • **YES** • **NO**
total_amt	Total transaction amount sent to the service.
total_amt_match	Result of the match query for the amount of the transaction associated with the order ID. Possible values are: • **YES** • **NO**
trans_id	Transaction ID sent to the service. Possible values are: • Your value • **NULL**
trans_id_match	Result of match query for the amount of the transaction associated with the order ID. Possible values are: • **YES** • **NO** • **NULL**
status	Result of the transaction based on the order ID match. Possible values are: • **success** • **failure**
ERROR	Indicates an error during request processing.
Message	Error description.

Card Verify

A Card Verify transaction confirms that your customer has entered a valid credit card and returns a token that you can use for future transactions with that customer. This section will show you how to collect a card from your customer in a Card Verify transaction, then follow up with a Card on File transaction.

Building a Card Verify Transaction

Card Verify transactions are built in the same manner as normal payment transactions, with a POST Request. To initiate a Card Verify transaction instead of a regular payment, do not pass the **trans_type** parameter. Instead, pass cre_tokenize with a value of "**store_only**". You may include any other parameters that you would normally include in a regular sale transaction.

For example, in a Secure Link integration, you should delete the line in the Payment Form Request:

```
<input type="hidden" name="trans_type" value=" auth_capture" />
```

And replace it with:

```
<input type="hidden" name="cre_tokenize" value=" store_only" />
```

Card Verify Response

A Card Verify response is returned in the same manner as a normal transaction, with the additional parameter, **CRE_Card_Token**. The value of this parameter is a unique token identifier that ties this credit card to your merchant account. Your system must collect and store this token in order to use the features of Card on File. Storing this token is not the same as storing a credit card number for the purposes of PCI Compliance. If you would like to present your returning customer with the option to choose between several saved cards, you should also save the fields that identify the card, such as **mPAN**, the last four digits of the credit card number, **name**, the cardholder name, **type**, the credit card brand, and **exp**, the expiration date.

Pre-auth complete through Direct Services

To finish an auth_only transaction without presenting another payment form to the cardholder, you may use this direct services call. Send an HTTP GET to the following endpoint:

https://direct.gtpaysecure.net/direct/services/authorize/

For the sandbox, use the following endpoint:

https://direct.sandbox-gtpaysecure.net/direct/services/authorize/

A URL for the transaction validation service will look something like this:

https://direct.gtpaysecure.net/direct/services/authorize?CRESecureID=cre1234567&CRESecureAPIToken=6f0b5e3e9bdb75b0425987b717323661&total_amt=100.00&order_id=000001&trans_id=1234567

The URL should contain the following parameters:

Parameter	***Type***	***Requirements***	***Description***
CRESecureID	Required	Provided by Global Transport	Unique Account Number for the Secure Pay
CRESecureAPIToken	Required	Provided by Global Transport	API Token as part of the authentication chain
total_amt	Required	Numeric, Decimal 2 places	The dollar amount of the auth_only transaction. This amount cannot be different from the original transaction.
order_id	Required	Alphanumeric	The original order ID.
trans_id	Required	Alphanumeric	The original transaction ID.

Secure Page will return a response in this format:

code=000&message=Success&mPAN=************1111&type=VISA&TxnGUID=4D8A5E36C2C06F1B6C4D8AB8D7F0C18BCAB05453

The possible response parameters are as follows:

Post Value	***Description***
code	Transaction code.
message	Success or failure.
mPAN	The masked PAN of the card used in the original transaction
type	Card type of the original transaction.
TxnGUID	Unique identifier for the reversal transaction.
ApprovalCode	Gateway message

uID

The uID service provides a way for merchants to send sensitive merchant and transaction data directly to Global Transport in order to avoid it being intercepted when passed through the customer’s browser. Using the uID service involves an HTTP POST before the transaction is processed to obtain the uID and an HTTP GET after the transaction has been processed to obtain the transaction details. The following steps describe how to use the post uID service:

1. Send an HTTP POST with the standard form request parameters, as described in Payment Request Form POST Values on page 12, to one of the following endpoints:

   - Production
     https://direct.gtpaysecure.net/direct/services/request/init/

   - Development and testing
     https://direct.sandbox-gtpaysecure.net/direct/services/request/init/

     Note: See Production Testing on page 10 for testing instructions and test credit card numbers.

