First Data Global Gateway Integration Guide Connect 2.0

Version 1.2.1

First Data Global Gateway

INTEGRATION GUIDE
CONNECT 2.0
VERSION 1.2.1

Contents

1 Introduction

First Data Global Gateway Connect 2.0 is a simple payment solution for connecting an online store to the powerful First Data Global Gateway.

Connect 2.0 manages all of your interactions with transaction processors and financial institutions.

This document describes how to integrate your website with Connect 2.0 and provides step-by-step instructions on how to quickly start accepting payments from your website.

1.1 Integration Roadmap

This section is intended to be a guide for the user to identify key sections within the integration guide to implement Connect 2.0 within the First Data Global Gateway (FDGG). Internal/external Hyperlinks are identified within the Document Section column that link to internal sections within this document or external users guides within the First Data web site(s).

The table below focuses on the steps and document sections for New and Existing Connect Merchants.

1.1.1 Existing Connect Merchant

Step	Action/Description	Involves	Document Section
1	Download FDGG Virtual Terminal Guide	Merchant	Hyperlink
2	Review changes in Connect 2.0	Merchant	Changes in Connect 2.0
3	Review Inbound Interface Fields	Merchant	Standard Fields
4	Review Outbound Interface Fields	Merchant	Transaction Response
5	Determine Web Service Environment and apply appropriate changes	Merchant	ASP Example PHP Example JSP Example Supporting Library Utilities
6	Update Test Connect 2.0 Settings within the FDGG Virtual Terminal	Merchant	First Data Global Gateway Setup
7	Test within the FDGG Test Area (CTE)	Merchant	Testing Transactions
8	Contact First Data to update production store to Connect 2.0	Merchant, First Data	
9	Update Production Connect 2.0 Settings within the FDGG Virtual Terminal	Merchant	First Data Global Gateway Setup
10	Deploy Connect 2.0 Implementation to Production	Merchant	
11	Validate Connect 2.0 Production Implementation	Merchant	Testing Transactions
12	Contact First Data Support Center if you have any questions.	Merchant	Contact Information

1.1.2 New Connect Merchant

Step	Action/Description	Involves	Document Section
1	Download FDGG Virtual Terminal Guide	Merchant	Hyperlink
2	Review Introduction Section	Merchant	Introduction
3	Review Inbound Interface Fields	Merchant	Standard Fields
4	Review Outbound Interface Fields	Merchant	Transaction Response
5	Determine Self-Hosted or First Data Hosted Options	Merchant	Form Hosting Options
6	Determine Payment Mode	Merchant	Payment Modes
7	Determine Web Service Environment and apply appropriate changes	Merchant	ASP Example PHP Example JSP Example Supporting Library Utilities
8	Contact First Data to update test store to Connect 2.0	Merchant, First Data	
9	Update Test Connect 2.0 Settings within the FDGG Virtual Terminal	Merchant	First Data Global Gateway Setup
10	Test within the FDGG Test Area (CTE)	Merchant	Testing Transactions
11	Contact First Data to update production store to Connect 2.0	Merchant, First Data	
12	Update Production Connect 2.0 Settings within the FDGG Virtual Terminal	Merchant	First Data Global Gateway Setup
13	Deploy Connect 2.0 Implementation to Production	Merchant	
14	Validate Connect 2.0 Production Implementation	Merchant	Testing Transactions
15	Contact First Data Support Center if you have any questions.	Merchant	Contact Information

1.2 Understanding Electronic Payment Processing

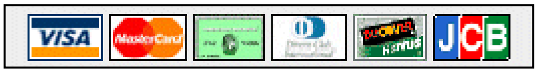
The First Data Global Gateway Connect 2.0 secure payment gateway is capable of securely receiving, storing, processing, and sending online transactions to a bank card processor or financial institution.

Data is encrypted by the secure payment gateway through protocols that ensure the security and privacy of the data. The purpose of First Data Global Gateway Connect 2.0 is to quickly and easily link you to the secure payment gateway. First Data is responsible for maintaining and upgrading the entire secure payment gateway system.

1.3 Supported Card Types

First Data Global Gateway Connect 2.0 supports the following credit card types:

- Visa®
- MasterCard®
- Discover®
- American Express®
- JCB® / Diner's Club®



First Data Global Gateway Connect 2.0 usually displays the supported card types in the format shown above.

For several card types a separate account may be required. If you want to add or change the credit card types accepted, please contact your processor's Merchant Services department.

1.4 Secure Sockets Layer (SSL) Encryption

By using Secure Sockets Layer (SSL) protocols, First Data Global Gateway Connect 2.0 provides:

- Data encryption
- Server authentication
- Message integrity
- Optional client authentication

SSL protocols provide secure communications on the Internet, such as transmitting credit card data and other data transfers. This process prevents the data from being compromised while in transit.

1.5 Other Helpful Skills

Knowledge of ASP, PHP, CGI, JavaScript, and other web technologies is helpful for implementing web site features, such as calculating order chargetotals and collecting or storing order data. Some of the suggested HTML resources can help you learn about other web technologies as well.

1.6 HTML Internet References

- W3C
  http://www.w3.org/
- Web Monkey
  http://www.webmonkey.com/
- Kevin Werbach's Bare Bones Guide to HTML
  http://werbach.com/barebones/

1.7 Equipment and Software

To use First Data Global Gateway Connect 2.0 for e-commerce, you need a web site hosted on a web server and a domain name.

First Data Global Gateway Connect 2.0 is compatible with all web servers and development languages.

When you set up your web site to process orders with First Data Global Gateway Connect 2.0, you will need one or more order forms along with a means to calculate the order chargetotal. JavaScript or any other web programming language, such as PHP or PERL, can be used to calculate the chargetotal. You may also need a means to calculate tax and shipping for your orders, as well as a database to store order data and transaction results.

A database with sensitive customer data, such as addresses and credit card numbers, should be protected with strong security measures. This protection ensures that you do not compromise your customers' sensitive information. With Connect 2.0, sensitive cardholder data is securely stored at First Data and not within your local database.

The secure payment gateway's average response time is less than 6 seconds.

1.8 The First Data Global Gateway Connect 2.0 Process

The following steps outline the First Data Global Gateway Connect 2.0 process.

- A customer selects items from an online store to purchase and is then transferred to a highly secure payment form hosted on the First Data Global Gateway Connect 2.0 secure payment gateway.

- The order and payment information are sent using a secure Internet connection to the payment gateway. The payment gateway transmits the order and payment information to the credit card processing network through a secure line and receives a response. Within 6 seconds*, the customer can review the transaction results.

- The customer reviews the First Data Global Gateway Connect 2.0 receipt page and confirms the details of the approved credit card transaction.

- Once configured, First Data Global Gateway Connect 2.0 posts all order and payment information back to the merchant's web site.

- The customer can view the confirmation page on the merchant's web site with the details of the order and a reminder that the receipt has been emailed.

- Transaction data can be downloaded in CSV or XML format and imported into the merchant's order management database.

* The secure payment gateway's average response time is less than 6 seconds.

1.9 Changes in Connect 2.0

If you are upgrading from Connect 1.0, note the following changes in Connect 2.0:

- Connect 2.0 supports JSP, PHP and ASP interface.
  - With the high-level interface languages (JSP, PHP and ASP), SHA2-256 inbound/outbound hashing is available to enhance transactional security.
- Transaction field hashing is utilized to enhance transaction validity (available only in JSP, PHP and ASP implementations)
- Connect 2.0 returns the tdate field to the merchant's response URL. Merchants must capture this field because it is required for secondary transactions (Void, PostAuth).
- For Visa retail transactions, Connect 2.0 does not enforce billing information fields; however, they are required and your transactions will be downgraded if you do not submit them.
- For all card types, the billing address is mandatory if transaction origin is MOTO and MOTO/ECI.
- A new posting URL for Connect 2.0 will be identified within the system generated welcome email.
- "**Shared Secret**" brings enhanced security to the Connect 2.0 product and must be set up in Virtual Terminal under the connect settings.
- Fraud FlexDetect^{SM} risk detection and management solution is available.
- Sale transactions can be set at $0 for card verification and/or to obtain a fraud score from Fraud FlexDetect^{SM}.

NOTE: A Technical Integration Appendix has been added to this document to illustrate the following:

- ASP, JSP and PHP Interface Examples,
- ASP, JSP and PHP SHA256 utility libraries,
- A Connect 1.0 HTML to Connect 2.0 ASP migration example.

1.10 Support

1.10.1 FDGG Virtual Terminal Manual

Located within the Global Gateway Code Wrapper and Manual Section of http://firstdata.com/ecommerce, the FDGG Virtual Terminal Manual provides additional support resources. Major sections include:

- Virtual Terminal Overview,
- Virtual Terminal Processing,
- Reports,
- How to Void Orders,
- Administration.

Note: The FDGG Virtual Terminal Manual needs be utilized in conjunction with this manual to deploy your hosted payment page solution. Section **3.1 First Data Global Gateway Setup** of this document provides hosted payment page setup details not referenced within the First Data Global Gateway Virtual Terminal manual.

1.10.2 Contact Information

If you have read the documentation and cannot find the answer to your question, you can contact Support at globalgateway.support@firstdata.com or 1-888-477-3611. You can find this information in the Virtual Terminal information menu on the right side of the Support main page.

2 Payment Processing Options

Before you begin integrating with First Data Global Gateway Connect 2.0, you must choose an integration method for each of the following options:

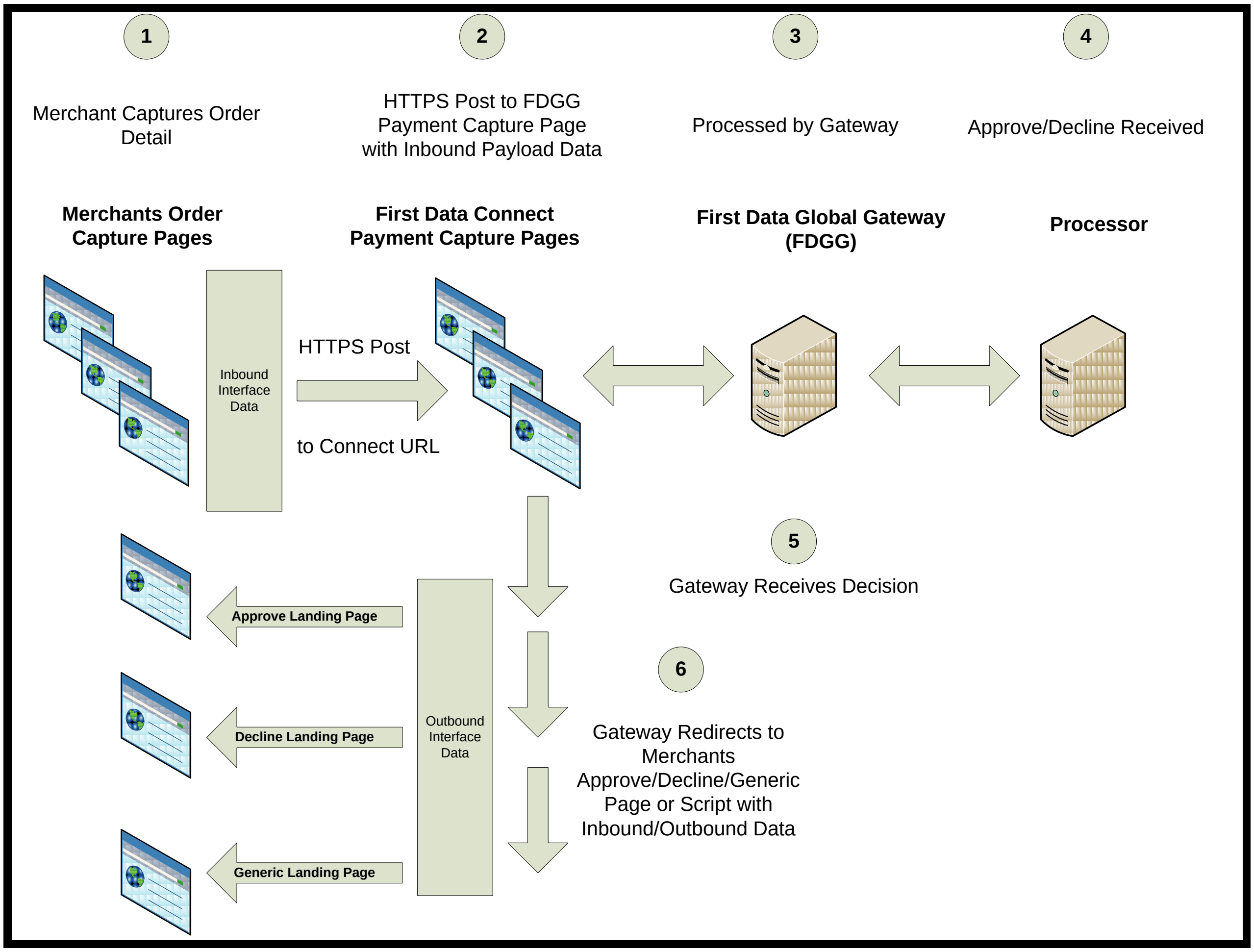
- **Form Hosting** – Decide whether to use the standard forms hosted by First Data or create your own forms and host them on your website.
- **Payment Mode** – Choose one of the three available payments modes (payonly, payplus, or fullpay) that determine what data First Data collects for each transaction.

2.1 Form Hosting Options

First Data Global Gateway Connect 2.0 allows two ways for collecting data from your customers:

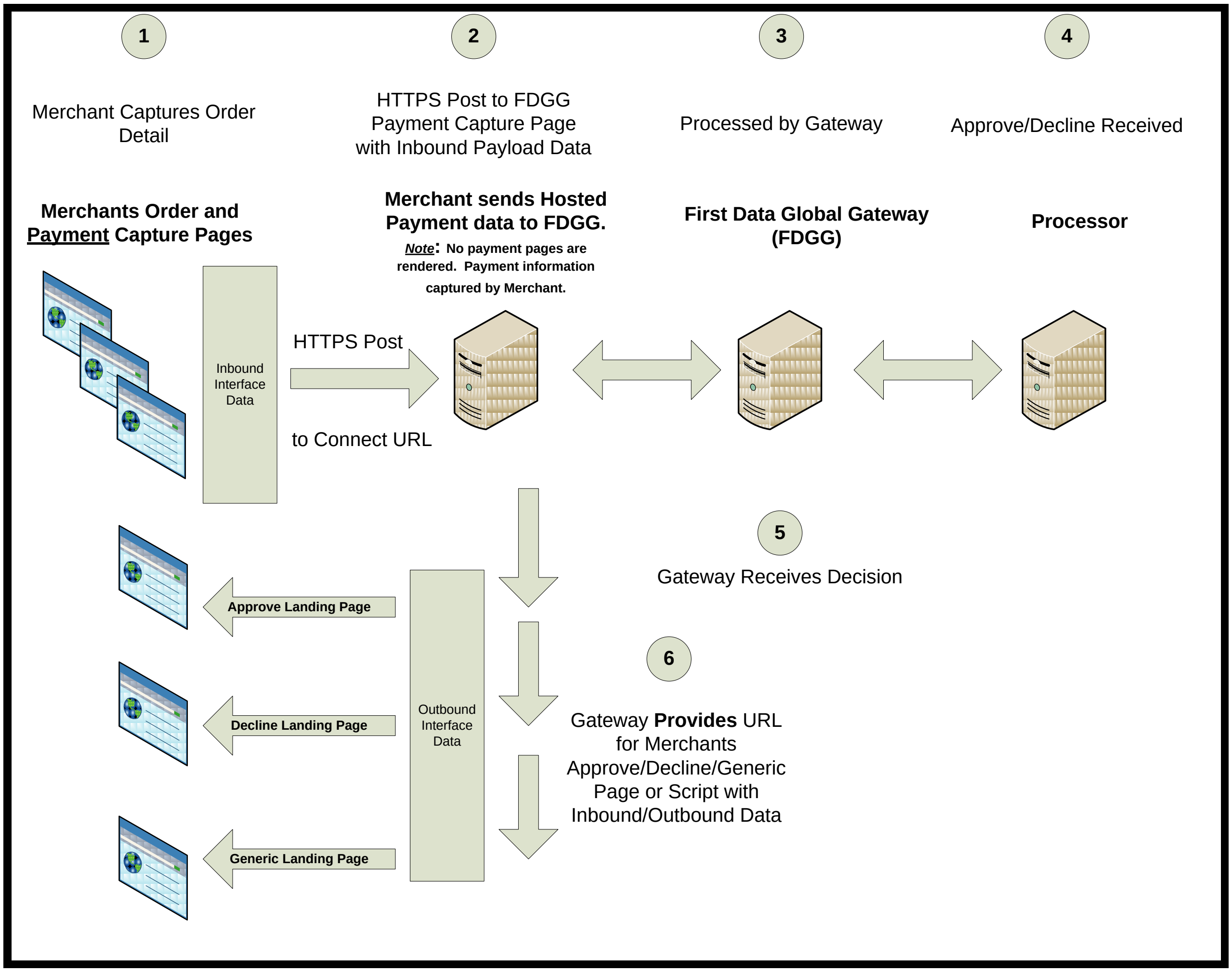
- The easiest option is to use the ready-made form pages for the payment process that First Data provides and host on our servers. With this option, you forward your customers to First Data for payment. They enter the sensitive cardholder data on First Data's SSL-encrypted page. Afterwards, Connect 2.0 redirects the customer back to your website and notifies your website of the payment result.

The transaction flow is pictorially represented as:


1
Merchant Captures Order Detail
2
HTTPS Post to FDGG Payment Capture Page with Inbound Payload Data
3
Processed by Gateway
4
Approve/Decline Received
Merchants Order Capture Pages
First Data Connect Payment Capture Pages
First Data Global Gateway (FDGG)
Processor
Inbound Interface Data
HTTPS Post
to Connect URL
5
Gateway Receives Decision
Approve Landing Page
6
Decline Landing Page
Outbound Interface Data
Gateway Redirects to Merchants Approve/Decline/Generic Page or Script with Inbound/Outbound Data
Generic Landing Page

- If you prefer that your customers stay on your website, you can create your own payment forms and host them on your server. Although your server hosts the forms, your website sends the sensitive cardholder data directly from the customer to the First Data Global Gateway so that you do not need to save any credit card data and therefore can avoid security risks. In order for your customers to see the secured website symbol in their browser, you must provide an SSL connection using HTTPS. Integration descriptions are available within Self-Hosted Payment Form Fields of this document.

The transaction flow is pictorially represented as:


1
Merchant Captures Order Detail
2
HTTPS Post to FDGG Payment Capture Page with Inbound Payload Data
3
Processed by Gateway
4
Approve/Decline Received
Merchants Order and Payment Capture Pages
Merchant sends Hosted Payment data to FDGG.
Note: No payment pages are rendered. Payment information captured by Merchant.
First Data Global Gateway (FDGG)
Processor
Inbound Interface Data
HTTPS Post
to Connect URL
5
Gateway Receives Decision
Approve Landing Page
Decline Landing Page
Generic Landing Page
Outbound Interface Data
6
Gateway Provides URL for Merchants Approve/Decline/Generic Page or Script with Inbound/Outbound Data

2.2 Payment Modes

First Data Global Gateway Connect 2.0 supports three different payment modes that define the range of data captured for each transaction. Depending on your business needs, you can choose a mode that only collects payment data or you can capture billing and shipping data, as well.

2.2.1 PayOnly Mode

In PayOnly mode, First Data Global Gateway Connect 2.0 collects the minimum information needed to process a transaction.

When using the forms hosted by First Data, the customer completes a single page containing payment information. Because billing information is mandatory for check transactions, PayOnly mode collects the same data as PayPlus mode when the customer pays with check.

2.2.2 PayPlus Mode

In PayPlus mode, First Data Global Gateway Connect 2.0 collects the same payment information as in PayOnly mode plus a full set of billing information.

When using the forms hosted by First Data, the customer completes two pages, one for the billing information and one for the payment information.

