Authorize.Net®
a CyberSource solution

Merchant Integration Guide

Card Not Present Transactions

Authorize.Net Trademarks:

Advanced Fraud Detection Suite™

Authorize.Net®

Authorize.Net Your Gateway to IP Transactions™

Authorize.Net Verified Merchant Seal™
Authorize.Net Where the World Transacts®

Automated Recurring Billing™

eCheck.Net®

FraudScreen.Net®

Table of Contents

Revision History

PUBLISH DATE	UPDATES
August 2007	Release of Merchant Integration Guide
May 2008	Removal of SecureSource requirements
July 2008	KB and CS update
October 2009	Clarify requirements for Prior_auth_Capture, Void, and Credit transaction types
May 2010	Clean up formatting
August 2010	Update MD5 Hash information Update instructions for customizing look and feel of payment form and receipt page
November 2010	Add Transaction Details API setting
May 2011	Corrected AVS and CCV settings instructions

Section 1

Introduction

Welcome to the Merchant Integration Guide. This document is designed to be a companion guide to the Web developer guides for connecting a website or business application to the Authorize.Net® Payment Gateway for processing online payments. Its purpose is to provide details about the settings available in the Merchant Interface for configuring your connection to the payment gateway.

The Merchant Interface at https://account.authorize.net is a secure website where you can manage your payment gateway account, submit manual transactions, monitor and review unsettled transactions, search for and view settled transactions, view account billing statements, configure account settings, and more. This particular guide focuses on the settings available in the Merchant Interface for your website connection to the payment gateway. For help with other Merchant Interface features and settings, see the Merchant Interface Online Help Files. These can be accessed from any page in the Merchant Interface by clicking the **Help** link in the top right corner of the page.

IMPORTANT: Connection settings that can be configured in the Merchant Interface can also be hard coded in your website code. To maintain a robust connection to the payment gateway, it is highly recommended that you work closely with your Web developer to identify those settings that should be hard coded in your website code versus those settings that you might need to configure yourself from time to time in the Merchant Interface.

You might consider creating a unique user account in the Merchant Interface for your Web developer, to give them direct access and permissions to configure connection settings for your account. This way, you do not need to worry about settings yourself—you can simply communicate requirements to your Web developer. For more information on creating user accounts, log on to the Merchant Interface at https://account.authorize.net, click **User Administration** under Account in the main menu on the left, and click the **Help** link in the top right corner of the page.

Note: Only Account Owners or Account Administrators have the permissions necessary to create new account users. If the Multiple User Accounts feature is not enabled for your Merchant Interface account, the principle owner or the person in your organization who set up your payment gateway account will need to activate it in order for you to create user accounts. For more information see the *Multiple User Accounts Merchant Preparation Guide* at http://www.authorize.net/files/MUprepguide.pdf.

Processing Requirements

This document assumes that the following requirements for processing payments through the Authorize.Net Payment Gateway are already in place:

- You already have a U.S. based merchant bank account that allows Internet transactions.

- You already have an e-commerce (Card Not Present) Authorize.Net Payment Gateway account.

- You are working with a Web developer or shopping cart to connect your e-commerce website or other business application to the Authorize.Net Payment Gateway.

Connection Methods

The Authorize.Net Payment Gateway provides many different methods for connecting an e-commerce website or other business application to the payment gateway by means of the Internet. If you or your Web developer have not already selected an integration method, discuss your business requirements with your Web developer for help determining which connection method is best for you. You can also review our *Connection Methods Guide* at http://www.authorize.net/files/connectionmethodsguide.pdf, or the Quick Start page at https://developer.authorize.net/integration/fifteenminutes.

You can choose from the following connection methods:

Server Integration Method (SIM)

Advanced Integration Method (AIM)

Simple Checkout

Server Integration Method (SIM)

SIM is a hosted payment processing solution, which means that Authorize.Net provides the necessary Web resources to handle all the steps in processing a transaction, including:

- Collecting customer payment information through a secure, hosted form

- Generating a receipt to the customer

- Secure transmission to the payment processing networks for settlement

- Funding of proceeds to your bank account

- Secure storage of cardholder information

SIM is an ideal integration solution for merchants who do not want to collect, transmit or store sensitive cardholder information to process transactions. Additionally, SIM does not require a Secure Sockets Layer (SSL) digital certificate. This removes the complexity of securely handling and storing cardholder information, simplifying compliance with the Payment Card Industry (PCI) Data Security Standard. For more information about the PCI Data Security Standard, see our *Security Best Practices White Paper* at http://www.authorize.net/files/securitybestpractices.pdf.