   The following URL is an example of a uID request:

   ```
   https://direct.gtpaysecure.net/direct/services/request/init/?
   collectAddress=0&action=buildForm&merchPass=XXXXXXXXXX&allowed_types=
   Visa|MasterCard|American Express|Discover&formType=&
   paymentType=&address=112 Krog Street&address2=Suite 19&city=Atlanta&
   state=GA&zip=33615&lang=en_US&customer_id=877133&order_desc=
   31x NewPaper&customer_email=johndoe@sample.com&analysis=&required=&
   name=Michael Presley&amount=1.00&currency_code=USD&sessionId=064402&
   orderId=520585
   ```

2. Global Transport responds by sending you a uID, which is a unique identifier that corresponds to the form request data you sent.

3. Perform the Payment Form Request as detailed in Payment Request Form on page 12. Send the uID instead of the standard form request variables.

   The following URL is an example of a form request using a uID:

   ```
   https://safe.sandbox-gtpaysecure.net/hpf/1_1/?uID=XXXXXXXXXXXXXXXX
   ```

4. After the customer has submitted the payment information and the transaction has been processed, send an HTTP GET containing the parameters described below to one of the following endpoints to obtain the transaction results:

   - Production
     https://direct.gtpaysecure.net/direct/services/request/query/

   - Development and testing
     https://direct.sandbox-gtpaysecure.net/direct/services/request/query/

     Note: See Production Testing on page 10 for testing instructions.

   The following is an example of a URL requesting transaction results using a uID:

   ```
   https://safe.sandbox-gtpaysecure.net/direct/services/request/query
   ?CRESecureID=CLINIX&CRESecureAPIToken=56C64808B83C9186D7F31ABA93DCAE2
   8&uID=ABCDEF1234ABCDEF1234ABCDE1234
   ```

Send the following parameters with your HTTP GET to obtain the transaction results:

Parameter Name	***Required***	***Description***
uID	Required	The same uID used to perform the transaction.
CRESecureID	Required	The GT Profile ID you received from the Global Transport Secure eCommerce Boarding site. Unique account number for Global Transport Secure Page.
CRESecureAPIToken	Required	The GT API Token you received from the Global Transport Secure eCommerce Boarding site.

Transaction Reversal

Use the Transaction Reversal service to void or refund a transaction. To perform a transaction void or refund, send an HTTP GET to one of the following endpoints:

- Production
  https://direct.gtpaysecure.net/direct/services/reversal/
- Development and testing
  https://direct.sandbox-gtpaysecure.net/direct/services/reversal/

  Note: See Production Testing on page 10 for testing instructions and test credit card numbers.

The void transaction can be used if the transaction has not already been settled. If the transaction has been settled, Global Transport Secure Page returns the following message:

“The+original+transaction+has+already+been+submitted+for+settlement.+To+reverse+the+transaction+please+submit+a+Refund+or+Sale+transaction”

In this case, perform a refund transaction.

The following URL is an example of a transaction reversal request:

```
https://direct.sandbox-gtpaysecure.net/direct/services/reversal?CRESecureID=
cre666855972SB&CRESecureAPIToken=6f0b5e3e9bdb75b0425987b717323661&
reversal_type=refund&transaction_id=4D8A59E6DD1EF52141D944CBC23BC91AEF125485
&reversal_amount=0.05&disable_amt=&submit=Reverse&orderId=121121
```

The following table describes the parameters to send in order to reverse a transaction:

Parameter Name	*Required*	*Description*
CRESecureID	Required	The GT Profile ID you received from the Global Transport Secure eCommerce Boarding site. Unique account number for Global Transport Secure Page.
CRESecureAPIToken	Required	The GT API Token you received from the Global Transport Secure eCommerce Boarding site.
reversal_type	Required	The reversal type to perform. Valid values are: • **void** – voids a transaction if it is not already settled • **refund** – performs a return transaction; requires reversal_amount input
transaction_id	Optional	PNRef number from the Global Transport Gateway identifying the transaction you want to reverse. Alphanumeric.
reversal_amount	Required if reversal_type =refund	The dollar amount of the reversal. Numeric, 2 decimal places.
orderId	Required	System value of the order or payment number. Minimum 1 character.

The following is an example of a transaction reversal response in name-value pair format:

```
code=000&message=Success&reversal_type=refund&TxnGUID=4D8A5E36C2C06F1B6C4D8A
B8D7F0C18BCAB05453
```

The following table describes the response parameters:

POST Value	***Description***
code	The response code. 000 indicates success.
message	The response message. For example, “success” or “error description”.
reversal_type	The reversal type performed. Either “void” or “refund”.
TxnGUID	The transaction ID from the gateway.