Review the Billing Fields section for further information.

2.2.3 FullPay Mode

In FullPay mode, First Data Global Gateway Connect 2.0 collects the same payment and billing information collected in PayPlus mode plus shipping information.

When using the forms hosted by First Data, the customer completes three pages, one for the payment information, one for the billing information, and one for the shipping information.

Review the Billing Fields and Shipping Fields sections for further information.

2.3 TeleCheck Transactions

For TeleCheck (First Data integrated electronic check service) transactions, the customer needs to authorize a debit to the account. There is an additional form added to the process where the customer gives authorization to continue the transaction. You have the option to bypass this form by setting the **authPageDisplayed** field to **False**. You also have the option to bypass the Select Payment Method page by setting the **PaymentMethod** data field to **check**.

If you choose to bypass the First Data Global Gateway Connect 2.0 payment form, there are rules that apply when using the Internet to initiate a debit to a customer's bank account. For more information about the rules for TeleCheck, see "Check Transactions.

2.4 Fraud Settings

You have access to both **Basic Fraud Settings** for blocking and limiting transactions, as well as **Fraud FlexDetect**^{SM} for advanced fraud detection and management. Setup for both programs can be found within the First Data Global Gateway Virtual Terminal under the **Administration** tab in the **Main Menu Bar**. For more information on Basic Fraud Settings, see the Support section of the First Data Global Gateway Virtual Terminal manual.

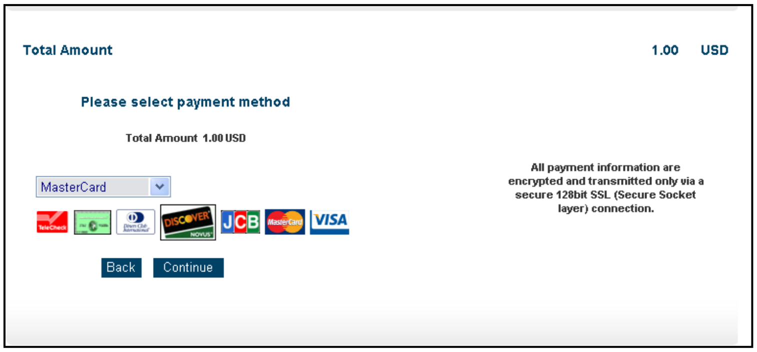
For more information on Fraud FlexDetect^{SM}, please reference the Fraud FlexDetect^{SM} User Guide (downloadable in the Virtual Terminal Administration section under Fraud FlexDetect^{SM} menu selection) or contact your representative.

2.5 Hosted Payment Forms

This section shows the payment forms hosted by First Data.

2.5.1 Payment Method Screen

The payment method screen allows the customer to choose the form of payment.



Total Amount 1.00 USD

Please select payment method

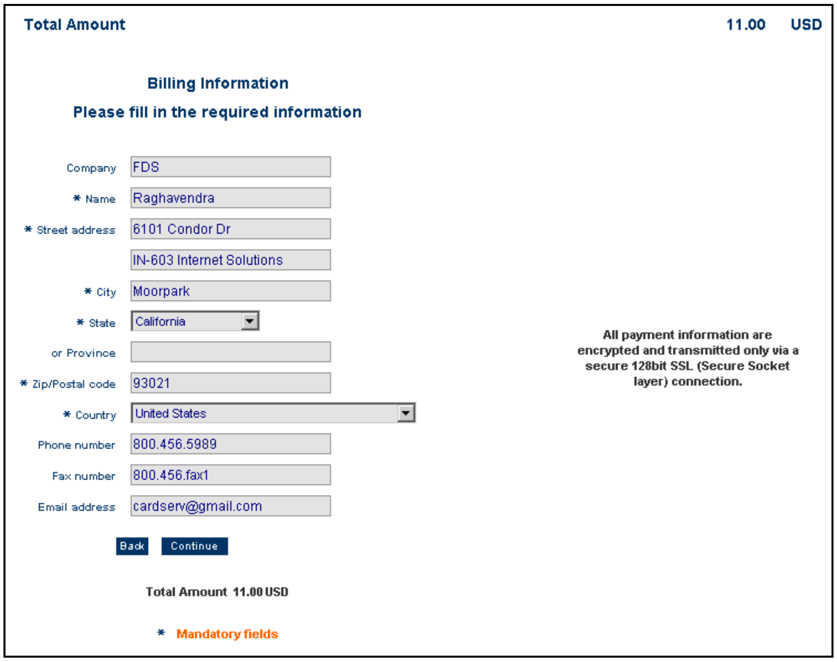
Total Amount 1.00 USD

MasterCard

All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

2.5.2 Billing Information Screen

The billing information screen displays for PayPlus transactions and all check transactions.



Total Amount 11.00 USD

Billing Information

Please fill in the required information

Company	FDS
* Name	Raghavendra
* Street address	6101 Condor Dr
	IN-603 Internet Solutions
* City	Moorpark
* State	California
or Province	
* Zip/Postal code	93021
* Country	United States
Phone number	800.456.5989
Fax number	800.456.fax1
Email address	cardserv@gmail.com

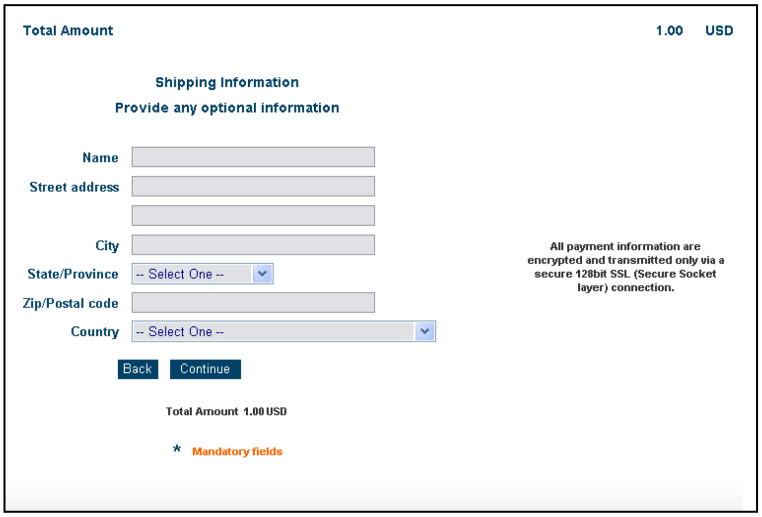
All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

Total Amount 11.00 USD

* Mandatory fields

2.5.3 Shipping Information Screen

The Shipping Information screen displays for FullPay transactions and all check transactions.



Total Amount 1.00 USD

Shipping Information

Provide any optional information

Name	
Street address	
City	
State/Province	-- Select One --
Zip/Postal code	
Country	-- Select One --

All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

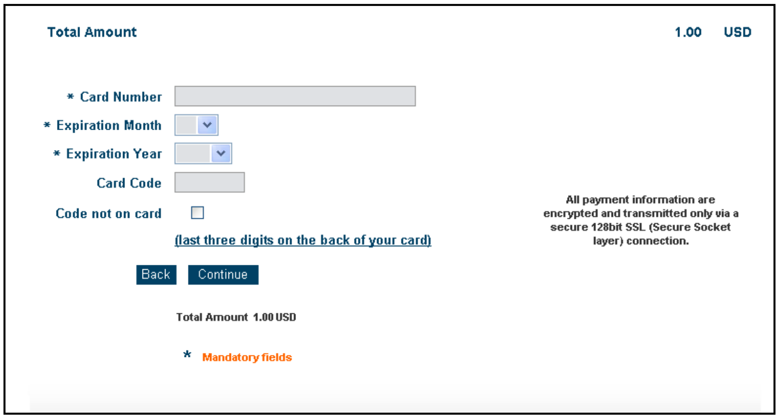
Total Amount 1.00 USD

* Mandatory fields

2.5.4 Payment Information Screen

The payment information screen allows customers to enter the details of their payment method.

The following shows the payment information screen for credit card transactions.



Total Amount 1.00 USD

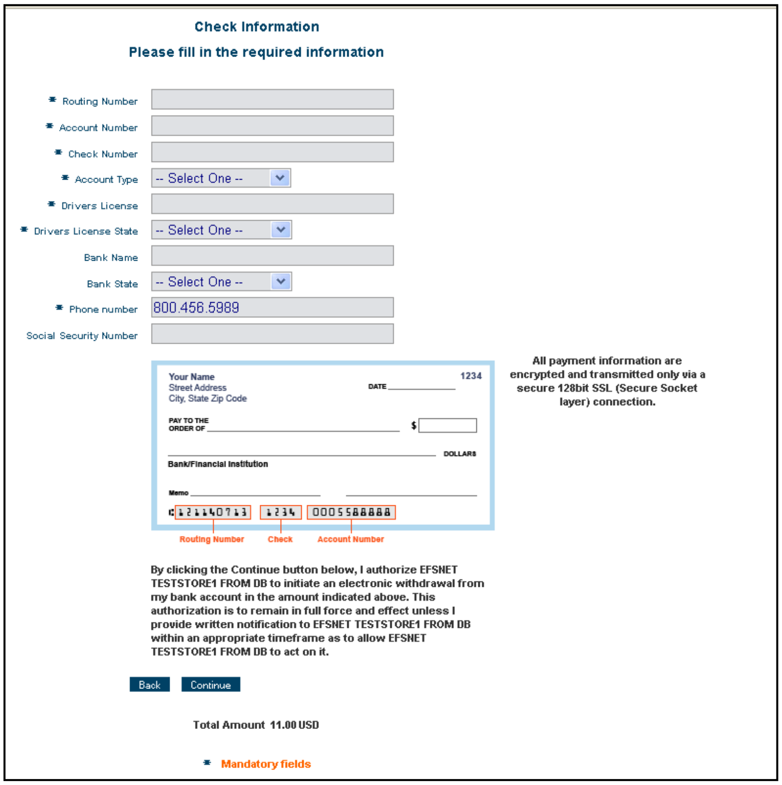
* Card Number	
* Expiration Month	
* Expiration Year	
Card Code	
Code not on card	□
	(last three digits on the back of your card)

All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

Total Amount 1.00 USD

* Mandatory fields

The following shows the payment information screen for check transactions.



Check Information

Please fill in the required information

* Routing Number	
* Account Number	
* Check Number	
* Account Type	-- Select One --
* Drivers License	
* Drivers License State	-- Select One --
Bank Name	
Bank State	-- Select One --
* Phone number	800.456.5989
Social Security Number	

All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

By clicking the Continue button below, I authorize EFSNET TESTSTORE1 FROM DB to initiate an electronic withdrawal from my bank account in the amount indicated above. This authorization is to remain in full force and effect unless I provide written notification to EFSNET TESTSTORE1 FROM DB within an appropriate timeframe as to allow EFSNET TESTSTORE1 FROM DB to act on it.

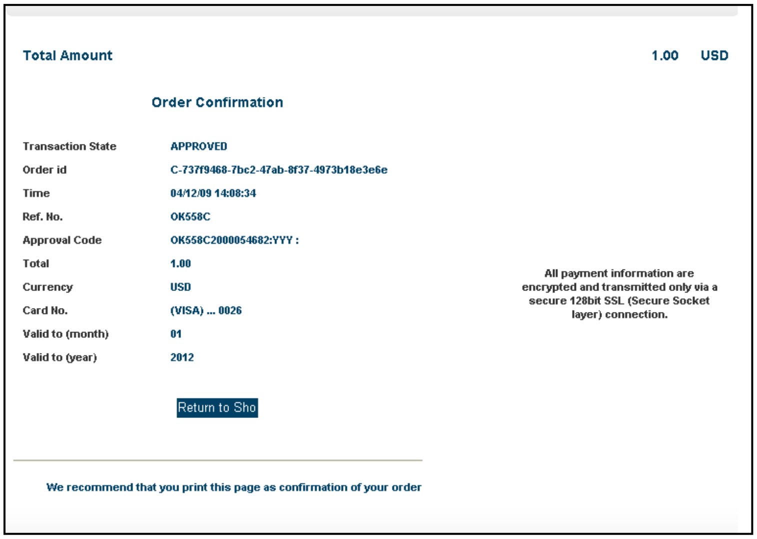
Total Amount 11.00 USD

* Mandatory fields

2.5.5 Confirmation Screen

The confirmation screen shows the customer the details of the completed transaction.

The following shows the confirmation screen for credit card transactions.



Total Amount 1.00 USD

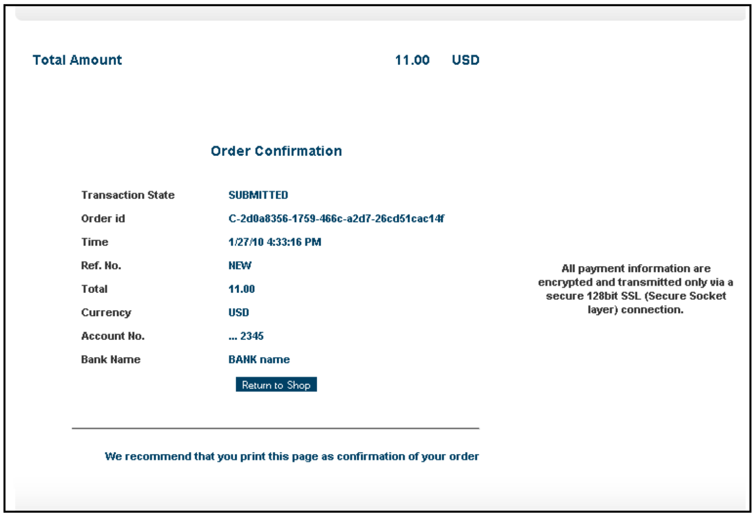
Order Confirmation

Transaction State	APPROVED
Order id	C-737f9468-7bc2-47ab-8f37-4973b18e3e6e
Time	04/12/09 14:08:34
Ref. No.	OK558C
Approval Code	OK558C2000054682:YYY :
Total	1.00
Currency	USD
Card No.	(VISA) ... 0026
Valid to (month)	01
Valid to (year)	2012

All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

We recommend that you print this page as confirmation of your order

The following shows the confirmation screen for check transactions.



Total Amount 11.00 USD

Order Confirmation

Transaction State	SUBMITTED
Order id	C-2d0a8356-1759-466c-a2d7-26cd51cac14f
Time	1/27/10 4:33:16 PM
Ref. No.	NEW
Total	11.00
Currency	USD
Account No.	... 2345
Bank Name	BANK name

All payment information are encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection.

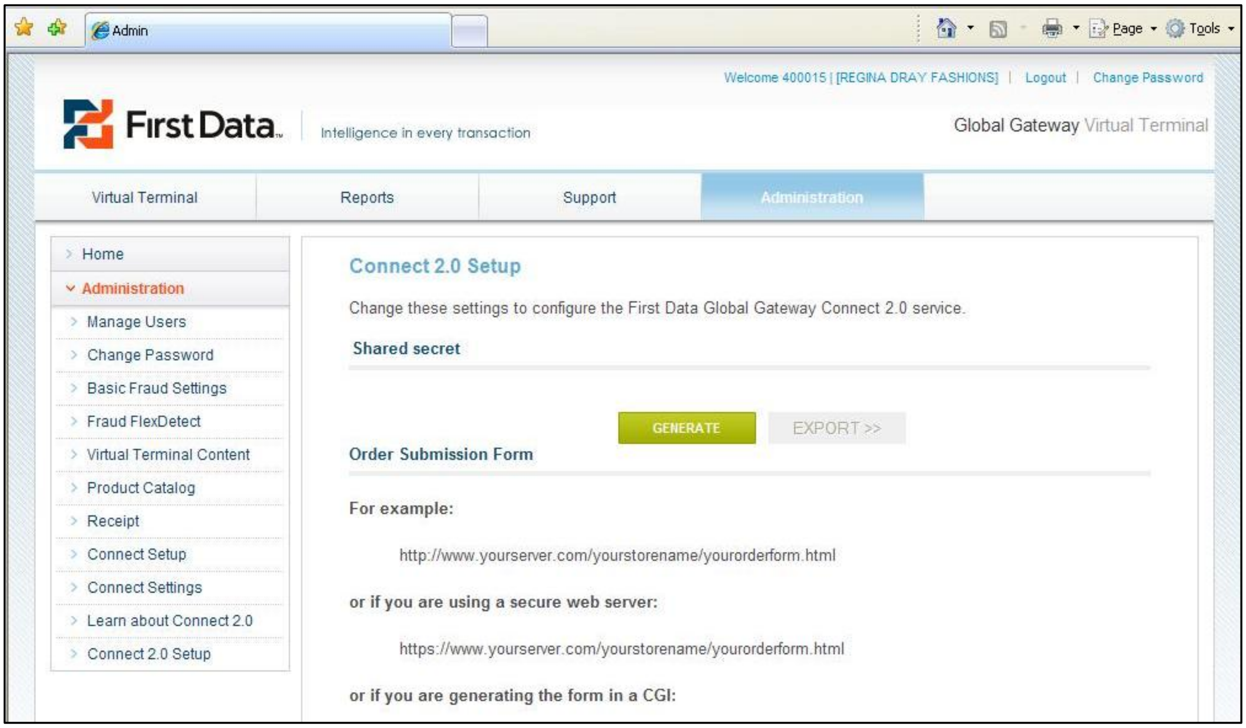
We recommend that you print this page as confirmation of your order

3 Getting Started

This section provides simple examples of how to integrate your website with First Data Global Gateway Connect 2.0 in FullPay Mode using ASP, PHP, and JSP. This section assumes that the developer has a basic understanding of his chosen scripting language.

3.1 First Data Global Gateway Setup

This section outlines the configuration you need to complete in Virtual Terminal for merchant to use First Data Global Gateway Connect 2.0. To set up your First Data Global Gateway Connect 2.0 store, in Virtual Terminal, select the Administration tab then select Connect 2.0 Setup.



Connect 2.0 Setup

Change these settings to configure the First Data Global Gateway Connect 2.0 service.

Shared secret

Order Submission Form

For example:

http://www.yourserver.com/yourstorename/yourorderform.html

or if you are using a secure web server:

https://www.yourserver.com/yourstorename/yourorderform.html

or if you are generating the form in a CGI:

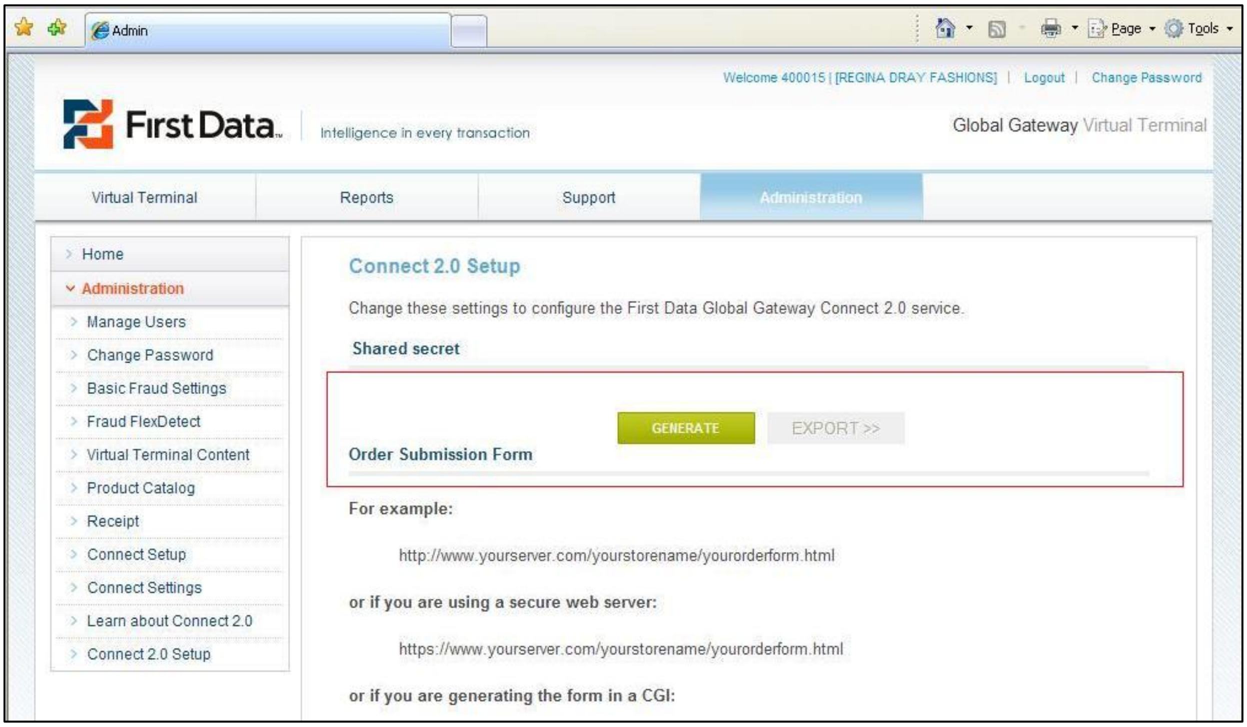
The following sections describe the setup required for each section of the Connect 2.0 Setup screen.