You can find the *SIM Developer Guide* in the Authorize.Net Developer Center at http://developer.authorize.net/guides/SIM/.

Advanced Integration Method (AIM)

AIM is a custom payment processing solution that gives you control over all the steps in processing a transaction, including:

- Collecting customer payment information through a custom application

- Generating a receipt to the customer

- Secure transmission to the payment gateway for transaction processing

- Secure storage of cardholder information

- And more, depending on your business requirements

AIM is an ideal integration solution for merchants who need the highest degree of customization and control over their customers' checkout experience. Because AIM involves the collection, transmission, and storage of cardholder data, compliance with the PCI Data Security Standard is required by the Card Associations. For more information, please see our *Security Best Practices White Paper* at http://www.authorize.net/files/securitybestpractices.pdf.

You can find the *AIM Developer Guide* in the Authorize.Net Developer Center at http://developer.authorize.net/guides/AIM/.

Simple Checkout

Simple Checkout gives you the ability to link to our secure payment page without having to write code to link your website to our system. You can create a profile for each product you sell, designate different pricing points for shipping costs, and then copy the code from the Merchant Interface and paste it into your site's HTML. This code adds a button that says "Buy Now" or "Donate" on your website, which will take the customer to Authorize.Net's secure checkout page, with all product information pre-filled.

To start using the Simple Checkout tool:

1. Log on to your Merchant Interface

2. Click **Tools**

3. On the left, select **Simple Checkout**

4. Sign up for **Multi User Account Management** (if not already enabled on the account)

5. Agree to **Terms of Service**

6. Generate an API Login ID and Transaction Key when prompted.

Customer and Developer Support

There are several resources available to help you and your Web developer successfully integrate a merchant website or other business application to the Authorize.Net Payment Gateway.

- Refer to the Merchant Interface Online Help Files. Log on to the Merchant Interface at https://account.authorize.net, click on the feature for which you need help from the main menu or **Settings** menu, and then click the **Help** link in the top right corner of the page.

- The Authorize.Net Knowledge Base, located at http://www.authorize.net/help, provides comprehensive answers to virtually any customer support question, as well as useful links to demos, help files and information on contacting us. We strongly recommend using the Knowledge Base anytime you need help.

- Customer Support is available to help you with questions regarding integration settings in the Merchant Interface. You can contact Customer Support by emailing support@authorize.net, or using chat by clicking **Live Help** in the top right corner of the Merchant Interface. Customer Support hours are 5:00 AM – 5:00 PM Pacific time, Monday through Friday.

- The Developer Center at http://developer.authorize.net provides Web developers with test accounts, sample code, FAQs, and troubleshooting tools.

- If you or your developer can't find what you need in the Developer Center, our Integration Team is available to answer your questions by email at integration@authorize.net. (Please note that our Integration Team can only assist with support requests specific to the Authorize.Net application programming interface (API) and/or services.)

If you have any suggestions about how we can improve or correct this guide, please email documentation@authorize.net.

Section 2
Submitting Transactions

There are two ways to submit transactions to Authorize.Net:

- Automatically through a website or custom application connected to Authorize.Net using Advanced Integration Method (AIM) or Server Integration Method (SIM).

- Manually process orders by using the Virtual Terminal.

It's a good idea to identify how your business plans to submit transactions so that you and/or your Web developer can properly integrate your payment gateway account to support your business processes.

For example, are you submitting transactions mainly through an e-commerce website? Are you integrating a custom application to allow call center representatives to enter mail order/telephone order (MOTO) transactions? Would you like the ability to verify the availability of funds on a customer's credit card account at the time of purchase and then charge their credit card at the time you ship the order?

By communicating your transaction processing practices or requirements, you can help your Web developer integrate your website or custom application more quickly.

Credit Card Transaction Types

The payment gateway supports the following credit card transaction types.

Authorization and Capture

This is the most common type of credit card transaction. The amount is sent for authorization, and if approved, is automatically submitted for settlement.

Authorization Only

This transaction type is sent for authorization only. The transaction will not be sent for settlement until the credit card transaction type Prior Authorization and Capture (see definition below) is submitted, or the transaction is submitted for capture manually in the Merchant Interface.