Error Messages

The following sections list error messages that may be returned during transactions using Global Transport Secure Page:

Global Transport Secure Page

These error messages may be returned by Global Transport Secure Page:

In form validation messages

Message	*Description*
The cardholder name cannot be blank.	The customer left the cardholder name field blank.
The credit card number cannot be blank.	The customer left the credit card number field blank.
Invalid credit card number.	The credit card number entered is not a valid credit card number.

Processing Messages

Message	*Description*
[110] Missing or unknown profile.	The Global Transport Secure Page ID sent in does not result is a successful read of the Merchant Profile.
[111] Authentication failure.	Global Transport Secure Page failed to authenticate Merchant credentials.
[120] No validation domains found in the profile.	No valid request domains were found for the Merchant.
[121] Domain validation check failed.	HTTP_REFERER does not match a request domain.

Transaction Validation Direct Web Service

Error messages returned by the transaction validation direct web service use the following format:

Message	*Description*
Required information is missing; XXXXX	The transaction validation request message did not include the required information indicated by the returned code.
ERROR: Invalid Global Transport Secure account credentials.	The Global Transport Secure account credentials sent in for authorization are invalid.

In this case, XXXXX is an error code.

The following formatting rules apply to these messages:

- Known Global Transport Gateway error messages return in parenthesis (XX).
- Unknown Global Transport Gateway error messages return in double parentheses ((XXXX)). The following section explains these error messages in greater detail.

Global Transport Gateway Response Codes

These error messages may be returned by Global Transport Gateway:

Value	Description
-1	There was an error completing your transaction to the Database. Timeout Reversal Attempted.
0	Approved
3	Invalid Transaction Type Unsupported Transaction Type
4	Invalid Amount Invalid Cash Back Amount
5	Invalid Merchant Info
7	Account number specified does not match original. Swiped and Card Present transactions are not supported in Card Not Present markets. Invalid Card Number. Invalid CVNumber Invalid Expiration Date. IVR not supported for this transaction KIOSK is an invalid entry mode for a non-sale transaction type. Kiosk not supported for given Industry Field Format Error Unsupported AppID Unsupported industry for Secure 3D. Unsupported card type for Secure 3D.
12	Decline ITEM VOIDED PREAUTH VOIDED Invalid Adjustment Request Cannot Complete a Voided PreAuth
19	Original Transaction Reference not found - PNRef or Approval Code Original Transaction ID Not Found. Original Transaction ID Not Found. Original Transaction Reference not found - PNRef or Approval Code
23	Invalid Account Number
26	Invalid PNRef
31	Cannot perform multiple captures on a PreAuth.
75	Visa Debit card acceptance not enabled.
76	Cannot Void a Returned Sale.
80	The original transaction has already been submitted for settlement. To reverse the transaction please submit a Refund or Sale transaction.
103	Error Reading Response From Host
104	Error Processing Host Transaction.
107	There was an error communicating with the Tandem

Value	***Description***
108	Void Error
110	Duplicate Transaction
113	Requested Refund Exceeds Available Refund Amount
114	Cannot refund a voided transaction.
115	Cash Back Amount cannot exceed total Amount. Sum of Tax, Tip, and Cash Back amount cannot exceed total Amount. Tax Amount cannot exceed total Amount. Tip Amount cannot exceed total Amount.
116	Unsupported Card Type
117	Only Sales, Repeat Sales, Force Captures, and Post Authorizations can be refunded.
118	The amount of a Pre-Auth Complete (Capture) must be less than or equal to the original amount authorized. Please retry.
119	The amount of a Pre-Auth Complete (Capture) must be equal to the original amount authorized. Please retry.
120	Pre-Auth transaction has expired per Card Brand operating regulations.
200	A Partial Authorization of a pre-paid card. This is considered an *Approved* transaction. Check the **ApprovedAmount** field in ExtData for the amount approved.
1000	General Exception Error Inserting into the DB Invalid characters in field Invalid Check Type Invalid Date Format Invalid Entry Mode Invalid Field Length IDNumber must be alphanumeric Personal checks must include valid ID between 4-24 alphanumeric characters Invalid ID Type Invalid Mag Data An attempt was made to reverse a non reversable transaction type. Invalid Parameter Data. Invalid SignatureData Invalid SignatureType Invalid Tip Amount Invalid transaction. The total amount of the transaction is required Card Expiration Date is required Card Number is required Key Serial Number is required The MAC value is required The data encoded on Track 2 is required Required PIN Block (Encrypted Personal Identification Number) Transaction Type is required Voucher Number is required Original transaction already has signature

Value	Description
1001	Invalid Login Information
1002	AVS Only transactions are not supported in E-Commerce markets. Debit/EBT Return transactions must provide the PNRef from the original Sale. Please retry.
1005	Service FSAHRA not allowed Service Debit not allowed Transaction Type Not Allowed
2000	Password Expired.