3.1.1 Shared Secret

The **Shared Secret** is a required field. It is used for constructing the SHA2 hash value that ensures your store communicates only with Connect 2.0. The **Shared Secret** field is no longer an User defined value.

3.1.1.1 Defining a New Shared Secret

If you are a ***NEW*** Connect 2.0 User and DO NOT have a **Shared Secret** defined, your Virtual Terminal display will look as follows:



Connect 2.0 Setup

Change these settings to configure the First Data Global Gateway Connect 2.0 service.

Shared secret

Order Submission Form

For example:

http://www.yourserver.com/yourstorename/yourorderform.html

or if you are using a secure web server:

https://www.yourserver.com/yourstorename/yourorderform.html

or if you are generating the form in a CGI:

To generate a **Shared Secret** perform the following actions:

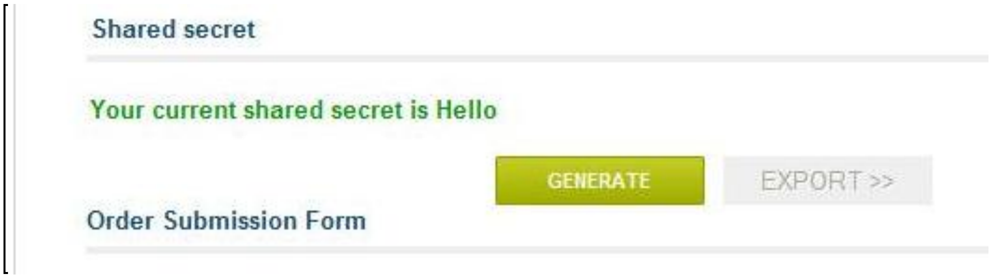
1. **Select Generate** –Initiates an application process to generate a **Shared Secret.**

2. **Select Export** – Opens a file dialogue box that enables you to download and access the **Shared Secret** value. **This value should be used as presented within the hash interface field** (defined in section 4.0 Standard Fields).

3. **Select Submit at the Bottom of the Page** – Updates and activates your new **Shared Secret.** Note: This action IMMEDIATELY ACTIVATES YOUR NEW **Shared Secret.**

3.1.1.2 Modifying an Existing Shared Secret

If you are an ***EXISTING*** Connect 2.0 User and have a **Shared Secret** defined, your Virtual Terminal display will look as defined below.



Shared secret

Your current shared secret is Hello

Order Submission Form

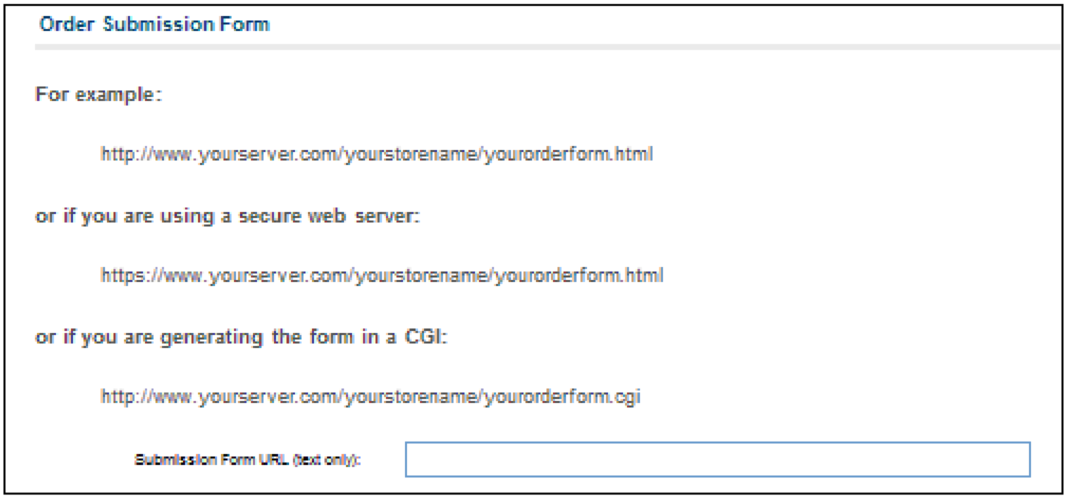
In the above display, your **Shared Secret** is defined as “**Hello**”.

To generate a new **Shared Secret** perform the following actions:

1. **Select Generate** –Initiates an application process to generate a **Shared Secret.**

2. **Select Export** – Opens a file dialogue box that enables you to download and access the **Shared Secret** value. **This value should be used as presented within the hash interface field** (defined in section 4.0 Standard Fields).

3.1.2 Order Submission Form



Order Submission Form

For example:

http://www.yourserver.com/yourstorename/yourorderform.html

or if you are using a secure web server:

https://www.yourserver.com/yourstorename/yourorderform.html

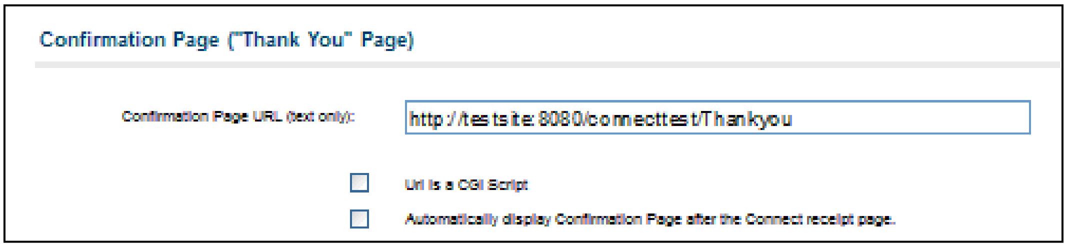
or if you are generating the form in a CGI:

http://www.yourserver.com/yourstorename/yourorderform.cgi

Submission Form URL (text only):

Enter the URL of your order form in the **Submission Form URL** field. This is a required field.

3.1.3 Confirmation Page



Confirmation Page ("Thank You" Page)

Confirmation Page URL (text only): http://testsite:8080/connecttest/Thankyou

□ Url is a CGI Script

□ Automatically display Confirmation Page after the Connect receipt page.

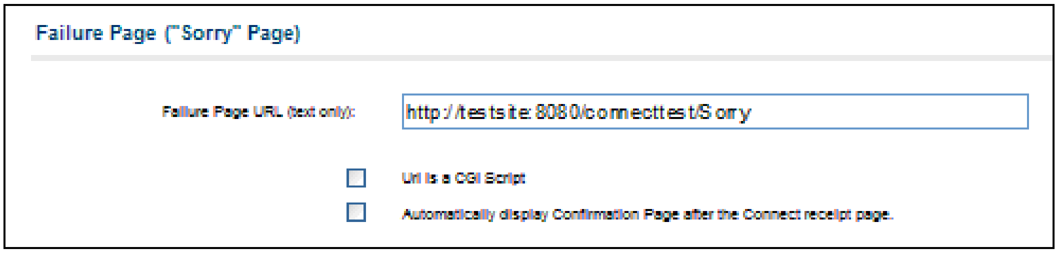
Enter the URL of your confirmation/thank you page in the **Confirmation Page URL** field. First Data Global Gateway Connect 2.0 redirects your customers to this URL after a successful transaction.

You can enable the option **URL is a CGI Script** if you want First Data Global Gateway Connect 2.0 to post the data back to your web site to collect the information using a scripting language like CGI, PHP, or ASP.

If you want to display this URL automatically after the receipt page, select the **automatically display Confirmation Page** ... checkbox. When you select this checkbox, the transaction result page will show momentarily before the customer is forwarded to the confirmation page.

If you don't configure this value in Virtual Terminal, you can submit this URL with the responseSuccessURL field for each transaction.

3.1.4 Failure Page



Failure Page ("Sorry" Page)

Failure Page URL (text only): http://testsite:8080/connecttest/Sorry

□ Url is a CGI Script

□ Automatically display Confirmation Page after the Connect receipt page.

Enter the URL of your failure page in the **Confirmation Page URL** field. First Data Global Gateway Connect 2.0 redirects your customers to this URL after an unsuccessful transaction.

You can enable the option **URL is a CGI Script** if you want First Data Global Gateway Connect 2.0 to post the data back to your web site to collect the information using a scripting language like CGI, PHP, or ASP.

If you want to display this URL automatically after the receipt page, select the **automatically display Confirmation Page** ... checkbox. When you select this checkbox, the transaction result page will show momentarily before the customer is forwarded to the confirmation page.

If you don’t configure this value in Virtual Terminal, you can submit this URL with the responseFailURL field for each transaction.

Note: If you have enabled the Fraud FlexDetect^{SM} product and there is a fraud decline, the consumer will be routed automatically to this URL.

3.1.5 Customizing First Data Global Gateway Connect Payment Forms

Some of the options allow you to enter either plain text or a reference to an HTML file. If you choose to enter a reference to an HTML file, verify the file is on an accessible, secure server and that your URL begins with "https://." Otherwise, every time one of your customers opens the payment form, a dialogue appears warning that some of the contents are not secure. The dialogue box requires a response from the customer before the form will be displayed.

The First Data Global Gateway Virtual Terminal displays the following fields on the Payment Form page.

Company Name (Text Only)

Enter your company name in this field to display the company name on the top of the secure order and order confirmation pages on the gateway. If both your company name and logo are provided, the company name will be displayed next to the logo at the top of the order and confirmation pages.

The company name entered here is only displayed on your secure order and order confirmation pages. The DBA company name you gave when you opened your account is not displayed.

Logo (HTML or Text)

You can display your logo on the top of the secure order and order confirmation pages on the gateway. Enter the URL for your Logo Graphic file. You can use any common web graphics format (gif, jpg, or png). The graphic must be available from a secure web server. The URL you enter should include the HTTPS protocol.

https://your_server_name/logo.gif

- https//: - indicates a secure server.
- your_server_name - the name of your web server (this name may or may not include www).
- logo.gif - the name of the file you want to use as your logo.

Background Image (HTML Only)

This is the image displayed behind your payment form. Enter an https URL for a graphics file in this field. Follow the same example as the **Logo** field.

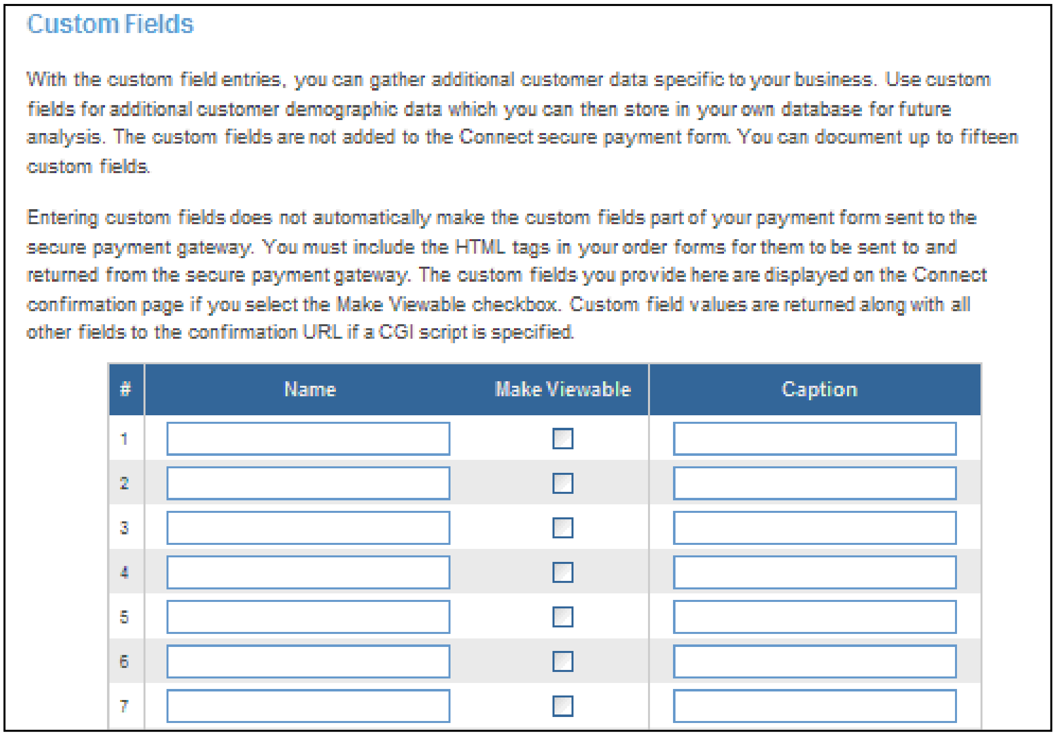
Payment Header (HTML or Text)

Enter text in this field for the payment header. The payment header is displayed at the top of your payment form.

Payment Footer (HTML or Text)

Enter text in this field for the payment footer. The payment footer is displayed at the bottom of your payment form.

3.1.6 Custom Fields



Custom Fields

With the custom field entries, you can gather additional customer data specific to your business. Use custom fields for additional customer demographic data which you can then store in your own database for future analysis. The custom fields are not added to the Connect secure payment form. You can document up to fifteen custom fields.

Entering custom fields does not automatically make the custom fields part of your payment form sent to the secure payment gateway. You must include the HTML tags in your order forms for them to be sent to and returned from the secure payment gateway. The custom fields you provide here are displayed on the Connect confirmation page if you select the Make Viewable checkbox. Custom field values are returned along with all other fields to the confirmation URL if a CGI script is specified.

#	Name	Make Viewable	Caption
1		□	
2		□	
3		□	
4		□	
5		□	
6		□	
7		□	

Use this section to define up to 15 custom fields that that Connect 2.0 collects data for on each transaction. Connect 2.0 returns the values for the custom fields in the response. You can submit as many custom fields as you like for every transaction; however, Connect 2.0 only collects data for the fields defined here for reporting. For each custom field, enter the following:

- **Name**: the name of the field as it will be submitted to Connect 2.0.
- **Make Viewable**: select if you want to display this field on the payment forms.
- **Caption**: the text to display for the field on payment forms.

For more information about custom fields, see 6 Additional Custom Fields.

Note: A hidden custom field could be utilized to aide in the reconciliation of inbound/outbound transactional data.

3.2 Transaction Types

It is important to understand the terminology for processing transactions so that you use the appropriate transaction type for your orders and returns. A Chargeback is fraud. In addition, what can a merchant do to prevent a fraud.

For the money associated with a transaction to transfer to and from your account, the batch of transactions for the day first have to be settled (this is also called closing the batch). Depending upon your merchant profile setting, transactions automatically settle by default at 7:00 PM (PST).

Transaction Types	
Name	**Description**
Sale	A credit card transaction that immediately charges a customer's credit card. To run a sale transaction, set the **txntype** data field to **Sale**, as in the following HTML sample: `<input type="hidden" name="txntype" value="sale">` **Note**: If txntype field is not provided, the transaction type of the transaction will default to a sale.
Authorize Only	A credit card transaction that reserves funds on a customer's credit card. An Authorize Only transaction does not charge the card until you perform a Ticket Only transaction and confirm shipment of the order (using an option available in First Data Global Gateway Virtual Terminal reports). To run an Authorize Only transaction, set the **txntype** data field to preauth, as shown in the following HTML sample: `<input type="hidden" name="txntype" value="preauth">` **Note**: Authorizations reserve funds for varying periods, depending on the issuing credit card company's policy. The period may be as little as three days or as long as several months. For your protection, it is recommended that you confirm shipment as soon as possible after authorization. Use the Point of Sale page for an Authorize Only transaction in the First Data Global Gateway Virtual Terminal.
Ticket Only	A Ticket Only transaction is a post-authorization transaction that captures the funds from an Authorize Only transaction, reserving funds on the customer's card for the amount specified. Funds are transferred when your batch of transactions is settled. If you enter a larger chargetotal in the Ticket Only transaction than was specified for the Authorize Only transaction, the Ticket Only transaction may be declined. To run a Ticket Only transaction, set the **txntype** data field to postauth, as shown in the following HTML sample: `<input type="hidden" name="txntype" value="postauth">` If you enter a smaller amount than was authorized, an adjustment is made to the authorization to reserve only the smaller amount of funds on the customer's card for the transaction. Use the Ticket Only page for a Ticket Only transaction in the First Data Global Gateway Virtual Terminal.
Forced Ticket	A Forced Ticket transaction is a credit card transaction used similarly to a Ticket Only transaction, except it is specifically for authorizations obtained over the phone. It requires a reference number (or approval code) that you should have received when you did the phone authorization. Use the Point of Sale page for a Forced Ticket transaction in the First Data Global Gateway Virtual Terminal.

Transaction Types	
Name	**Description**
Return	A return transaction returns funds to a customer's credit card for an existing order on the system. To perform a return, you need the order number, which you can find in your reports in the First Data Global Gateway Virtual Terminal. If you perform a return of the full order amount, the order will appear in your reports with a transaction amount of 0.00. To perform a return transaction, use the Return page in the First Data Global Gateway Virtual Terminal. You must be logged in to the First Data Global Gateway Virtual Terminal to perform a return transaction.
Credit	A credit transaction returns funds to a customer's credit card for orders where you do not have an order number. This transaction is intended for returns on orders processed outside the system. Use the Credit page to perform a credit transaction in the First Data Global Gateway Virtual Terminal. Credit transactions are marked as returns in your reports. You must be logged in to the First Data Global Gateway Virtual Terminal to perform a credit transaction.
Void	A void transaction cancels the transaction. Void transactions must be run manually in First Data Global Gateway Virtual Terminal reports. Only transactions in the current batch (that have not been sent for settlement) can be voided.

3.3 Check Transactions

TeleCheck Services (TeleCheck Internet Acceptance and TeleCheck Phone Acceptance) are a way to process Automated Clearing House (ACH) transactions using the Internet or a phone line. ACH transactions debit a customer's account and transfer the funds to a merchant's account. To enable TeleCheck, contact your merchant service provider.

There are rules that apply when initiating a debit to a customer's bank account. These rules are established and maintained by the National Automated Clearing House Association (NACHA) and are published periodically in *ACH Rules: A Complete Guide to Rules & Regulations Governing the ACH Network*. You can view these rules here:

http://www.nacha.org/

It is each merchant's responsibility to understand and abide by the published rules and regulations.

The rules for authorization differ depending on whether the transaction is:

- E-commerce
- Retail or Mail Order
- Telephone Order

During a check transaction, a real-time response will be provided by TeleCheck on whether or not a check is accepted. Based on the response from TeleCheck, a transaction can be marked as either Submitted or Declined.

If the check was declined for credit reasons, a message will appear with some information for the customer, including a phone number for the customer to call with questions. When this occurs, you must give the information, word-for-word, to the customer. If the check was submitted successfully, the transaction status will be **Submitted**.

If an error occurred, the reason for the error will appear here. If the error was due to data entry, you may have an opportunity to re-enter the data.

Error message:

We are sorry that we cannot accept your check at this time. Our decision is based, in whole or in part, on information provided to us by TeleCheck. We encourage you to call TeleCheck at 1-877-678-5898 or write TeleCheck Customer Care at P.O. Box 4513, Houston, TX 77210-4513. Please provide TeleCheck your driver's license number and the state where it was issued, and the complete banking numbers printed on the bottom of your check. Under the Fair Credit Reporting Act, you have the right to a free copy of your information held in TeleCheck's files within 60 days from today. You may also dispute the accuracy or completeness of any information in TeleCheck's customer report. TeleCheck did not make the adverse decision not to accept your check and is unable to explain why this decision was made.Sample Verbal authorization for telephone order transactions:

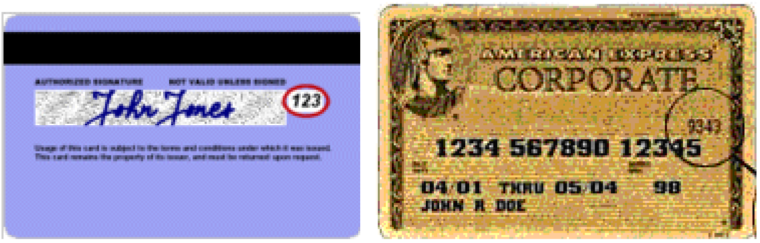
On [insert today's date], [insert customer's First and Last Name] authorizes an electronic debit in the amount of [insert amount]. This withdrawal will be processed using the regular banking system. If your payment is returned unpaid, you will be charged a returned item fee up to the maximum allowed by law. If you have any questions at any time, you may call us at [insert Merchant Customer Care Phone Number] during business hours. Do you authorize the transaction? (Please answer Yes or No)

AVS Code	Visa	MasterCard	Discover	American Express	Description
YY	Y	Y	A	Y	Address and zip code match.
NY	Z	Z	Z	Z	Only the zip code matches.
YN	A	A	Y	A	Only the address matches.
NN	N	N	N	N	Neither the address nor the zip code match.
XX	-	W	-	-	Card number not on file.
XX	U	U	U	U	Address information not verified for domestic transaction.
XX	R	-	R	R	Retry - system unavailable.
XX	S	-	S	S	Service not supported.
XX	E	-	-	-	AVS not allowed for card type.
XX	-	-	-	-	Address verification has been requested, but not received.
XX	G	-	-	-	Global non-AVS participant. Normally an international transaction.
YN	B	-	-	-	Street address matches for international transaction; Postal code not verified.
NN	C	-	-	-	Street address and Postal code not verified for international transaction.
YY	D	-	-	-	Street address and Postal code match for international transaction.
YY	F	-	-	-	Street address and Postal code match for international transaction. (UK Only)
NN	I	-	-	-	Address information not verified for international transaction.
YY	M	-	-	-	Street address and Postal code match for international transaction.

AVS Code	Visa	MasterCard	Discover	American Express	Description
NY	P	-	-	-	Postal codes match for international transaction; Street address not verified.

3.4 Card Codes

The card code is a three or four-digit security code. For Visa, MasterCard, and Discover, the number typically appears at the end of the signature panel. For American Express, the number appears on the front of the card. This security card program helps validate that a genuine card is being used during a transaction. A card code mismatch blocks the transaction.



The card code is circled.

Mail order, Telephone Order (MOTO), and other transactions when the card is not present have higher fraud rates than face-to-face transactions. To help reduce fraud, use the card code.

You should always enter a card code (if on the card) when processing an authorization for MOTO and e-commerce transactions.

For retail transactions, you may want to enter the card code printed on the card to ensure that the card was not fraudulently reproduced.

By using the card code results along with the Address Verification System (AVS), you can make better-informed decisions about whether to accept transactions.

3.4.1 Using the Card Code

Enter the card code on the Virtual Terminal page when processing an order in the First Data Global Gateway Virtual Terminal. First Data Global Gateway Connect 2.0 compares the card code with the code from the card-issuing bank. The results of this comparison show in the transaction approval code.

The following string is a typical transaction result.

0097820000019564:YNAM:12345678901234567890123:

The last alphabetic character in the middle (M) is a code indicating whether the card code matched the card-issuing bank's code.

3.4.2 Card Code Definitions

Card Code	Description
M	Card code matches.
N	Card code does not match.
P	Not processed.
S	Merchant has indicated that the card code is not present on the card.
U	Issuer is not certified and/or has not provided encryption keys.
X	No response from the credit card association was received.
A blank response indicates no code was sent and there was no indication the code was not present on the card.	

3.5 Testing Transactions

With First Data Global Gateway Connect 2.0, you can run test transactions. You should immediately delete all your test orders when you are done testing. If you want to do extensive testing, you can use a test server. Apply for a Test Account here:

http://www.firstdata.com/product_solutions/ecommerce/global_gateway/index.htm

For testing purposes, you can use the following card numbers:

- 4111 1111 1111 1111 for Visa.
- 5419 8400 0000 0003 for MasterCard.
- 6011000993010978 for Discover.
- 372700997251009 for American Express.

When running test transactions in the production environment, transaction fees may apply. For details, contact your merchant account provider.

3.6 Checklist

In order to integrate with the gateway, you must have the following items:

- **Store Name** - ID of your store given to you by First Data. For example: 10123456789
- **Shared Secret** - Shared secret that you should set up in Virtual Terminal. This value is used for constructing the hash value (see below).

4 Standard Fields

This section describes the fields that are used for all transactions to First Data Global Gateway Connect 2.0, regardless of who hosts the forms.

If you use the forms hosted by First Data, you do not need to submit additional fields. If you use forms hosted on your own server, you will also need to include the relevant fields.

Note: Connect 2.0 only utilized the *en* (US English) character set. Inbound field names are case sensitive. The usage of international character sets may produce unpredictable results within Connect 2.0.

4.1 Credit Card

4.1.1 Sale

The following table describes the fields required for a Sale transaction.

> Differing from previous versions, Connect 2.0 now allows the merchant to perform a zero dollar sale transaction. Also referred to as an "AVS-only" transaction, it is used to test account validity. With a $0.00 authorization, $1.00 ghost authorizations no longer appear in the cardholders billing statement, eliminating confusion. Visa's new Zero Dollar or Zero Dollar Floor Limit Account Verification program, billed at normal transaction rates, will also include Address Verification (AVS) and CVV verification

Field	Required	Description
txntype	Required.	Transaction type. If you do not submit this field, Connect 2.0 defaults to sale mode. Valid value is: sale
timezone	Required.	Time zone of the transaction. Valid values are: GMT, EST, CST, MST, PST
txndatetime	Required.	Date and time of the transaction in YYYY:MM:DD-hh:mm:ss format.
hash	Required	The SHA2 hash of the following values: **storename + txndatetime + chargetotal + Shared Secret.** The values must be in this order when creating the hash. See the examples below for how to create the hash values.
storename	Required.	The Store ID provided by First Data.
mode	Optional.	The payment mode for the transaction. If you do not submit this field, Connect 2.0 defaults to PayOnly mode. Valid values are: payonly payplus fullpay

Field	Required	Description
chargetotal	Required at 0.00 or greater	The total amount of the transaction, including tax and shipping. Use dot or comma separators for decimals. For example, 12.34 is $12.34. Thousandths-place separators are not allowed.
oid	Optional.	The order ID of the transaction. If you do not submit this field, the system automatically generates a value. Limit 100 valid US character set characters.
subtotal	Required at 0.00 or greater	The subtotal amount of the transaction, before tax and shipping.
tax	Optional.	The tax amount of the transaction.
shipping	Optional.	The shipping amount of the transaction.
paymentMethod	Optional.	Allows you to specify the type of payment. If you do not submit this field, Connect 2.0 displays a drop-down menu to the customer to choose from the payment methods available for your shop. Valid values are: M – MasterCard V – Visa A – American Express C – Diners J – JCB D – Discover
userid	Optional.	A user ID allowing merchants to track their customers.
invoicenumber	Optional.	The invoice number for the transaction. If an InvoiceNumber is not provided by the merchant, the system will utilize the TransactionSequenceNumber generated by the system in this value to the processor.
trxOrigin	Required.	The source of the transaction. If you do not submit this field, Connect 2.0 defaults to ECI. Valid values are: ECI – email or Internet MOTO – mail order/telephone order RETAIL – face-to-face
refer	Optional.	Text describing who referred the customer to your store.
comments	Optional.	Any comments about the transaction.
responseSuccessURL	Optional.	The URL to direct customers after a successful transaction (e.g., your Thank You URL). You only need to submit this value if it is not set up in Virtual Terminal.

Field	Required	Description
responseFailURL	Optional.	The URL to direct customers after a declined or unsuccessful transaction (e.g., your Sorry URL). You only need to submit this value if it is not set up in Virtual Terminal. **Note**: If you have enabled the Fraud FlexDetect^{SM} product and there is a fraud decline, the consumer will be routed automatically to this URL.
ponumber	Optional.	The purchase order number or other customer-supplied number to identify the transaction (for example, a department code.) Up to 30 characters, including spaces.
taxexempt	Optional.	Indicates that the transaction is tax exempt. Default is false. Valid values are: True false
deviceId	Optional.	The DeviceID for Fraud FlexDetect^{SM} transactions. If merchant doesn't pass the DeviceID, Connect will generate the DeviceID if the merchant is using Fraud FlexDetect^{SM}.

4.1.2 PreAuth

The following table describes the fields required for a PreAuth transaction:

Field	Required	Description
txntype	Required.	Transaction type. If you do not submit this field, Connect 2.0 defaults to sale mode. Valid value is: preauth
timezone	Required.	Time zone of the transaction. Valid values are: GMT, EST, CST, MST, PST
txndatetime	Required.	Date and time of the transaction in YYYY:MM:DD-hh:mm:ss format.
hash	Required	The SHA2 hash of the following values: **storename + txndatetime + chargetotal + Shared Secret.** The values must be in this order when creating the hash. See the examples below for how to create the hash values.
storename	Required.	The Store ID provided by First Data.

Field	Required	Description
mode	Optional.	The payment mode for the transaction. If you do not submit this field, Connect 2.0 defaults to PayOnly mode. Valid values are: payonly payplus fullpay
chargetotal	Required at 0.00 or greater	The total amount of the transaction, including tax and shipping. Use dot or comma separators for decimals. For example, 12.34 is $12.34. Thousandths-place separators are not allowed.
oid	Optional.	The order ID of the transaction. If you do not submit this field, the system automatically generates a value. Limit 100 valid US character set characters.
subtotal	Required.	The subtotal amount of the transaction, before tax and shipping.
tax	Optional.	The tax amount of the transaction.
shipping	Optional.	The shipping amount of the transaction.
paymentMethod	Optional.	Allows you to specify the type of payment. If you do not submit this field, Connect 2.0 displays a drop-down menu to the customer to choose from the payment methods available for your shop. Valid values are: M – MasterCard V – Visa A – American Express C – Diners J – JCB D – Discover
userid	Optional.	A user ID allowing merchants to track their customers
invoicenumber	Optional.	The invoice number for the transaction. If an InvoiceNumber is not provided by the merchant, the system will utilize the TransactionSequenceNumber generated by the system in this value to the processor.
trxOrigin	Required.	The source of the transaction. If you do not submit this field, Connect 2.0 defaults to ECI. Valid values are: ECI – email or Internet MOTO – mail order/telephone order RETAIL – face-to-face
refer	Optional.	Text describing who referred the customer to your store.
comments	Optional.	Any comments about the transaction.

Field	Required	Description
responseSuccessURL	Optional.	The URL to direct customers after a successful transaction (e.g., your Thank You URL). You only need to submit this value if it is not set up in Virtual Terminal.
responseFailURL	Optional.	The URL to direct customers after a declined or unsuccessful transaction (e.g., your Sorry URL). You only need to submit this value if it is not set up in Virtual Terminal. **Note**: If you have enabled the Fraud FlexDetect^{SM} product and there is a fraud decline, the consumer will be routed automatically to this URL.
ponumber	Optional.	The purchase order number or other customer-supplied number to identify the transaction (for example, a department code.) Up to 30 characters, including spaces.
taxexempt	Optional.	Indicates that the transaction is tax exempt. Default is false. Valid values are: true false
deviceId	Optional.	The DeviceID for Fraud FlexDetect^{SM} transactions. If merchant doesn't pass the DeviceID, Connect will generate the DeviceID if the merchant is using Fraud FlexDetect^{SM}.

4.1.3 PostAuth

The following table describes the fields required for a PostAuth transaction:

Field	Required	Description
txntype	Required.	Transaction type. If you do not submit this field, Connect 2.0 defaults to sale mode. Valid value is: postauth
timezone	Required.	Time zone of the transaction. Valid values are: GMT, EST, CST, MST, PST
txndatetime	Required.	Date and time of the transaction in YYYY:MM:DD-hh:mm:ss format.
hash	Required	The SHA2 hash of the following values: **storename + txndatetime + chargetotal + Shared Secret.** The values must be in this order when creating the hash. See the examples below for how to create the hash values.
storename	Required.	The Store ID provided by First Data.

Field	Required	Description
mode	Optional.	The payment mode for the transaction. If you do not submit this field, Connect 2.0 defaults to PayOnly mode. Valid values are: payonly payplus fullpay
chargetotal	Required at 0.00 or greater	The total amount of the transaction, including tax and shipping. Use dot or comma separators for decimals. For example, 12.34 is $12.34. Thousandths-place separators are not allowed.
oid	Required.	The oid of the PreAuth transaction being completed.
paymentMethod	Optional.	Allows you to specify the type of payment. If you do not submit this field, Connect 2.0 displays a drop-down menu to the customer to choose from the payment methods available for your shop. Valid values are: M – MasterCard V – Visa A – American Express C – Diners J – JCB D – Discover
userid	Optional.	A user ID allowing merchants to track their customers
invoicenumber	Optional.	The invoice number for the transaction. If an InvoiceNumber is not provided by the merchant, the system will utilize the TransactionSequenceNumber generated by the system in this value to the processor.
trxOrigin	Required.	The source of the transaction. If you do not submit this field, Connect 2.0 defaults to ECI. Valid values are: ECI – email or Internet MOTO – mail order/telephone order RETAIL – face-to-face
refer	Optional.	Text describing who referred the customer to your store.
comments	Optional.	Any comments about the transaction.
responseSuccessURL	Optional.	The URL to direct customers after a successful transaction (e.g., your Thank You URL). You only need to submit this value if it is not set up in Virtual Terminal.

Field	Required	Description
responseFailURL	Optional.	The URL to direct customers after a declined or unsuccessful transaction (e.g., your Sorry URL). You only need to submit this value if it is not set up in Virtual Terminal. **Note**: If you have enabled the Fraud FlexDetect^{SM} product and there is a fraud decline, the consumer will be routed automatically to this URL.
ponumber	Optional.	The purchase order number or other customer-supplied number to identify the transaction (for example, a department code.) Up to 30 characters, including spaces.
taxexempt	Optional.	Indicates that the transaction is tax exempt. Default is false. Valid values are: true false

4.1.4 Void

This transaction voids the original transaction. This transaction voids the exact amount of the original transaction, regardless of the value sent in the chargetotal field. Connect 2.0 echoes the value submitted in the chargetotal field in the response message.

Note: First Data Global Gateway Connect 2.0 does not support Partial Voids.

The following table describes the fields required for a Void transaction:

Field	Required	Description
txntype	Required.	Transaction type. If you do not submit this field, Connect 2.0 defaults to sale mode. Valid value is: void
timezone	Required.	Time zone of the transaction. Valid values are: GMT, EST, CST, MST, PST
txndatetime	Required.	Date and time of the transaction in YYYY:MM:DD-hh:mm:ss format.
hash	Required	The SHA2 hash of the following values: **storename + txndatetime + chargetotal + Shared Secret.** The values must be in this order when creating the hash. See the examples below for how to create the hash values.
storename	Required.	The Store ID provided by First Data.
mode	Optional.	The payment mode for the transaction. If you do not submit this field, Connect 2.0 defaults to PayOnly mode. Valid values are: payonly payplus fullpay
chargetotal	Required at 0.00 or greater	The total amount of the transaction, including tax and shipping. Use dot or comma separators for decimals. For example, 12.34 is $12.34. Thousandths-place separators are not allowed.
oid	Required.	The oid of the transaction being voided.
tdate	Required.	The tdate value returned for the transaction being voided.

Field	Required	Description
paymentMethod	Optional.	Allows you to specify the type of payment. If you do not submit this field, Connect 2.0 displays a drop-down menu to the customer to choose from the payment methods available for your shop. Valid values are: M – MasterCard V – Visa A – American Express C – Diners J – JCB D – Discover
userid	Optional.	A user ID allowing merchants to track their customers
invoicenumber	Optional.	The invoice number for the transaction. If an InvoiceNumber is not provided by the merchant, the system will utilize the TransactionSequenceNumber generated by the system in this value to the processor.
trxOrigin	Required.	The source of the transaction. If you do not submit this field, Connect 2.0 defaults to ECI. Valid values are: ECI – email or Internet MOTO – mail order/telephone order RETAIL – face-to-face
refer	Optional.	Text describing who referred the customer to your store.
comments	Optional.	Any comments about the transaction.
responseSuccessURL	Optional.	The URL to direct customers after a successful transaction (e.g., your Thank You URL). You only need to submit this value if it is not set up in Virtual Terminal.
responseFailURL	Optional.	The URL to direct customers after a declined or unsuccessful transaction (e.g., your Sorry URL). You only need to submit this value if it is not set up in Virtual Terminal. **Note**: If you have enabled the Fraud FlexDetect^{SM} product and there is a fraud decline, the consumer will be routed automatically to this URL.
ponumber	Optional.	The purchase order number or other customer-supplied number to identify the transaction (for example, a department code.) Up to 30 characters, including spaces.
taxexempt	Optional.	Indicates that the transaction is tax exempt. Default is false. Valid values are: true false

4.2 Check

First Data Global Gateway Connect 2.0 supports Check Sale transactions. If you need to perform a Check Void transaction on a previous Check Sale, you must use Virtual Terminal. You can only void a check transaction in the current batch.

4.2.1 Sale

The following table describes the fields required for a Check Sale transaction:

Field	Required	Description
txntype	Required.	Transaction type. If you do not submit this field, Connect 2.0 defaults to sale mode. Valid value is: sale
timezone	Required.	Time zone of the transaction. Valid values are: GMT, EST, CST, MST, PST
txndatetime	Required.	Date and time of the transaction in YYYY:MM:DD-hh:mm:ss format.
hash	Required	The SHA2 hash of the following values: **storename + txndatetime + chargetotal + Shared Secret.** The values must be in this order when creating the hash. See the examples below for how to create the hash values.
storename	Required.	The Store ID provided by First Data.
mode	Optional.	The payment mode for the transaction. If you do not submit this field, Connect 2.0 defaults to PayOnly mode. Valid values are: payonly payplus fullpay
chargetotal	Required at 0.00 or greater	The total amount of the transaction, including tax and shipping. Use dot or comma separators for decimals. For example, 12.34 is $12.34. Thousandths-place separators are not allowed.
oid	Optional.	The order ID of the transaction. If you do not submit this field, the system automatically generates a value. Limit 100 valid US character set characters.
subtotal	Required.	The subtotal amount of the transaction, before tax and shipping.
tax	Optional.	The tax amount of the transaction.
shipping	Optional.	The shipping amount of the transaction.