Troubleshooting

ERROR: ((1000)) and ERROR: ((1001))

The Global Transport Gateway typically returns ERROR: ((1000)) and ERROR: ((1001)) messages after you change your Global Transport Virtual Terminal password. You can stop these messages by re-boarding your website.

To stop ERROR: ((1000)) and ERROR: ((1001)) messages:

1. Navigate to the following boarding site URL.

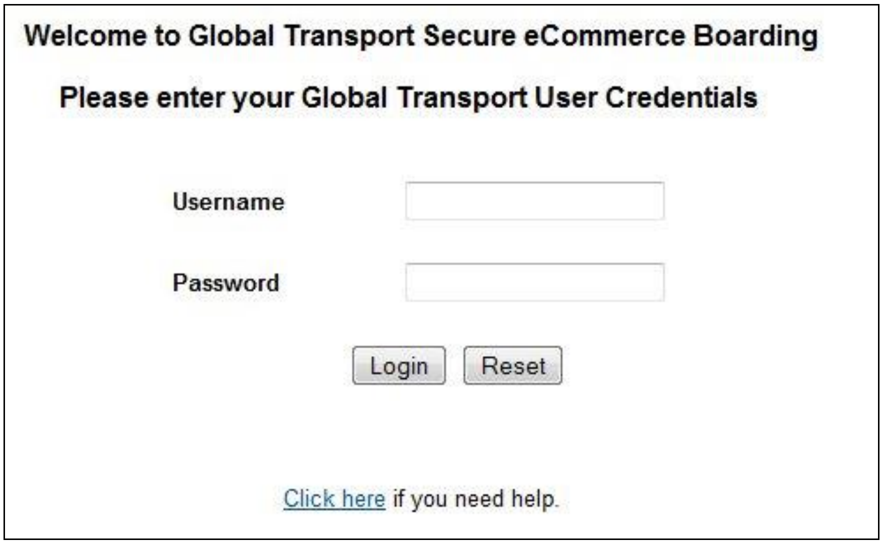
   For production, use the following URL:

   https://manage.gtpaysecure.com

   For sandbox testing, use the following URL:

   https://manage-sandbox.gtpaysecure.com/

   The following screen displays:



Welcome to Global Transport Secure eCommerce Boarding

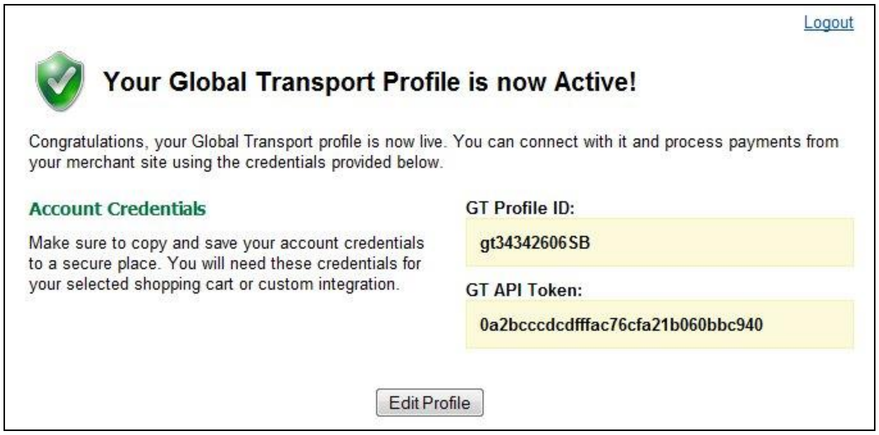
Please enter your Global Transport User Credentials

Click here if you need help.

2. Enter your Global Transport user name and password and click **Login**.

3. Click **Continue** through the screens that display.

   The following screen displays:



Logout

Your Global Transport Profile is now Active!

Congratulations, your Global Transport profile is now live. You can connect with it and process payments from your merchant site using the credentials provided below.

Account Credentials

Make sure to copy and save your account credentials to a secure place. You will need these credentials for your selected shopping cart or custom integration.