Field	Required	Description
paymentMethod	Optional.	Allows you to specify the type of payment. If you do not submit this field, Connect 2.0 displays a drop-down menu to the customer to choose from the payment methods available for your shop. Valid value is: 9 – Check
userid	Optional.	A user ID allowing merchants to track their customers
invoicenumber	Optional.	The invoice number for the transaction. If an InvoiceNumber is not provided by the merchant, the system will utilize the TransactionSequenceNumber generated by the system in this value to the processor.
trxOrigin	Required.	The source of the transaction. If you do not submit this field, Connect 2.0 defaults to ECI. Valid values are: ECI – email or Internet MOTO – mail order/telephone order RETAIL – face-to-face
refer	Optional.	Text describing who referred the customer to your store.
comments	Optional.	Any comments about the transaction.
responseSuccessURL	Optional.	The URL to direct customers after a successful transaction (e.g., your Thank You URL). You only need to submit this value if it is not set up in Virtual Terminal.
responseFailURL	Optional.	The URL to direct customers after a declined or unsuccessful transaction (e.g., your Sorry URL). You only need to submit this value if it is not set up in Virtual Terminal. **Note**: If you have enabled the Fraud FlexDetect^{SM} product and there is a fraud decline, the consumer will be routed automatically to this URL.
deviceId	Optional.	The DeviceID for Fraud FlexDetect^{SM} transactions. If merchant doesn't pass the DeviceID, Connect will generate the DeviceID if the merchant is using Fraud FlexDetect^{SM}.

5 Self-Hosted Payment Form Fields

If you decide to host payment forms using your server, you need to include additional fields for payment information. The required fields depend on the payment mode you use.

The following table lists describes the fields required or allowed for each payment mode:

	Required Fields		
Payment Mode	**Payment**	**Billing**	**Shipping**
PayOnly	Required.	**Credit**: Optional. **Check**: Mandatory.	Optional.
PayPlus	Required.	**Credit**: Mandatory. **Check**: Mandatory.	Optional.
FullPay	Required.	**Credit**: Mandatory. **Check**: Mandatory.	Optional.

The recurring payment and level 2 purchasing card fields are optional and can be included along with the required payment, billing, and shipping fields.

“***Please Note***: If you are actively using the Fraud FlexDetect^{SM} service, or plan on using it, we highly recommend passing more than the minimum required fields. The more fields you collect and pass, the more accurate your fraud scoring and detection system will be.

5.1 Payment Fields

After your customer has decided how to pay, you must display a form collecting the required information for the selected payment type. Some of these values may be contained in hidden fields.

5.1.1 Credit Card

The following table describes the payment fields required for a credit card transaction:

Field	Required	Description
cardnumber	Required.	The customer’s credit card number. 15-17 digits.
expmonth	Required.	The expiration month of the customer’s credit card. 2 digits.
expyear	Required.	The expiration year of the customer’s credit card. 4 digits.
cvm	Optional.	The card security code (CSC), card verification value (CVV) or code (CVC), which is typically printed on the back of the credit card. For information about using CSC, contact support. 3 or 4 digits.

Field	Required	Description
cvmnotpres	Optional.	A flag for indicating when the card code is not present on the card. Default is false. Valid values are: true false

5.1.2 Check

The following table describes the payment fields required for a check transaction:

Field	Required	Description
acnttype	Required.	Account type for the customer's check. Valid values are: PC – Personal checking PS – Personal savings BC – Business checking BS – Business savings
checknum	Required.	The check number on the customer's check.
route	Required.	The customer's bank routing number. Must be a valid, 9-digit routing number for a US bank.
accountnum	Required.	The account number for the customer's bank account.
bankname	Optional.	The name of the customer's bank.
bankstate	Optional.	The state in which the customer's bank is located.
dlnumber	Required.	The customer's driver's license number.
dlstate	Required.	The two-digit abbreviation for the state that issues the customer's driver's license.
ssn	Optional.	The customer's 9-digit social security number.
phone	Required.	The customer's phone number. Up to 20 digits.

For check transactions, billing information is mandatory and must be submitted in all payment modes.

5.2 Billing Fields

Merchants in PayPlus and FullPay mode can also submit billing information for each transaction. Check transactions require billing fields regardless of payment mode. Merchants in PayOnly mode require billing information for MOTO and ECI transactions. Connect 2.0 downgrades these transactions if you do not submit billing information.

The following table describes the billing fields:

Field	Required	Description
bcompany	Not required.	The customer's company. Alphanumeric characters, spaces, and dashes.
bname	Required.	The customer's name. Alphanumeric characters, spaces, and dashes.
baddr1	Required.	The first line of the customer's address. Up to 30 characters, including spaces.
baddr2	Not required.	The second line of the customer's address. Up to 30 characters, including spaces.
bcity	Required.	The customer's city. Up to 30 characters, including spaces.
bstate	Required.	The customer's state. For US customers. 2 letters.
bstate2	Not required.	The customer's province or territory. Up to 30 characters, including spaces.
bcountry	Required.	The customer's 2-letter country code
bzip	Required.	The customer's ZIP or postal code.
phone	Not required.	The customer's phone number. Up to 20 digits.
fax	Not required.	The customer's fax number. Up to 20 digits.
email	Not required.	The customer's email address. Up to 45 characters.

5.3 Shipping Fields

Merchants in FullPay mode can also submit shipping information for each transaction.

The following table describes the shipping fields:

Field	Required	Description
sname	Not required.	The recipient's name. Alphanumeric characters, spaces, and dashes.
saddr1	Not required.	The first line of the recipient's address. Up to 30 characters, including spaces.
saddr2	Not required.	The second line of the recipient's address. Up to 30 characters, including spaces.
scity	Not required.	The recipient's city. Up to 30 characters, including spaces.
sstate	Not required.	The recipient's state. For US customers. 2 letters.
sstate2	Not required.	The recipient's province or territory. Up to 30 characters, including spaces.
scountry	Not required.	The recipient's 2-letter country code
szip	Not required.	The recipient's ZIP or postal code.

5.4 Recurring Payment Fields

The following table describes the fields required to perform a recurring transaction:

Field	Required	Description
submode	Required.	Indicated a recurring payment. Valid value is: periodic
periodicity	Required.	The period of the installment. Combines with the frequency to determine when the installments occur. Valid values are: d – Day w – Week m – Month y – Year
frequency	Required.	The frequency of the installment. Combines with the periodicity to determine when the installments occur. Numeric value between 1-999.
startdate	Required.	The start date of the recurring payment transaction in YYYYMMDD format.
installments	Required.	The number of installments of the recurring payment. Numeric value between 1-999.
threshold	Required.	The number of failures to allow before the merchant is notified by email. Numeric value between 1-5.

5.5 Level 2 Purchasing Card Fields

A purchasing card is a corporate card used by some companies for their business purchases. The following information must be included with the order information for purchasing cards. This information is optional for a regular credit card transaction.

1. You must determine whether the order is tax exempt or not. If the order is tax exempt, you must set the tax exempt value to 1 or True.

```
<input type="hidden" name="taxexempt" value="1">
```

2. If the order is not tax exempt, then the **tax** field must be populated with the appropriate tax amount for the order (a value from 0.01 to 99999.99).

```
<input type="hidden" name="tax" value="1.35">
```

3. You must enter a value in the **ponumber** field associated with the order. The **ponumber** field can be populated with any customer-supplied alphanumeric value.

For example, the purchase order (PO) number can be a customer code associated with the purchasing card or a purchase order number. It cannot be the same as the order ID number (oid). The customer supplies the value for the ponumber. The same ponumber may be used for several orders.

```
<input type="text" name="ponumber" size="25">
```

Please note that the Level 2 Purchasing Card transaction will be downgraded if all the necessary data is not included at the time of the request. ponumber and tax are two of those fields.

The following table contains the minimum required fields to run Level 2 Purchasing Card transaction.

Level 2 Purchasing Cards Fields				
Field Name	**Possible Values**	**Description**	**Required**	**Sample HTML**
Chargetotal	Credit Cards - 0.01 - 99999.99 Checks - 0.01 - 5000.00	The chargetotal amount of the transaction. Subchargetotal, shipping, and tax must add up to the Chargetotal.	Yes	`<INPUT type="hidden" name="Chargetotal" value="13.99">`
mode	payplus, fullpay, payonly	The payment mode. If used, the value must be set to one of the three values: PayPlus, Fullpay, or PayOnly. If this field is not used, the secure payment gateway will collect all the fields required for the transaction that were not included on the merchant order form.	No	`<input type="hidden" name="mode" value="fullpay">`
storename	6 to 10-digit integer	Used to identify your merchant store to the secure payment gateway. Use the store number from your Welcome Email.	Yes	`<input type="hidden" name="storename" value="123456">`
baddr1	Up to 96 alphanumeric characters	Billing address. Cannot be all spaces.	Required for PayPlus mode.	`<input type="text" name="baddr1" size="30" maxlength="30">`

Level 2 Purchasing Cards Fields				
Field Name	Possible Values	Description	Required	Sample HTML
bzip	5-digit zip code (for US orders) or international postal code	Billing zip or postal code.	Required for PayPlus mode if country is US.	`<input type="text" name="bzip" size="5" maxlength="10">`
ponumber	Limit of 128 alphanumeric characters	Purchase order number or other customer-supplied value, such as a department code.	Required for purchasing card transactions.	`<input type="text" name="ponumber" size="30" maxlength="30">`
Tax	Number from 1 to 99999.99	Tax applied to the order. The chargetotal must equal the sum of the subchargetotal, shipping, and tax.	Required for purchasing card transactions if the order is not tax exempt.	`<input type="hidden" name="tax">`
taxexempt	True	Used to indicate whether the purchase is tax exempt. Value must be set to either True (1) or not passed. If you use a checkbox for this field, when it is selected the value is True. When the checkbox is not selected, the field is not sent.	Required for purchasing card transactions.	`<input type="checkbox" name="taxexempt" value="true">`

6 Additional Custom Fields

You may send as many custom fields to the gateway as you wish. Custom field values are returned along with all other fields to the response URL.

It is also possible to document up to fifteen custom fields in your store configuration. You may use these fields to gather additional customer data geared toward your business specialty, or you may use them to gather additional customer demographic data which you can then store in your own database for future analysis.

Custom Fields need to be created by merchant on their website and values passed to Connect 2.0 Application. Connect 2.0 will pass the values over back to Merchant in the response after processing the transaction.

Note: If these fields need to be displayed post-checkout, the merchant must generate the necessary code to take such action.

7 Transaction Response

After you process a transaction with First Data Global Gateway Connect 2.0, the secure payment gateway returns information to your web server. The information returned from the secure payment gateway includes:

- Response Fields
- Fraud Block Messages from Basic Fraud Settings
- Fraud Score and Disposition if using Fraud FlexDetect^{SM}
- TeleCheck Errors

For credit cards, the approval code is returned. The approval code shows the AVS and Card Code Comparison result.

The approval code is returned in the **Approval Code** field. The field will be set to a value containing a string of 6 alphanumeric characters. An example of an approval code is:

```
Y:0097820000019564:YNAM:12345678901234567890123:
```

The Y at the beginning of the string indicates that this transaction was approved. The next 6 digits of this string (009782) are the approval number.

The next 10 digits (0000019564) are the reference number.

The first three alphabetic characters in the middle (YNA) are the AVS Code. The AVS code can help you prevent fraud and costly chargebacks. For more information, see the "AVS Codes section

The last alphabetic character in the middle (M) is a code indicating whether the card code matched the card-issuing bank's code. An "M" indicates the code matched.

Depending on whether the card code was passed and the service was available for the type of card used, this code may or may not be present. For more information on card codes, See "Card Codes" section.

The remaining portion of the approval code (12345678901234567890123) is the Lease Line transaction identifier. Not all transactions have an associated Lease Line transaction identifier.

Note: Connect 2.0 only utilized the *en* (US English) character set. Transaction response field names are case sensitive. The usage of international character sets may produce unpredictable results within Connect 2.0.

7.1 Response Fields

After a transaction is processed, First Data Global Gateway Connect 2.0 posts response fields to your web site.

Response fields include:

- All fields, including custom fields, posted from the merchant order form.
- Extra fields indicating the status of the transaction.

The following table displays the response fields indicating the status of the transaction.

<table>
<tr><th>Field Name</th><th>Possible Values</th><th>Description</th></tr>
<tr><td>approval_code</td><td>0097820000019564:YNAM:
12345678901234567890123</td><td>Used for credit card orders only. Unique approval code for the transaction. Includes AVS and Card Code response for credit card orders</td></tr>
<tr><td>status</td><td>For credit cards: Approved, Declined, or Fraud.
For checks: Approved or Declined.
For Fraud FlexDetect^{SM}:
If the merchant is enabled for Fraud FlexDetect^{SM} and the transaction response is “APPROVED” the following will be displayed to the shopper:
<table>
<tr><th>Transaction Response</th><th>Fraud Response</th><th>Display Message</th></tr>
<tr><td>Approved</td><td>Accept</td><td>Approved</td></tr>
<tr><td>Approved</td><td>Review</td><td>Approved</td></tr>
<tr><td>Approved</td><td>Reject</td><td>Declined</td></tr>
<tr><td>Approved (check)</td><td>Not scored by Fraud FlexDetect^{SM}</td><td>Approved</td></tr>
<tr><td>Declined</td><td>Not scored by Fraud FlexDetect^{SM}</td><td>Declined</td></tr>
<tr><td>Fraud</td><td>Not scored by Fraud FlexDetect^{SM}</td><td>Declined</td></tr>
</table>
</td><td>Approval status for the order.</td></tr>
<tr><td>fail_reason</td><td>Any error message.</td><td>Provides additional information about errors and declines.</td></tr>
</table>

Field Name	Possible Values	Description
oid	A string of numbers and letters. 60.222.10.60-1064863861 -337-503200-1	Unique order ID number for the transaction. If the number is not posted by the merchant web site, the secure payment gateway automatically assigns an order ID to each transaction.
ttime	Day Month Date hh:mm:ss yyyy. Example: Thu Sep 18 09:14:32 2007	Date and time the transaction occurred.
response_hash		Outbound SHA2 hash of transaction data. Hash derived from the following: ***Shared Secret*** + *approval_code* + *chargetotal* + *currency-code* (**note1**) + *txndatetime* (**note 2**) + *storied* **note 1** – Currently, the FDGG only supports USD (currency code 840). **note 2**—txndatetime refers to the txndatetime string used to generate the original hash value of the transaction.

7.2 Fraud Block Messages

When a transaction is blocked because of the Basic Fraud Setting as defined by the merchant, the following messages may appear in the **r-error** data field.

Message	Description
The host you are ordering from has been blocked.	The merchant has blocked the customer's host from making transactions.
The credit card you are using has been blocked.	The merchant has blocked the customer's credit card number from making transactions.
The domain of your host has been blocked.	The merchant has blocked the customer's domain name from making transactions.
The class C subnet for this IP has been blocked.	The merchant has blocked the customer's Class C address from making transactions.
The name that was entered has been blocked.	The merchant has temporarily blocked the customer's name from making transactions.

Message	Description
The credit card you are using has been temporarily blocked.	The merchant has temporarily blocked the customer's credit card from making transactions.
The purchase amount exceeds the merchant approved limit.	The chargetotal amount of the order exceeds the maximum purchase limit set by the merchant.
Merchant transaction limit is less than the amount requested for that transaction.	The chargetotal amount of the order is less than the minimum purchase limit set by the merchant.
Duplicate	A Transaction for the identical dollar amount and the identical credit card number was processed within the last X hours. X is generally 24 hours, but can be altered by changing the duplicate lockout time in the merchant's fraud protection settings.

7.3 TeleCheck Errors

The errors below may be returned from the API when a validation or transmission error occurs when processing a TeleCheck transaction.

Error Code	Error Message	Comments
Status code 0	duplicate txn, stop	Two identical transactions were received. This is the second, which will not be processed.
Status code 10	Invalid parameters	Check input parameter format and validity. Check that all required parameters were included.
Status code 20	Dig Sig invalid	Check the digital certificate for the merchant site.
Status code 30	User Canceled auth -Or- incomplete data	User canceled the transaction, or not all required fields were provided.
Status code 40	User account error -Or- We are sorry that we cannot accept your check at this time. Our decision is based, in whole or in part, on information provided to us by TeleCheck. We encourage you to call TeleCheck at 1-877-678- 5898 or write TeleCheck Customer Care at P.O. Box 4513, Houston, TX 77210- 4513. Please provide TeleCheck your driver’s license number and the state where it was issued, and the complete banking numbers printed on the bottom of your check. Under the Fair Credit Reporting Act, you have the right to a free copy of your information held in TeleCheck’s files within 60 days from today. You may also dispute the accuracy or completeness of any information in TeleCheck’s customer report. TeleCheck did not make the adverse decision to not accept your check and is unable to explain why this decision was made.	If this text block is included with the response, the merchant has a legal obligation to display it to the customer.
Status code 50	System not available	Contact customer support if the problem persists.

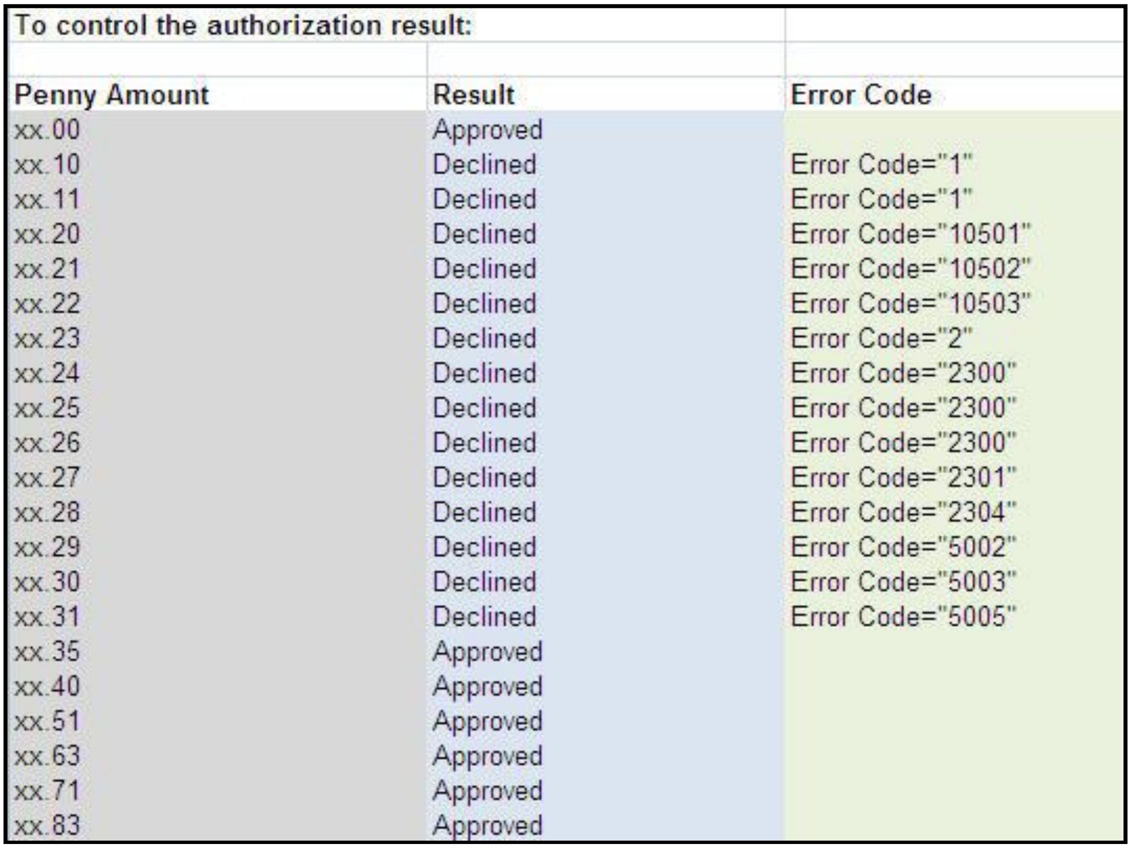
Error Code	Error Message	Comments
110	Payment Authorization Invalid	There is no matching authorization for this merchant, the authorization has expired, or is voided. This error message can also indicate the transaction cannot be voided because a payment has already been requested for the authorization. The merchant must correct the problem and resubmit the Clearing Request as appropriate.
120	Clearing entry invalid	One or more fields were missing or malformed. The merchant must correct the problem and resubmit the Clearing Request as appropriate.
130	Transfer amount invalid	The amount requested, or the sum of all partial payments up to and including this transaction, exceed the original authorization amount. This error can also indicate the amount field was malformed. The merchant must correct the problem and resubmit the Clearing Request as appropriate.
140	Account Disabled	The user or merchant account has been disabled The merchant should verify the account status or contact the user to find another payment method.
180	Authorization Void confirmation	Confirmation to the merchant that an Authorization Void was received and completed. This is initiated by the merchant or user. If initiated by the user, the **Message** field will contain additional information.
210	Account Invalid	User's checking account is no longer active. TeleCheck will attempt to contact the user to correct the problem. If unsuccessful, the merchant will receive a Funds Transfer Notification with a debit or credit as necessary to reverse the transaction.
220	Stop Payment	The user has placed a stop payment on this specific transaction. No action required. This is a notification.
230	NSF	Insufficient funds notification. TeleCheck will attempt twice to transfer funds, as specified by the merchant. The user will also be contacted to correct the problem. If successful, the merchant will not receive any other notifications. If funds cannot be obtained from the user, they will be reversed from the merchant's account.
240	Final NSF	Insufficient funds notification. Funds will be reversed from the merchant's account. The merchant will receive a Funds Transfer Notification with a debit or credit as necessary to reverse the transaction.