GT Profile ID: gt34342606SB

GT API Token: 0a2bcccdcdfffac76cfa21b060bbc940

You have successfully re-boarded your website. You should stop receiving ERROR: ((1000)) and ERROR: ((1001)) messages. If you continue to receive these messages, contact technical support. See Support on page 1 for contact information.

Using Global Transport Secure Page with WordPress

Web sites built using WordPress cause a conflict with the name parameter returned on the transaction success response page. The parameter name is a reserved URL parameter in WordPress. See Transaction Success Response Page on page 19 for a complete list of response parameters.

To use Global Transport Secure Page with WordPress, you must create a page separate from the WordPress application to use as the return_url parameter in the payment request form POST. This page can then process the response or redirect the response values to the WordPress site without using the name parameter.

AVS Result Codes

Global Payments returns one of the following codes as part of the Authorization Response for AVS.

American Express

Code	Description
A	Billing address only correct.
N	No, billing address and postal code are both incorrect.
R	System unavailable; Retry.
S	SE not allowed AAV function.
U	Information unavailable.
Y	Yes, billing address and postal code are both correct.
Z	Billing postal code only correct.

Discover

Code	Description
A	All digits match, five-digit ZIP code.
N	Nothing matches.
S	AVS not supported at this time.
T	Nine-digit ZIP code matches, address does not.
U	Retry, system unable to process.
W	No data from issuer/authorization system.
X	All digits match, nine-digit ZIP code.
Y	Address matches, ZIP code does not.
Z	Five-digit ZIP code matches, address does not.

MasterCard

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

Code	Description
W	For U.S. addresses, nine-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not.
X	For U.S. addresses, nine-digit postal code and address match; for address outside the U.S., postal code and address match.
Y	For U.S. addresses, five-digit postal code and address matches.
Z	For U.S. addresses, five-digit postal code matches, address does not.

Visa

Code	Description
A	Address matches, ZIP does not.
B	Street addresses match. Postal code not verified due to incompatible formats.
C	Street address and postal code not verified due to incompatible formats.
D	Street addresses and postal codes match. (International transactions.)
G	Address information not verified for international transaction.
I	Address information not verified. (International transactions.)
M	Street address and postal code match. (International transactions.)
N	No match.
P	Postal code match. Street address not verified due to incompatible formats.
R	Retry: System unavailable or timed out.
U	Address not verified for domestic transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, or Visa performs AVS on behalf of the issuer and there was no address record on file for this account.
Y	Street address and postal code match.
Z	Postal/ZIP matches; street address does not match or street address not included in request.

CVV Result Codes

If submitted with an approved transaction, Global Payments includes the Visa CVV2, MasterCard CVC2, American Express CID, and Discover CID result codes as part of the Authorization Response Messages. The result code is a one-character alphanumeric field. Valid values are listed in the table below.

Code	***Description***
M	Match
N	No match
P	Not processed
S	CVV2/CID should be on the card, but the merchant has indicated that CVV2/CID is not present (Visa and Discover only)
U	Issuer is not certified CID was not checked (American Express only).

Note: There is no CAV2 result code value for JCB.

PCI Compliance

Note: If you follow the proper procedures for Global Transport Secure Page implementation, your web site is outside of the scope of PCI compliance. This section is provided for your information only.

Overview

This section describes the requirements for compliance with the Payment Card Industry (PCI) Data Security Standards. Each merchant is responsible for complying with these requirements.

Global Payments has implemented several security features, which were assessed for compliance with the Payment Card Industry Data Security Standards (PCI/DSS). Although Global products are developed with security in mind, you are required to follow the following guidelines to maintain PCI compliance:

- Create PCI-compliant complex passwords
- Control access to cardholder data, via unique user names and passwords
- Use PCI-compliant lockout settings
- Use PCI-compliant wireless settings
- Avoid storing cardholder data on Internet-accessible systems
- Practice secure remote network access

For a list of the most up-to-date requirements for meeting PCI/DSS standards, visit **https://www.pcisecuritystandards.org/**.

Complex Passwords

Global Payments supports complex password functionality. To implement products in a PCI-compliant manner, all passwords used must conform to PCI standards. These include but are not limited to:

- Removing inactive user accounts at least every 90 days
- Changing user passwords at least every 90 days
- Requiring a minimum password length of at least eight characters
- Using passwords containing both numeric and alphabetic characters
- Requiring individuals to submit new passwords that are different from any of the last four passwords used
- Applying complex passwords to administrative accounts to reduce the risk of compromise
- Locking out the user ID for 30 minutes after six repeated access attempts

Login names and their associated passwords may be added, deleted, or modified via the relevant password section.