Error Code	Error Message	Comments
LP-8996	Non-live TeleCheck transactions are not supported	TeleCheck account not set up yet. Check with your sales agent or merchant services on account status. Contact customer support if problem persists.
32001	CheckErr: Invalid order data	Invalid order data.
32002	CheckErr: Invalid check data	Invalid check data.
32003	CheckErr: Invalid request	Invalid request.
32004	CheckErr: Invalid account type	Invalid account type.
32005	CheckErr: Invalid transit routing	Invalid transit routing.
32006	CheckErr: Invalid MICR	Invalid MICR.
32007	CheckErr: Invalid check number	Invalid check number.
32008	CheckErr: Invalid check comment	Invalid check comment.
32009	CheckErr: Routing number does not match	Routing number does not match.
32010	CheckErr: Check order type is wrong	Check order type is wrong.
32011	CheckErr: Invalid check order data	Invalid check order data.
32012	CheckErr: Error inserting order	Error inserting order.
32013	CheckErr: Error inserting transaction	Error inserting transaction.
32014	CheckErr: Error inserting batch transaction	Error inserting batch transaction.
32015	CheckErr: Unable to verify check processing status	Unable to verify check-processing status.
32016	CheckErr: Error deleting check batch entry	Error deleting check batch entry.
32017	CheckErr: Check sent for processing	You may be trying to void a check that has been sent for processing.
32018	CheckErr: Error voiding check	Error voiding check.
32019	CheckErr: Error updating transaction	Error updating transaction.

7.3.1 Other TeleCheck Messages

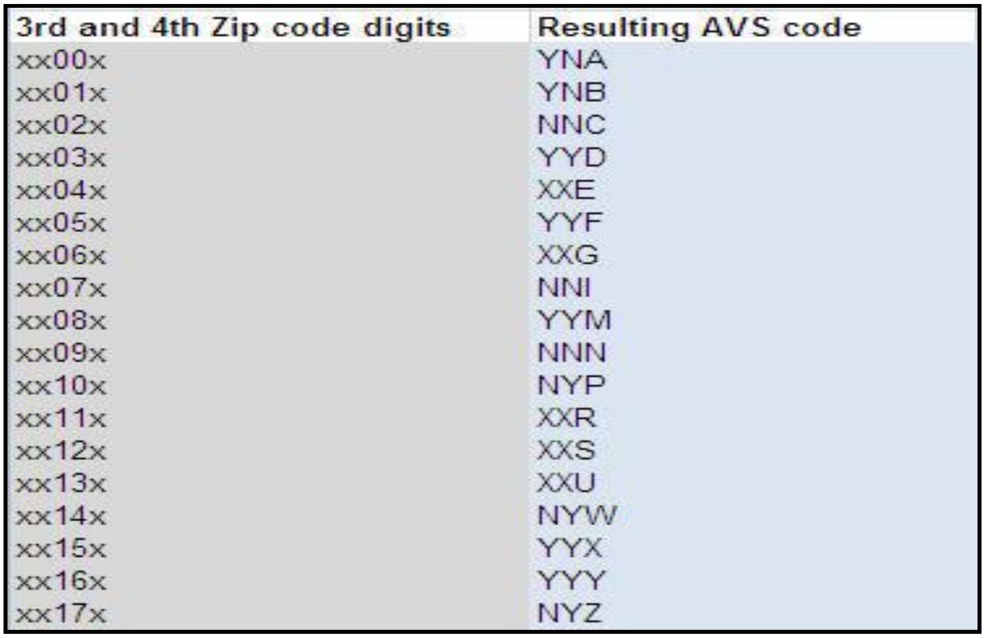
- Your session has expired.
- You have exceeded the maximum number of authorization attempts. Please choose another payment option.
- We are unable to verify your checking account information. Please review the information you entered to ensure that all information is correct, and then click Authorize.
- We are unable to verify your checking account information because your bank account may not be set up to handle electronic funds transfers through the Automated Clearing House (ACH). Please contact your bank to determine whether this account accepts Automated Clearing House (ACH) transactions. If you have another checking account, you may change your routing and account number information below.
- Please enter a First Name.
- Please enter a valid First Name.
- Please enter a Last Name.
- Please enter a valid Last Name.
- Please enter an Address.
- Please enter a valid Address (Address Line 1).
- Please enter a valid Address (Address Line 2).
- Please enter a City.
- Please enter a valid City.
- Please enter your entire Driver's License or State ID Number.
- Please verify all information is entered correctly. Submit your request again. You may also select another payment option.
- Please enter a valid Driver's License or State ID Number.
- Please select the state where your Driver's License or State ID was issued.
- Please select a State.
- Please enter a ZIP Code.
- Please enter a valid ZIP Code.
- Please enter an Email.
- Please enter a valid Email.
- Please enter a Home Phone Number.
- Please enter a valid Home Phone Number.
- Please enter the name of your Bank.
- Please enter valid information for the name of your Bank.
- Please select a Bank State.
- Please enter a Routing Number.
- Please enter a valid Routing Number.
- Please enter a Checking Account Number.
- Please enter a valid Checking Account Number.

7.4 Test Account Simulator Responses (Credit) :



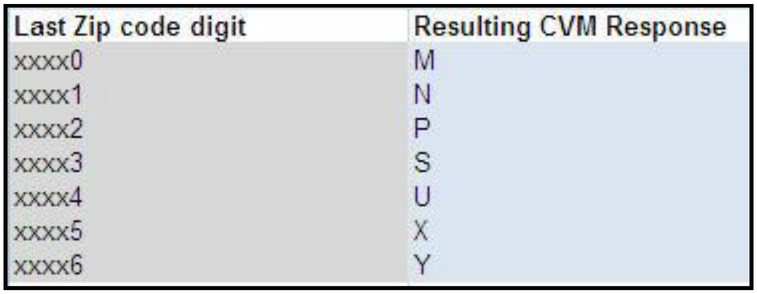
To control the authorization result:		
Penny Amount	**Result**	**Error Code**
xx.00	Approved	
xx.10	Declined	Error Code="1"
xx.11	Declined	Error Code="1"
xx.20	Declined	Error Code="10501"
xx.21	Declined	Error Code="10502"
xx.22	Declined	Error Code="10503"
xx.23	Declined	Error Code="2"
xx.24	Declined	Error Code="2300"
xx.25	Declined	Error Code="2300"
xx.26	Declined	Error Code="2300"
xx.27	Declined	Error Code="2301"
xx.28	Declined	Error Code="2304"
xx.29	Declined	Error Code="5002"
xx.30	Declined	Error Code="5003"
xx.31	Declined	Error Code="5005"
xx.35	Approved	
xx.40	Approved	
xx.51	Approved	
xx.63	Approved	
xx.71	Approved	
xx.83	Approved	

To control the AVS response, pass the Zip Code digits specified below:



3rd and 4th Zip code digits	Resulting AVS code
xx00x	YNA
xx01x	YNB
xx02x	NNC
xx03x	YYD
xx04x	XXE
xx05x	YYF
xx06x	XXG
xx07x	NNI
xx08x	YYM
xx09x	NNN
xx10x	NYP
xx11x	XXR
xx12x	XXS
xx13x	XXU
xx14x	NYW
xx15x	YYX
xx16x	YYY
xx17x	NYZ

To control the CVM response pass the ZIP Code digit specified below:



Last Zip code digit	Resulting CVM Response
xxxx0	M
xxxx1	N
xxxx2	P
xxxx3	S
xxxx4	U
xxxx5	X
xxxx6	Y

7.5 Test Account Simulator Responses (Fraud FlexDetect^{SM}) :

To control Fraud FlexDetect^{SM} response values pass the cents value as specified below:

Penny Amount	Simulated Fraud FlexDetect^{SM} Response
>= 0 and <= 09	Auto Accept
>= 51 and <= 55	Auto Reject
>=56 and <= 60	Pending Review & Manual Accept
>=61 and <=65	Pending Review & Manual Reject
>=66 and <=70	Pending Review & Time Trigger Accept
>=71 and <=75	Pending Review & Time Trigger Reject
>=76 and <=80	Error/No Score
>=81 and <=85	Not Qualified Transaction for Score
>=86 and <=90	Timeout

8 3-D Secure (aka Payer Auth., Verified by Visa and MasterCard SecureCode)

The First Data Internet Payment Gateway includes the ability to authenticate transactions using Verified by Visa and MasterCard SecureCode. If your credit card agreement includes 3-D Secure and your Merchant ID has been activated to use this service, you do not need to modify your payment page.

If you are enabled to submit 3-D Secure transactions but want to submit specific transactions without using the 3-D Secure protocol, you can use the additional parameter *authenticateTransaction* and set it to either “true” or “false”.

Example for a transaction without 3-D Secure:

```
<input type="hidden" name="authenticateTransaction" value="false"/>
```

If 3-D Secure authentications cannot be processed successfully for technical reason, for example, one of the systems involved in the authentication process is temporarily not responding, the payment transaction will be processed as a “regular” eCommerce transaction (GICC ECI 1 & 7). **A liability shift to the card issuer for possible chargebacks is not warranted in this case.**

Please note that the technical process of 3-D Secure transactions differs in some points compared to a normal authorization flow. If you already have an existing shop integration and plan to activate 3-D Secure subsequently, we recommend performing some test transactions on our test environment.

Additional 3-D Secure integration support can be obtained by contacting the technical support desk at 1-888-477-3611.

9 Technical Integration Appendix

This section provides the additional technical information which would be helpful for the Integration.

9.1 ASP Example

The following ASP example shows a simple page that communicates with the First Data Global Gateway Connect 2.0. When customers click **Submit**, they are redirected to the secure forms hosted by First Data where they can enter their billing, shipping and payment information. After completing payment, Connect 2.0 redirects customers back to the merchant's receipt page, which is set in Virtual Terminal or using optional form fields.

```
<!-- connect.asp -->
<!-- #include file="fdgg-util_sha2.asp"-->
<html>
   <head>
      <meta http-equiv="Content-Type"
         content="text/html; charset=ISO-8859-1">
      <title>FDGG Connect Sample for ASP</title>
   </head>

    <script type="text/javascript">
        function forward(){
         var identifier =
'<%Response.Write(Request.Form("identifier"))%>'
         if(identifier){
            /* For Merchant Test Environment (CTE) */

   //document.redirectForm.action="https://connect.merchanttest.firstdata
globalgateway.com/IPGConnect/gateway/processing";
            /* For Production Environment (PROD) */

   document.redirectForm.action="https://connect.firstdataglobalgateway.c
om/IPGConnect/gateway/processing";
            document.redirectForm.submit();
         }
      }
    </script>
   <BODY onLoad="forward()">

 <% If len(Request.Form("identifier")) = 0 Then  %>
     <P>

      <H1>Order Form </H1>
     <FORM action=<%=CStr(chr(34)) + CStr(Request.ServerVariables("URL"))
+ "?" + CStr(Request.ServerVariables("QUERY_STRING")) + CStr(chr(34))%>
method=post><BR>
      <TABLE border=0>
      <TBODY>
   <TR>
         <TD>Transaction Type</TD>
            <TD>
               <INPUT type=radio CHECKED value=sale name=txntype>Sale<BR>
               <INPUT type=radio value=preauth name=txntype>Authorize
Only<BR>
```

```
               <INPUT type=radio value=postauth name=txntype>Ticket
Only<BR>
               <INPUT type=radio value=void name=txntype>Void<BR>
            </TD>
         </TR>
         <TR>
            <TD>* Credit Card Type</TD>
            <TD><SELECT size=1 name=paymentMethod> <OPTION value=V
selected>Visa</OPTION>
               <OPTION value=M>MasterCard</OPTION> <OPTION
value=A>American
               Express</OPTION> <OPTION value=D>Discover</OPTION> <OPTION
value=J>JCB</OPTION> <OPTION value=9>Check</OPTION>
               <OPTION value="">Other</OPTION>
               </SELECT></TD>
         <TR>
         <TR>
            <TD>* Payment Mode:</TD>
            <TD><SELECT name=mode> <OPTION value=payonly
selected>PayOnly</OPTION>
            <OPTION value=payplus>PayPlus</OPTION> <OPTION
            value=fullpay>FullPay</OPTION> <OPTION
value=""></OPTION></SELECT> </TD></TR>
         <TR>
            <TD>Transaction Origin</TD>
            <TD>
               <INPUT type=radio value=RETAIL name=trxOrigin>RETAIL<BR>
               <INPUT type=radio value=MOTO name=trxOrigin>MOTO<BR>
               <INPUT type=radio CHECKED value=ECI name=trxOrigin>ECI<BR>
            </TD>
         </TR>
         <TR>
            <TD>OrderId</TD>
            <td>
               <input type="text" name="oid" value=""/>
            </td>
         </TR>
         <tr>
            <td>Transaction Date</td>
            <td>
            <input type="text" name="tdate" value=""/>
            </td>
         </tr>
         <TR>
            <TD>* Charge Total:</TD>
            <TD><INPUT value=11.00 name=chargetotal> </TD></TR>
         <TR>
             <TD>* Sub Total:</TD>
             <TD><INPUT value=11.00 name=subtotal> </TD></TR>
         <TR>
         <TD></TD></TR>
         <TR>
            <TD></TD></TR>
         <TR>
            <TD align=middle colSpan=2><INPUT type=submit value="Submit
This Form" name=submitBtn></TD></TR></TBODY></TABLE>
            <input type="hidden" name="identifier" value="true" />
```

```
      </FORM>

      <% Else %>

        <FORM method="post" id="redirectForm" name="redirectForm">

      <%
         formattedDate = getFormattedDate()

         mode = Request.Form("mode")
         chargetotal = Request.Form("chargetotal")
         subtotal = Request.Form("subtotal")
         storename = getStoreName()
         sharedsecret = getSharedSecret()
         timezone = getTimeZone()


         str = storename + formattedDate + chargetotal + sharedsecret
         hex_str = ""
         for i = 1 to len(str)
            hex_str = hex_str + lcase(cstr(hex(asc(mid(str, i, 1)))))
         next

         createdHash = SHA256(hex_str)
         'Response.Write("<p><b>createdHash:</b> " & createdHash &
"</p>")

      %>
         <input type="hidden" name="timezone" value="<%
Response.Write(timezone)%>" />
         <input type="hidden" name="authenticateTransaction"
value="false" />
         <input size="50" type="hidden" name="paymentMethod" value="<%
Response.Write(Request.Form("paymentMethod"))%>" />
         <input size="50" type="hidden" name="txntype" value="<%
Response.Write(Request.Form("txntype"))%>" />
         <input size="50" type="hidden" name="txndatetime" value="<%
Response.Write(formattedDate)%>" />
         <input size="50" type="hidden" name="hash" value="<%
Response.Write(createdHash)%>" />
         <input size="50" type="hidden" name="mode" value="<%
Response.Write(Request.Form("mode"))%>" />
         <input size="50" type="hidden" name="storename" value="<%
Response.Write(storename) %>" />
         <input size="50" type="hidden" name="chargetotal" value="<%
Response.Write(chargetotal) %>"/>
         <input size="50" type="hidden" name="subtotal" value="<%
Response.Write(subtotal) %>" />

         <input size="50" type="hidden" name="trxOrigin" value="<%
Response.Write(Request.Form("trxOrigin"))%>" />
         <input size="50" type="hidden" name="oid" value="<%
Response.Write(Request.Form("oid"))%>" />
         <input size="50" type="hidden" name="tdate" value="<%
Response.Write(Request.Form("tdate"))%>" />
```

```
     </FORM>
   <%End If%>
</BODY>
</HTML>
```

The fdgg-util_sha2.asp file (see 9.6 fdgg-util_sha2.asp reference below) includes code for generating a SHA2 hash, as required by First Data. The hash in the example ensures that this merchant is the only merchant that can send in transactions for this store.

Note: The POST URL used is for integration testing only. When you are ready to go into production, please contact First Data for the live production URL.

Sample code is presented for educational purposes only.

Your specific environment should be considered when integrating to Connect 2.0. Processing environments (Windows, Linux, AIX, etc…) and scripting environments (ASP, JSP or PHP) should be considered and reflected in the integration effort to Connect 2.0.