Controlled Access

Access to cardholder data, and any PCs or servers where they may be stored, as well as any PCs or servers running payment software, should be controlled via unique user names and PCI-compliant complex passwords.

Group, shared, and generic accounts or passwords should not be used. Administrative accounts should not be used for application login or access to cardholder data.

Cardholder Data Storage

Global Payments does not recommend or require that cardholder data be stored on any Internet accessible system. All PCs connected to the Internet pose a high risk of compromise unless they are properly isolated and controlled with PCI-compliant firewall and anti-virus applications.

Internet connections should be protected with a firewall to prevent direct Internet attacks. The network should have a proper Internet architecture with DMZ (if applicable) to segment Internet connected systems. Verify that any databases or credit card data are properly protected and encrypted.

Vendor Release Agreement

To comply with PA-DSS guidelines, the merchant should abide by the following guidelines:

> Acceptance of a given payment application by the PCI Security Standards Council, LLC (PCI SSC) only applies to the specific version of that payment application that was reviewed by a PA-QSA and subsequently accepted by PCI SSC (the “Accepted Version”). If any aspect of a payment application or version thereof is different from that which was reviewed by the PA-QSA and accepted by PCI SSC – even if the different payment application or version (the “Alternate Version”) conforms to the basic product description of the Accepted Version – then the Alternate Version should not be considered accepted by PCI SSC, nor promoted as accepted by PCI SSC.
>
> No vendor or other third party may refer to a payment application as “PCI Approved” or “PCI SSC Approved”, and no vendor or other third party may otherwise state or imply that PCI SSC has, in whole or part, accepted or approved any aspect of a vendor or its services or payment applications, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a PA-DSS letter of acceptance provided by PCI SSC. All other references to PCI SSC’s approval or acceptance of a payment application or version thereof are strictly and actively prohibited by PCI SSC.
>
> When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC’s goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the payment application vendor or the functionality, quality, or performance of the payment application or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or noninfringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC, shall be provided by the party providing such products or services, and not by PCI SSC or any payment brands.

Safeguarding Cardholder Account Information

The following information is provided by Global Payments Inc. as an informational tool to help you stay informed of pertinent industry information, Visa® and MasterCard® compliance requirements, and other information about the electronic payments industry. Web sites for the following topics are provided for your reference:

Global Payments Card Acceptance Guide:

https://www.globalpaymentsinc.com/GPDB/AccessDOC.aspx?SubDoc_ID=211

Merchant Requirements for Securing Cardholder Information:

https://www.globalpaymentsinc.com/GPDB/AccessDOC.aspx?SubDoc_ID=593

And

https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

Receipts:

http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/cardTransRequire.html

Payment Card Industry Data Security Standards for Merchants (CISP) (SDP):

http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/PCI_merchants.html

Merchant Use of Third Parties:

http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/merchant-use-third-parties.html

PCI Standard: Overview for Merchants and Service Providers:

https://www.pcisecuritystandards.org/

https://www.globalpaymentsinc.com/USA/customerSupport/industryInit/PCI_DSS_About_Homepage.html

Payment Card Industry Data Security Standards for Service Providers (CISP) (SDP):

http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/PCI-service-provider.html

Other Compliance Information

MasterCard and Diners Club International Changes:

US Merchants:

http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/mc-dc-us.html

Canadian Merchants:

http://www.globalpaymentsinc.com/Canada/customerSupport/industryInit/diners_club.html

Visa: Verified by Visa:

http://usa.visa.com/merchants/risk_management/vbv.html

Rules for Accepting MasterCard:

http://www.mastercard.com/us/merchant/support/rules.html

Card Acceptance and Chargeback Management Guide for Visa Merchants:

http://usa.visa.com/merchants/new_acceptance/merchant_responsibility.html

American Express CAPN Project:

http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/amex-CAPN.html

Additional useful sites:

http://www.mastercard.com/us/merchant/security/data_security_rules.html http://usa.visa.com/merchants/new_acceptance/merchant_responsibility.html

https://masterpass.com/SP/Merchant/OperatingRules

Global Transport Secure eCommerce online support:

http://quickstart.hps.controlscan.com/gt/gt-helper/
https://quickstart.hps.controlscan.com/gt/

Index