9.2 PHP Example

The following PHP example shows a simple page that communicates with the First Data Global Gateway Connect 2.0. When customers click **Submit**, they are redirected to the secure forms hosted by First Data where they can enter their billing, shipping and payment information. After completing payment, Connect 2.0 redirects customers back to the merchant's receipt page, which is set in Virtual Terminal or using optional form fields.

```
<!-- connect.php -->
<?php include("fdgg-util_sha2.php"); ?>

<HTML>
<head><title>FDGG Connect Sample for PHP</title></head>

   <script type="text/javascript">
      function forward(){
         var identifier = '<?php echo $_REQUEST["identifier"]; ?>';

         if(identifier){
            /* For Merchant Test Environment (CTE) */

   //document.redirectForm.action="https://connect.merchanttest.firstdata
globalgateway.com/IPGConnect/gateway/processing";
            /* For Production Environment (PROD) */

   document.redirectForm.action="https://connect.firstdataglobalgateway.c
om/IPGConnect/gateway/processing";
            document.redirectForm.submit();
         }
      }
   </script>

   <BODY onLoad="forward()">

   <?php if ($_REQUEST["identifier"]== NULL ) { ?>

     <P>
      <H1>Order Form </H1>
     <!--<FORM action="/connect_p.php"  method=post name="mainform"><BR>-
->
     <FORM action="<?php echo $_SERVER['REQUEST_URI']; ?>"  method="post"
name="mainform"><BR>
      <TABLE border=0>
      <TBODY>
         <TR>
         <TD>Transaction Type</TD>
            <TD>
               <INPUT type=radio CHECKED value=sale name=txntype>Sale<BR>
               <INPUT type=radio value=preauth name=txntype>Authorize
Only<BR>
               <INPUT type=radio value=postauth name=txntype>Ticket
Only<BR>
               <INPUT type=radio value=void name=txntype>Void<BR>

            </TD>
         </TR>
         <TR>
            <TD>* Credit Card Type</TD>
            <TD><SELECT size=1 name=paymentMethod> <OPTION value=V
selected>Visa</OPTION>
               <OPTION value=M>MasterCard</OPTION> <OPTION
value=A>American
               Express</OPTION> <OPTION value=D>Discover</OPTION> <OPTION
value=J>JCB</OPTION> <OPTION value=9>Check</OPTION>
               <OPTION value="">Other</OPTION>
               </SELECT></TD>
         <TR>
         <TR>
            <TD>* Payment Mode:</TD>
            <TD><SELECT name=mode> <OPTION value=payonly
selected>PayOnly</OPTION>
            <OPTION value=payplus>PayPlus</OPTION> <OPTION
            value=fullpay>FullPay</OPTION> <OPTION
value=""></OPTION></SELECT> </TD></TR>
         <TR>
            <TD>Transaction Origin</TD>
            <TD>
               <INPUT type=radio value=RETAIL name=trxOrigin>RETAIL<BR>
               <INPUT type=radio value=MOTO name=trxOrigin>MOTO<BR>
               <INPUT type=radio CHECKED value=ECI name=trxOrigin>ECI<BR>

            </TD>
         </TR>
         <TR>
            <TD>OrderId</TD>
            <td>
               <input type="text" name="oid" value=""/>
            </td>
         </TR>
         <tr>
            <td>Transaction Date</td>
            <td>
            <input type="text" name="tdate" value=""/>
            </td>
         </tr>
         <TR>
            <TD>* Charge Total:</TD>
            <TD><INPUT value=11.00 name=chargetotal> </TD></TR>

         <TR>
             <TD>* Sub Total:</TD>
             <TD><INPUT value=11.00 name=subtotal> </TD></TR>
         <TR>
         <TD></TD></TR>
         <TR>
            <TD></TD></TR>
         <TR>
            <TD align=middle colSpan=2><INPUT type=submit value="Submit
This Form" name=submitBtn></TD></TR></TBODY></TABLE>
            <input type="hidden" name="identifier" value="true" />
      </FORM>

       <?php } else {?>
       <FORM method="post" id="redirectForm" name="redirectForm">

       <?php
         $mode = $_REQUEST["mode"];
         $chargetotal = $_REQUEST["chargetotal"];
         $subtotal = $_REQUEST["subtotal"];

       ?>

         <input type="hidden" name="timezone" value="<?php echo
getTimezone() ?>" />
         <input type="hidden" name="authenticateTransaction"
value="false" />
         <input size="50" type="hidden" name="paymentMethod" value="<?php
echo $_REQUEST["paymentMethod"] ?>"/>
         <input size="50" type="hidden" name="txntype" value="<?php echo
$_REQUEST["txntype"] ?>"/>
         <input size="50" type="hidden" name="txndatetime" value="<?php
echo getDateTime() ?>" />
         <input size="50" type="hidden" name="hash" value="<?php echo
createHash($chargetotal) ?>" />
         <input size="50" type="hidden" name="mode" value="<?php echo
$mode ?>"/>
         <input size="50" type="hidden" name="storename" value="<?php
echo getStorename() ?>"/>
         <input size="50" type="hidden" name="chargetotal" value="<?php
echo $chargetotal ?>"/>
         <input size="50" type="hidden" name="subtotal" value="<?php echo
$subtotal ?>"/>

         <input size="50" type="hidden" name="trxOrigin" value="<?php
echo $_REQUEST["trxOrigin"] ?>"/>
         <input size="50" type="hidden" name="oid" value="<?php echo
$_REQUEST["oid"] ?>"/>
         <input size="50" type="hidden" name="tdate" value="<?php echo
$_REQUEST["tdate"] ?>"/>

      </FORM>
     <?php } ?>
  </BODY>
 </HTML>
```

The fdgg-util_sha2.php file (see 07

fdgg-util_sha2.php reference below) includes code for generating a SHA2 hash, as required by First Data. The hash in the example ensures that this merchant is the only merchant that can send in transactions for this store.

Note: The POST URL used is for integration testing only. When you are ready to go into production, please contact First Data for the live production URL.

Sample code is presented for educational purposes only.

Your specific environment should be considered when integrating to Connect 2.0. Processing environments (Windows, Linux, AIX, etc…) and scripting environments (ASP, JSP or PHP) should be considered and reflected in the integration effort to Connect 2.0.

9.3 JSP Example

The following JSP example shows a simple page that communicates with the First Data Global Gateway Connect 2.0. When customers click **Submit**, they are redirected to the secure forms hosted by First Data where they can enter their billing, shipping and payment information. After completing payment, Connect 2.0 redirects customers back to the merchant's receipt page, which is set in Virtual Terminal or using optional form fields.

```
<!-- connect.jsp -->
<%@ include file="fdgg-util_sha2.jsp" %>
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
   pageEncoding="ISO-8859-1"%>

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
  <HTML>

     <head>
      <meta http-equiv="Content-Type"
         content="text/html; charset=ISO-8859-1">
      <title>FDGG Connect Sample for JSP</title>
   </head>

   <script type="text/javascript">
   function forward(){
      var identifier = <%=request.getParameter("identifier")%>
      if(identifier != null){

       /* For Merchant Test Environment (CTE) */

//document.redirectForm.action="https://connect.merchanttest.firstdataglo
balgateway.com/IPGConnect/gateway/processing";

      /* For Production Environment (PROD) */

   document.redirectForm.action="https://connect.firstdataglobalgateway.c
om/IPGConnect/gateway/processing";
      document.redirectForm.submit();
       }
   }
   </script>
   <BODY onLoad="forward()">

    <% if(request.getParameter("identifier")== null){ %>

     <P>
      <H1>Order Form </H1>
     <FORM action='<%=request.getRequestURI()%>'  method="post"
name="mainform"><BR>
      <TABLE border=0>
      <TBODY>
         <TR>
         <TD>Transaction Type</TD>
            <TD>
               <INPUT type=radio CHECKED value=sale name=txntype>Sale<BR>
               <INPUT type=radio value=preauth name=txntype>Authorize
Only<BR>
               <INPUT type=radio value=postauth name=txntype>Ticket
Only<BR>
               <INPUT type=radio value=void name=txntype>Void<BR>

            </TD>
         </TR>
         <TR>
            <TD>* Credit Card Type</TD>
            <TD><SELECT size=1 name=paymentMethod> <OPTION value=V
selected>Visa</OPTION>
               <OPTION value=M>MasterCard</OPTION> <OPTION
value=A>American
               Express</OPTION> <OPTION value=D>Discover</OPTION> <OPTION
value=J>JCB</OPTION> <OPTION value=9>Check</OPTION>
               <OPTION value="">Other</OPTION>
               </SELECT></TD>
         <TR>
         <TR>
            <TD>* Payment Mode:</TD>
            <TD><SELECT name=mode> <OPTION value=payonly
selected>PayOnly</OPTION>
            <OPTION value=payplus>PayPlus</OPTION> <OPTION
            value=fullpay>FullPay</OPTION> <OPTION
value=""></OPTION></SELECT> </TD></TR>
         <TR>
            <TD>Transaction Origin</TD>
            <TD>
               <INPUT type=radio value=RETAIL name=trxOrigin>RETAIL<BR>
               <INPUT type=radio value=MOTO name=trxOrigin>MOTO<BR>
               <INPUT type=radio CHECKED value=ECI name=trxOrigin>ECI<BR>

            </TD>
         </TR>
         <TR>
            <TD>OrderId</TD>
            <td>
               <input type="text" name="oid" value=""/>
            </td>
         </TR>
         <tr>
```

```
            <td>Transaction Date</td>
            <td>
            <input type="text" name="tdate" value=""/>
            </td>
         </tr>
         <TR>
            <TD>* Charge Total:</TD>
            <TD><INPUT value=11.00 name=chargetotal> </TD></TR>

         <TR>
             <TD>* Sub Total:</TD>
             <TD><INPUT value=11.00 name=subtotal> </TD></TR>
         <TR>
         <TD></TD></TR>
         <TR>
            <TD></TD></TR>
         <TR>
            <TD align=middle colSpan=2><INPUT type=submit value="Submit
This Form" name=submitBtn></TD></TR></TBODY></TABLE>
            <input type="hidden" name="identifier" value="true" />
      </FORM>

    <%} else { %>

       <FORM method="post" id="redirectForm" name="redirectForm">
         <%
            String storename = getStoreName();
            String chargetotal = request.getParameter("chargetotal");

            String calculatedHash = createHash(chargetotal);
            String txnDateTime = getFormattedSysDate();
            String timeZone = getTimeZone();

         %>

         <input type="hidden" name="timezone" value='<%=timeZone%>'/>
         <input type="hidden" name="authenticateTransaction"
value="false" />
         <input size="50" type="hidden" name="paymentMethod"
value='<%=request.getParameter("paymentMethod")%>' />
         <input size="50" type="hidden" name="txntype"
value='<%=request.getParameter("txntype")%>' />
         <input size="50" type="hidden" name="txndatetime"
value="<%=txnDateTime%>" />
         <input size="50" type="hidden" name="hash"
value="<%=calculatedHash%>" />
         <input size="50" type="hidden" name="mode"
value='<%=request.getParameter("mode")%>' />
         <input size="50" type="hidden" name="storename"
value='<%=storename%>' />
         <input size="50" type="hidden" name="chargetotal"
value='<%=request.getParameter("chargetotal")%>' />
         <input size="50" type="hidden" name="subtotal"
value='<%=request.getParameter("subtotal")%>' />

         <input size="50" type="hidden" name="trxOrigin"
value='<%=request.getParameter("trxOrigin")%>' />
```

```
         <input size="50" type="hidden" name="oid"
value='<%=request.getParameter("oid")%>' />
         <input size="50" type="hidden" name="tdate"
value='<%=request.getParameter("tdate")%>' />

      </FORM>
    <%}%>
  </BODY>
 </HTML>
```

The fdgg-util_sha2.jsp file (see 08 fdgg-util_sha2.jsp reference below) includes code for generating a SHA2 hash, as required by First Data. The hash in the example ensures that this merchant is the only merchant that can send in transactions for this store.

Note: The POST URL used is for integration testing only. When you are ready to go into production, please contact First Data for the live production URL.

Sample code is presented for educational purposes only.

Your specific environment should be considered when integrating to Connect 2.0. Processing environments (Windows, Linux, AIX, etc…) and scripting environments (ASP, JSP or PHP) should be considered and reflected in the integration effort to Connect 2.0.

9.4 SHA2 (Secure Hash Algorithm)

In cryptography, SHA-2 is a set of cryptographic hash functions (converting a large, possibly variable-sized amount of data into a small reference value) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.

In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2.

9.5 Supporting Library Utilities

If you are utilizing PHP, ASP or JSP, you must utilize one of the utility libraries indicated below within the following sections to enable the cryptographic hash functions.

9.5.1 fdgg-util_sha2.asp

```
<script language="javascript" type="text/javascript" runat="server">


   var storename = "111111"; // Replace with your Storenumber here
   var sharedSecret = "222222"; //Replace with your Shared Secret here

   /* If you don't want to set the Default TimeZone, then you have to do
the following
   changes to set your server timeZone:
   Example: If your server is in "PST" timezone, here are the changes:
      //var formattedDate = defaultTime(); // Comment this line
      var formattedDate = getServerTime(); // Uncomment this line
      $timezone = "PST" // change to your server timeZone
   */
   var formattedDate = defaultTime();
   //var formattedDate = getServerTime();
   var timezone = "IST";

   /* END */



   /**
   *
   *  Secure Hash Algorithm (SHA256)
   *
   **/

   function SHA256(s){

      var chrsz   = 8;
      var hexcase = 0;
      function safe_add (x, y) {
         var lsw = (x & 0xFFFF) + (y & 0xFFFF);
         var msw = (x >> 16) + (y >> 16) + (lsw >> 16);
         return (msw << 16) | (lsw & 0xFFFF);
      }

      function S (X, n) { return ( X >>> n ) | (X << (32 - n)); }
      function R (X, n) { return ( X >>> n ); }
      function Ch(x, y, z) { return ((x & y) ^ ((~x) & z)); }
      function Maj(x, y, z) { return ((x & y) ^ (x & z) ^ (y & z)); }
      function Sigma0256(x) { return (S(x, 2) ^ S(x, 13) ^ S(x, 22)); }
      function Sigma1256(x) { return (S(x, 6) ^ S(x, 11) ^ S(x, 25)); }
      function Gamma0256(x) { return (S(x, 7) ^ S(x, 18) ^ R(x, 3)); }
      function Gamma1256(x) { return (S(x, 17) ^ S(x, 19) ^ R(x, 10)); }

      function core_sha256 (m, l) {
         var K = new Array(0x428A2F98, 0x71374491, 0xB5C0FBCF,
0xE9B5DBA5, 0x3956C25B, 0x59F111F1, 0x923F82A4, 0xAB1C5ED5, 0xD807AA98,
0x12835B01, 0x243185BE, 0x550C7DC3, 0x72BE5D74, 0x80DEB1FE, 0x9BDC06A7,
0xC19BF174, 0xE49B69C1, 0xEFBE4786, 0xFC19DC6, 0x240CA1CC, 0x2DE92C6F,
0x4A7484AA, 0x5CB0A9DC, 0x76F988DA, 0x983E5152, 0xA831C66D, 0xB00327C8,
0xBF597FC7, 0xC6E00BF3, 0xD5A79147, 0x6CA6351, 0x14292967, 0x27B70A85,
0x2E1B2138, 0x4D2C6DFC, 0x53380D13, 0x650A7354, 0x766A0ABB, 0x81C2C92E,
0x92722C85, 0xA2BFE8A1, 0xA81A664B, 0xC24B8B70, 0xC76C51A3, 0xD192E819,
0xD6990624, 0xF40E3585, 0x106AA070, 0x19A4C116, 0x1E376C08, 0x2748774C,
0x34B0BCB5, 0x391C0CB3, 0x4ED8AA4A, 0x5B9CCA4F, 0x682E6FF3, 0x748F82EE,
0x78A5636F, 0x84C87814, 0x8CC70208, 0x90BEFFFA, 0xA4506CEB, 0xBEF9A3F7,
0xC67178F2);
         var HASH = new Array(0x6A09E667, 0xBB67AE85, 0x3C6EF372,
0xA54FF53A, 0x510E527F, 0x9B05688C, 0x1F83D9AB, 0x5BE0CD19);
         var W = new Array(64);
         var a, b, c, d, e, f, g, h, i, j;
         var T1, T2;

         m[l >> 5] |= 0x80 << (24 - l % 32);
         m[((l + 64 >> 9) << 4) + 15] = l;

         for ( var i = 0; i<m.length; i+=16 ) {
            a = HASH[0];
            b = HASH[1];
            c = HASH[2];
            d = HASH[3];
            e = HASH[4];
            f = HASH[5];
            g = HASH[6];
            h = HASH[7];

            for ( var j = 0; j<64; j++) {
               if (j < 16) W[j] = m[j + i];
               else W[j] = safe_add(safe_add(safe_add(Gamma1256(W[j -
2]), W[j - 7]), Gamma0256(W[j - 15])), W[j - 16]);

               T1 = safe_add(safe_add(safe_add(safe_add(h, Sigma1256(e)),
Ch(e, f, g)), K[j]), W[j]);
               T2 = safe_add(Sigma0256(a), Maj(a, b, c));

               h = g;
               g = f;
               f = e;
               e = safe_add(d, T1);
               d = c;
               c = b;
               b = a;
               a = safe_add(T1, T2);
            }

            HASH[0] = safe_add(a, HASH[0]);
            HASH[1] = safe_add(b, HASH[1]);
            HASH[2] = safe_add(c, HASH[2]);
            HASH[3] = safe_add(d, HASH[3]);
            HASH[4] = safe_add(e, HASH[4]);
            HASH[5] = safe_add(f, HASH[5]);
            HASH[6] = safe_add(g, HASH[6]);
            HASH[7] = safe_add(h, HASH[7]);
         }
         return HASH;
      }

      function str2binb (str) {
         var bin = Array();
         var mask = (1 << chrsz) - 1;
         for(var i = 0; i < str.length * chrsz; i += chrsz) {
            bin[i>>5] |= (str.charCodeAt(i / chrsz) & mask) << (24 -
i%32);
         }
         return bin;
      }

      function Utf8Encode(string) {
         string = string.replace(/\r\n/g,"\n");
         var utftext = "";

         for (var n = 0; n < string.length; n++) {

            var c = string.charCodeAt(n);

            if (c < 128) {
               utftext += String.fromCharCode(c);
            }
            else if((c > 127) && (c < 2048)) {
               utftext += String.fromCharCode((c >> 6) | 192);
               utftext += String.fromCharCode((c & 63) | 128);
            }
            else {
               utftext += String.fromCharCode((c >> 12) | 224);
               utftext += String.fromCharCode(((c >> 6) & 63) | 128);
               utftext += String.fromCharCode((c & 63) | 128);
            }

         }

         return utftext;
      }
      function binb2hex (binarray) {
         var hex_tab = hexcase ? "0123456789ABCDEF" : "0123456789abcdef";
         var str = "";
         for(var i = 0; i < binarray.length * 4; i++) {
            str += hex_tab.charAt((binarray[i>>2] >> ((3 - i%4)*8+4)) &
0xF) +
            hex_tab.charAt((binarray[i>>2] >> ((3 - i%4)*8  )) & 0xF);
         }
         return str;
      }

      s = Utf8Encode(s);
      return binb2hex(core_sha256(str2binb(s), s.length * chrsz));

   }


   function defaultTime() {

      d = new Date();
      utc = d.getTime() + (d.getTimezoneOffset() * 60000);
      nd = new Date(utc + (3600000*5.5));
      strdate = nd.getYear()+":"+
pad(nd.getMonth()+1,2)+":"+pad(nd.getDate(),2)+"-
"+pad(nd.getHours(),2)+":"+pad(nd.getMinutes(),2)+":"+pad(nd.getSeconds()
,2);
      return strdate;

   }

   function getServerTime() {

      nd = new Date();
      strdate = nd.getYear()+":"+
pad(nd.getMonth()+1,2)+":"+pad(nd.getDate(),2)+"-
"+pad(nd.getHours(),2)+":"+pad(nd.getMinutes(),2)+":"+pad(nd.getSeconds()
,2);
      return strdate;

   }

   function pad(number, length) {
      var str = '' + number;
      while (str.length < length) {

             str = '0' + str;

          }

       return str;
    }

   function getTimeZone() {
      return timezone;
   }

   function getStoreName() {
      return storename;
   }

   function getSharedSecret() {
      return sharedSecret;
   }

   function getFormattedDate() {
      return formattedDate;
   }

</script>
```

9.5.2 fdgg-util_sha2.php

```
<?php

   $storename = "111111"; // Replace with your Storenumber here
   $sharedSecret = "222222"; //Replace with your Shared Secret here

   /* If you have below PHP version 5.1 OR Don't want to set the Default
TimeZone, then you have to do the following
   changes to set your server timeZone:
   Example: If your server is in "PST" timezone, here are the changes:
      //date_default_timezone_set("Asia/Calcutta"); // Comment this line
      $timezone = "PST" // change to your server timeZone
   */
   date_default_timezone_set("Asia/Calcutta");
   $timezone = "IST";

   /* ---- */

   $dateTime = date("Y:m:d-H:i:s");

   function getDateTime() {
      global $dateTime;
      return $dateTime;
   }

   function getTimezone() {
      global $timezone;
      return $timezone;
   }

   function getStorename() {
      global $storename;
      return $storename;
   }

   function createHash($chargetotal) {
      global $storename, $sharedSecret;

      $str = $storename . getDateTime() . $chargetotal . $sharedSecret;

      for ($i = 0; $i < strlen($str); $i++){
         $hex_str.=dechex(ord($str[$i]));
      }

      return hash('sha256', $hex_str);
   }
?>
```

9.5.3 fdgg-util_sha2.jsp

```
<!-- fdgg-util_p.jsp -->
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
   pageEncoding="ISO-8859-1"
   import="java.util.Date, java.util.TimeZone,
java.security.MessageDigest, java.text.SimpleDateFormat"
%>
<%!

   String storeName="111111"; // Replace with your Storenumber here
   String sharedSecret = "222222"; //Replace with your Shared Secret here
   /* --- */

   private static SimpleDateFormat dateFormat = new
SimpleDateFormat("yyyy:MM:dd-HH:mm:ss");
   String fmtDate;
   String timeZone;

   public String createHash(String charge) {

      /* If you Don't want to set the Default TimeZone, then you have to
do the following
      changes to set your server timeZone:
      Example: If your server is in PST timezone, here are the changes:
         //TimeZone.setDefault(TimeZone.getTimeZone("Asia/Calcutta")); //
Comment this line
         timeZone = "PST"; // change to your server timeZone
      */
      TimeZone.setDefault(TimeZone.getTimeZone("Asia/Calcutta"));
      timeZone = "IST";
      /* --- */

      Date now = new java.util.Date(System.currentTimeMillis());
      fmtDate = dateFormat.format(now);
      String stringToHash = storeName + fmtDate + charge + sharedSecret;
      return calculateHashFromHex(new StringBuffer(stringToHash));
   }

   private String calculateHashFromHex(StringBuffer buffer) {

        String algorithm = "SHA-256";
        MessageDigest messageDigest = null;

        try {
         messageDigest = MessageDigest.getInstance(algorithm);
        } catch (Exception e) {
         throw new IllegalArgumentException("Algorithm '" + algorithm +
"' not supported");
        }

        StringBuffer result = new StringBuffer();
        StringBuffer sb = new StringBuffer();
        byte[] bytes = buffer.toString().getBytes();
        int byteLen = bytes.length;

        for (int i = 0; i < byteLen; i++) {

         byte b = bytes[i];
         sb.append(Character.forDigit((b & 240) >> 4, 16));
         sb.append(Character.forDigit((b & 15), 16));

        }

        buffer = new StringBuffer(sb.toString());
        messageDigest.update(buffer.toString().getBytes());
        byte[] message = messageDigest.digest();
        int messageLen = message.length;

        for (int j = 0; j < messageLen; j++) {

         byte b = message[j];
         String apps = Integer.toHexString(b & 0xff);
         if (apps.length() == 1) {
           apps = "0" + apps;
         }
         result.append(apps);
        }

        return result.toString();
   }

   public String getTimeZone() {
       return timeZone;
   }

   public String getStoreName() {
       return storeName;
   }

   public String getFormattedSysDate() {
       return fmtDate;
   }

%>
```

9.5.4 Programmatic Upgrade Considerations

The code fragment presented in the table below presents a side-by-side comparison between a legacy Connect 1.0 HTML version and a Connect 2.0 ASP implementation. Note that FDC supplied functions are invoked within the ASP version that are not present within the legacy Connect 1.0 implementation. These functions enable the creation of the SHA256 hash and retrieval of the shared secret.

Connect 1.0 (HTML)	Connect 2.0 (ASP)

Gather Form Data:
 	
<input type="hidden" name="storename" value="1234567890">
 	
<TD>* Payment Mode:</TD>
<TD><SELECT name=mode>
        <OPTION value=payonly selected>PayOnly</OPTION>
        <OPTION value=payplus>PayPlus</OPTION>
        OPTION value=fullpay>FullPay</OPTION>
        <OPTION value="">
</OPTION></SELECT>
 	
<TD>* Charge Total:</TD>
        <TD><INPUT value=11.00 name=chargetotal>
</TD></TR>
<TR>
 	
<TD>* Sub Total:</TD>
         <TD><INPUT value=11.00 name=subtotal>
</TD></TR>
</TD></TR>
	Gather Form Data:
	
	mode = Request.Form("mode")
	chargetotal = Request.Form("chargetotal")
	subtotal = Request.Form("subtotal")
	…
	Call FDC Supplied Functions:
	
	formattedDate = getFormattedDate()
	storename = getStoreName()
	sharedsecret = getSharedSecret()
	timezone = getTimeZone()
	
	*** Concatenate Hash ***
	str = storename + formattedDate + chargetotal + sharedsecret
	hex_str = ""
	        for i = 1 to len(str)
	                hex_str = hex_str + lcase(cstr(hex(asc(mid(str, i, 1)))))
	        next
	
	*** Create Hash ***
	createdHash = SHA256(hex_str)
	
	<input type="hidden" name="timezone" value="<% Response.Write(timezone)%>" />
	…

Send Message:
 	
<FORM action="https://www.linkpointcentral.com/lpc/servlet/lppay" method="post">
	Send Message:
	
	/* For Production Environment (PROD) */
	
	document.redirectForm.action="https://connect.firstdataglobalgateway.com/IPGConnect/gateway/processing";
	document.redirectForm.submit();

10 Glossary

Account Number

The account number for a checking or savings account is a unique number that identifies the customer's account. The account number appears on the check next to the transit routing number. The numbers are separated by a non-alphabetic or non-numeric symbol.

ACH

ACH is an abbreviation for Automated Clearing House. Automated Clearing House (ACH) is the name of an electronic network for financial transactions in the United States. ACH processes large volumes of both credit and debit transactions which are originated in batches. ACH allows merchants to accept payments from a customer's checking or savings account.

Acquiring Bank

An acquiring bank is a bank, which provides a service to its business customers allowing them to accept card payments for goods and services.

Address Verification Service

The Address Verification System (AVS) is a system used to verify the identity of the person claiming to own the credit card. The system will check the stated billing address of the credit card, with the address on file at the credit card company. The gateway provides an AVS code in each approved transaction result that tells you how well the two addresses match. If they match, there is a lower probability of fraud. If there is a discrepancy in either the address or zip code, the probability of fraud is higher. Merchants can use AVS codes to help protect themselves from Chargebacks and fraud.

Antivirus Software

Antivirus software consists of computer programs that attempt to identify, deter, and eliminate computer viruses and other malicious software. Antivirus software typically uses two different techniques to accomplish this: Examining (scanning) files to look for known viruses matching definitions in a virus dictionary, and identifying suspicious behavior from any computer program, which might indicate infection. Such analysis may include data captures, port monitoring, and other methods. Due to the risk of computer viruses harming your computer files, antivirus software is recommended for all Internet users.

Application Programming Interface (API)

First Data Global Gateway API is a tool that allows a merchant to create a customer commerce solution. Our Application Programming Interface (API) allows you to add payment functionality to custom built web sites or online applications.

Authorization

An authorization reserves funds on a customer's credit card. An authorization does not charge the card until you perform a Ticket Only transaction or confirm shipment of the order. The period during which funds are reserved may be as little as three days or as long as several months.

Authorize Only

An Authorize Only transaction reserves funds on a customer's credit card. An Authorize Only transaction does not charge the card until you perform a Ticket Only transaction and confirm shipment of the order using an option available in the Reports section. Authorize-only transactions reserve funds for varying periods, depending on the issuing credit card company's policy. The period may be as little as three days or as long as several months. For your protection, you should confirm shipment as soon as possible after authorization.

Batch

Credit Card or Check transactions that is combined and submitted as a group to the payment gateway for settlement. On the payment gateway, batches are submitted automatically once a day.

Blocking and Limiting

If you suspect certain transactions might be fraudulent, you can block further purchases by blocking credit card numbers, persons' names, domain names, and IP addresses or Class C addresses from purchasing at your store. You can limit the amount that any customer can spend at your store by setting a maximum purchase amount. You can set how long automatic lockouts and duplicate lockouts will continue to be blocked.

Browser

Short for web browser, a browser is a software application that enables a user to display and interact with text, images, videos, music, and other information typically located on a web page at a web site on the Internet.

Cable Modem

A cable modem is a type of modem that provides access to the Internet through the cable television infrastructure. Cable modems are primarily used to deliver broadband Internet access, taking advantage of unused bandwidth on a cable television network. If the cable network is shared with many other Internet subscribers, Internet access speed may go down.

Card Code

The card code is the card security code, sometimes called Card Verification Value or Code (CVV or CVC). It is a security feature for credit or debit card transactions, giving increased protection against credit card fraud. This code (also known as a CCID or Credit Card ID) is often asked for by merchants to secure transactions when the card is not present, usually occurring over the Internet, by mail, fax, or over the phone. The payment gateway will compare the card code with the code on file at the card-issuing bank. Results of this comparison will show in the transaction approval code. By using the card code results along with the Address Verification Service (AVS), you can make a more informed decision about whether to accept transactions. MasterCard, Visa, and Discover credit and debit cards have a three-digit code, called the "CVC2" (card validation code), "CVV2" (card verification value), and "CID" (card identification number), respectively. It is always the final group of numbers printed on the back signature panel of the card. New North American MasterCard and Visa cards feature the card code in a separate panel to the right of the signature strip. American Express cards have a four-digit code printed on the front side of the card above the number, referred to as the CID.

Card-Issuing Bank

The financial institution or bank that issues a credit, debit, or purchasing card to a business or consumer. The card-issuing bank has an address on file for the card, which the Address Verification System (AVS) compares to the address given to the merchant.

Chargeback

A chargeback is a forced refund to the customer through your bank account. Chargebacks can occur with any type of business whether it is online or at an actual store location. Each fraudulent credit card transaction typically results in a chargeback. Credit card associations penalize merchant banks for Chargebacks. Naturally, the bank passes the fines on to the responsible merchant, and these penalties can be severe. While consumers are provided with a certain degree of protection if their credit card numbers are stolen and misused, Internet merchants are fully liable for all transactions because Internet transactions are classified as "card-not-present."

Check Number

The check number is a number unique to each check. The check number is always found in the top right corner of the check. The check number is only provided as a reference to process the ACH transaction.

Commerce Service Provider (CSP)

The commerce service provider (CSP) supplies businesses with the tools and services they need to buy and sell products and services over the Internet, and to manage their online enterprises. CSPs can generally host a secure web site that could be connected to a secure payment gateway for selling products or services over the Internet.

Credit

A Credit transaction returns funds to a customer’s credit card on orders without an order number. This transaction is intended for returns against orders processed outside the system. Credit transactions are marked as Returns in your reports.

Credit Card

A credit card is a card (usually plastic) that assures a seller that the person using it has a satisfactory credit rating, and that the issuer will see to it that, the seller receives payment for the merchandise delivered.

CVC2

The CVC2 is the card validation code or card code for MasterCard. See the definition for card codes for more information.

CVV2

The CVC2 is the card verification value or card code for Visa cards. See the definition for card codes for more information.

Data Field

A data field is an area on a web form or software application where you can enter information relevant to the name of the field. For example, you would enter the zip code in the data field named zip code.

DDA Number

The DDA (demand deposit account) number is the deposit account held at a bank or other financial institution for the purpose of securely and quickly providing frequent access to funds on demand.

Dial-Up Connection

A dial-up connection is a way to access the Internet through a telephone line. A modem is connected to a computer and a telephone line to dial into an Internet service provider's (ISP) node to establish a modem-to-modem link, which is then routed to the Internet. The speed of dial up connections is usually slower than other Internet access options.

Digital Certificate

A digital certificate is an electronic certificate that establishes the merchant's credentials for performing business on the Internet. It is an encrypted set of information issued by an Internet certification authority such as Thawte. Digital certificates are required for merchants who choose to use the API. For other products, the merchant does not need a digital certificate.

Domain Name

A name that identifies a computer or computers on the internet. These names appear as a component of a web site's URL, such as microsoft.com. This type of domain name is also called a hostname.

DSL

DSL (Digital Subscriber Line) is a technology for bringing fast Internet service to homes and small businesses over the wires of a local telephone network.

E-commerce (ECI)

E-commerce (ECI) or electronic commerce consists of the buying and selling of products or services over electronic systems, such as the Internet and other computer networks.

Electronic Check Acceptance (ECA)

With electronic check acceptance (ECA), the check is electronically submitted as a check. The check is no longer usable and the paper check must be voided. The customer signs and receives a paper receipt. ECA services may include a check guarantee service. ECA is used for retail payments only.

Field

A field is an area on a web form or software application where you can enter information relevant to the name of the field. For example, you would enter the zip code in the field named zip code.

Firewall

A firewall is a hardware or software device, which is configured to permit, deny, or proxy data through a computer network which has different levels of trust. A firewall protects the resources of a private network from users of other networks.

First Data Global Gateway Connect 2.0

The First Data Global Gateway Connect 2.0 service is an e-Commerce solution using a hosted payment page. This eliminates some of the complexity and is great for a merchant with limited resources or expertise.

Forced Ticket

A Forced Ticket transaction is a credit card transaction for authorizations you obtained over the phone. It requires a reference number (or approval code) that you should have received when you made the phone authorization.

Hierarchy

A term used to describe the organizational tree structure for multi-store reports. Merchants describe their organization by defining an org chart in the form of a tree structure. The structure is used for combining store reports into groups at different levels. The term hierarchy refers to the entire organizational tree structure containing levels and elements.

HTML

HTML is short for Hypertext Markup Language. HTML is a markup language used to structure text and multimedia documents and to set up hypertext links between documents used extensively on the Internet. Other than manually entering transactions using the Virtual POS Terminal, HTML is the simplest way to send payment transactions to the payment gateway.

HTTP

HTTP (Hypertext Transfer Protocol) is a communications protocol used to transfer or convey information on the Internet. For example, when you enter a URL in your browser, it sends an HTTP command to the web server directing it to receive and transmit the requested web page.

Hyperlink

A hyperlink is a reference or navigation element in a document or web page linking to another section of the same document or web page or to another document or web page that may be on a different web site.

Internet Check Acceptance (ICA)

Internet Check Acceptance (ICA) is the type of check service provided on the payment gateway. ICA uses the Automated Clearing House (ACH) to transfer funds from the customer’s account. The account information is entered in an online payment form, and no check is used. The customer may or may not sign a payment form. In either case, the merchant needs a documented record of the customer's authorization to transfer funds from the account. ICA includes an electronic receipt. There is no check guarantee service with

ICA. ICA is typically used for mail orders/telephone orders (MO/TO) or e-commerce transactions, but may also be used for retail.

Internet Service Provider (ISP)

An Internet service provider (ISP) is a business or organization that provides consumers or businesses access to the Internet and related services. An ISP can also host a web site.

IP Address

IP address is short for Internet Protocol address. An IP address is a number that is used to identify a specific computer on a network or on the Internet. The format of an IP address is written as four numbers separated by periods. Each number can be from zero to 255. For example, 1.160.10.240 could be an IP address.

Issuing Bank

The financial institution or bank that issues a credit, debit, or purchasing card to a business or consumer. The issuing bank has an address on file for the card, which the Address Verification System (AVS) compares to the address given to the merchant.

Level

A level is a single tier in the hierarchy or organizational tree structure for multi-store users. The top level (1) is typically the root (or corporate) level containing one element. The lowest level of the tree is always the User level; the next level up from the lowest is the Store level. Merchants define the number of levels and names of each level for their own organization up to 10 chargetotal levels.

Local Area Network (LAN)

A local area network (LAN) is a computer network covering a small geographic area, like a home, office, or group of buildings. The defining characteristics of LANs, in contrast to Wide Area Networks (WANs), include their much higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines.

Log In

To log in is the process by which individual access to a computer system is controlled by identification of the user in order to obtain credentials to permit access. It is an integral part of computer security. A user can log in to a system to obtain access, and then log out when the access is no longer needed.

Log Out

To log out is to close off one's access to a computer system after previously having logged in. To log out of the First Data Global Gateway Virtual Terminal, click the Logout link in the top right corner of the application. To prevent unauthorized users from accessing their account, merchants should always log off and close the browser window when they are finished using the system.

Multi-Store

Multi-stores are multiple accounts with different store numbers.

Network

A network is a group of two or more computer systems linked together.

Password

A password is a form of secret authentication data that is used to control access to a resource. It is recommend that users change their password frequently and do not share it with anyone to prevent unauthorized access to their accounts.

Payment Gateway

A payment gateway is an e-commerce application service that authorizes payments for e-businesses and online retailers. It is the equivalent of a physical POS (Point-of-sale) terminal located in most retail outlets. Payment gateways encrypt sensitive information, such as credit card numbers, to ensure that information passes securely between the customer and the merchant.

PDF File

PDF is short for Portable Document Format. It is the file format created by Adobe Systems in 1993 for document exchange. PDF is used for representing two-dimensional documents in a device-independent and display resolution-independent fixed-layout document format. Internet users need an Adobe Acrobat viewer to open a PDF file, which can be downloaded free of charge at http://www.adobe.com.

Periodic Billing

Periodic billing is recurring payments or the capability to charge customers on a recurring basis according to merchant-defined rules. Gateway products allow a merchant to charge a customer's card in exchange for products and services one or more times every day, week, month, or year.

Plug-In

A plug-in is a hardware or software module that adds a specific feature or service to a larger system. For example, there are a number of plug-ins for the Mozilla Firefox browser that enables it to display different types of audio or video files.

Point of Sale (POS)

The consumer is purchasing a product from the merchant and the merchant is processing the payment transaction. POS is commonly used to refer to the payment terminals or software merchants use to process the payment transaction.

Protocol

A Protocol is a set of guidelines or rules that help in governing an operation on the Internet and communications over it. There are several different protocols. HTTP is the protocol used for the Internet.

Purchasing Card

A purchasing card is a corporate card used by some companies for their business purchases. When a customer pays for goods or services using a purchasing card, the following information must be included with the order information. This information is optional for a regular credit card transaction: An indication of whether the order is tax exempt. The amount of tax applied to the order. If the order is tax exempt, the tax amount should be zero. A purchase order number associated with the order. One purchase order can apply to several individual orders to allow for delivery of goods over time. If there is not a purchase order associated with the order, the customer must supply some value for the order.

Recurring Payment

The capability to charge customers on a recurring basis according to merchant-defined rules. Gateway products allow a merchant to charge a customer's card in exchange for products and services one or more times every day, week, month, or year.

Return

A Return transaction returns funds to a customer’s credit card for an existing order on the system. To perform a return, you need the order number (which you can find in your reports). After you perform a Return for the full order amount, the order will appear in your reports with a transaction amount of 0.00.

Sale

A sale transaction immediately charges a customer's credit card when the batch of transactions is closed.

Secure Shell (SSH)

Secure Shell (SSH) is a network protocol that allows data to be exchanged over a secure channel between two computers.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications on the Internet, such as transmitting credit card data and other data transfers.

Settlement

Settlement is the completion of a payment transaction. When a transaction is settled, it has been funded and the funds deposited in the merchant account.

Store Name

The store name (also called DBA or store number) is a six to ten-digit number needed to identify the merchant. The store name is given to the merchant in the Welcome E-mail. Merchants need the store name, user ID, and password to access the Virtual POS Terminal, as well as reports, admin, and customization functions. The store name is also needed for using the API and other products.

Ticket Only

A Ticket Only transaction is a post-authorization transaction that captures funds from an Authorize Only transaction. Funds are transferred when your batch of transactions is settled. If you enter a larger chargetotal for the Ticket Only transaction than was specified for the Authorize Only transaction, the Ticket Only transaction may be blocked. If you enter a smaller amount than was authorized, an adjustment is made to the Authorization to reserve only the smaller amount of funds on the customer’s card for the transaction.

Transit Routing Number

A transit routing number is a nine-digit bank code, used in the United States, which appears on the bottom of checks. This code is used by the Automated Clearing House to process direct deposits and other automated transfers.

URL

URL is short for Uniform Resource Locator. The URL is the address for documents and other pages on the Internet. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

User ID

For accounts with multiple users, each individual user will be assigned a User ID. The user will need this User ID, along with the store name and password, to log in to the system.

Virtual

Virtual is often used on the Internet to denote a web-based program that functions similarly to a physical device or system. For example, a virtual point-of-sale terminal is a computer program that performs the same functions as a physical point-of-sale terminal.

Void

To void a transaction is to cancel a payment transaction. Merchants can void transactions prior to settlement. Once the transaction has settled, the merchant has to perform a return or credit to reverse the charges and credit the customer's card.

WAN

A WAN is a wide-area computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

Web Server

A web server is a computer program responsible for accepting HTTP requests from clients and serving HTTP responses along with optional data contents. The responses are usually web pages, such as HTML documents and linked objects (images, etc.).

XML
XML is the Extensible Markup Language, which is a universal format for the representation of documents and data. It is classified as an extensible language because it allows its users to define their own tags. Its primary purpose is to facilitate the sharing of structured data across different information systems, particularly through the Internet.

11 Revision Log

Ver	Date	Author	Content
1.1	May 13, 2011	First Data	Initial Connect 2.0 Content.
	June 23, 2011	First Data	Correct Mode to correct case (fullpay, payplus and payonly).
1.2	August 29, 2011	First Data	Modified LPC Shared Secret Interface Defination.
1.2.1	November 2, 2011	First Data	Clarified outbound SHA-2 Hash definition.