If action for the Authorization Only transaction is not taken on the payment gateway within 30 days, the authorization expires and is no longer available for capture. A new Authorization Only transaction would then have to be submitted to obtain a new authorization code.

You can submit Authorization Only transactions if you want to verify the availability of funds on the customer's credit card before finalizing the transaction. This transaction type can also be submitted in the event that you do not currently have an item in stock or you want to review orders before shipping goods.

Note: If you are using SIM, the hosted payment form can be configured to submit either Authorization and Capture or Authorization Only transactions. Please communicate to your Web developer your preferences regarding which of these credit card transaction types should be used for your website.

Prior Authorization and Capture

This transaction type is used to complete an Authorization Only transaction that was successfully authorized through the payment gateway.

Note: An Authorization Only and a Prior Authorization and Capture together are considered one complete transaction. Once the Prior Authorization and Capture is submitted, the transaction will be sent for settlement.

The payment gateway accepts this transaction type and initiates settlement if the following conditions are met:

- The original Authorization Only transaction was submitted within the previous 30 days (Authorization Only transactions expire on the payment gateway after 30 days).

- The transaction is submitted with the valid transaction ID of an original, successfully authorized, Authorization Only transaction.

- The original transaction is not already settled, expired or errored.

- The amount being requested for capture is less than or equal to the original authorized amount.

For this transaction type, the amount is only required in the event that a Prior Authorization and Capture is submitted for an amount that is *less* than the amount of the original Authorization Only transaction. If no amount is submitted, the payment gateway will initiate settlement for the amount of the original authorized transaction.

If this transaction type is required, we recommend you process the transactions by logging on to the Merchant Interface directly, or by using a desktop application that uses AIM. You can search for the transaction by Transaction ID, then open the Transaction Details page for that transaction.

Capture Only

This transaction type is used to complete a previously authorized transaction that was *not* originally submitted through the payment gateway or that required voice authorization.

The payment gateway accepts Capture Only transactions if the following conditions are met:

- The transaction is submitted with the valid authorization code issued to the merchant to complete the transaction.

- The transaction is submitted with the customer's full credit card number and expiration date.

Note: If you are using SIM, we strongly recommend that you only submit Capture Only transactions through the Virtual Terminal. This transaction type requires the submission of full sensitive customer information, which requires a greater level of compliance with the Payment Card Industry (PCI) Data Security Standard. If your business needs the ability to submit this transaction type from a custom application, please consider using AIM. For more information about AIM, please see the *AIM Developer Guide* at http://developer.authorize.net/guides/AIM/.

Note: This transaction type might be subject to a higher discount rate. Please contact your Merchant Service Provider for more information about submitting Capture Only transactions.

Credit

This transaction type is used to refund a customer for a transaction that was originally processed and successfully settled through the payment gateway.

The payment gateway accepts Credits if the following conditions are met:

- The transaction is submitted with the valid transaction ID of an original, successfully settled transaction.

- The amount being requested for refund is less than or equal to the original settled amount.

- The total amount of multiple Credit transactions submitted against the original transaction is less than or equal to the original settled amount.

- At least the last four digits of the credit card number used for the original, successfully settled transaction are submitted. An expiration date is not required.

- The transaction is submitted within 120 days of the settlement date of the original transaction.

If this transaction type is required, we recommend you process the transactions by logging on to the Merchant Interface directly, or by using a desktop application that uses AIM. You can search for the transaction by Transaction ID, then open the Transaction Details page for that transaction.

Unlinked Credit

This transaction type is used to issue a refund for a transaction that was *not* originally submitted through the payment gateway. It also allows you to override restrictions for submitting refunds for payment gateway transactions, for example, if you are beyond the 120-day period for submitting a refund or you would like to refund an amount that is greater than the original transaction amount.

The ability to submit unlinked credits is not a standard payment gateway account feature. To request the Expanded Credits Capability (ECC) feature, you must submit an application. For more information about the ECC application, please see http://www.authorize.net/files/ecc.pdf.

IMPORTANT: A transaction ID must **not** be submitted with an Unlinked Credit. If ECC is enabled for your account, and a transaction ID is submitted with the Unlinked Credit transaction, then the payment gateway will attempt to apply the credit to an original transaction with the transaction ID submitted.

Note:	If you are using SIM, we strongly recommend that you only submit Unlinked Credit transactions through the Virtual Terminal. This transaction type requires the submission of full sensitive customer information, which requires a greater level of compliance with the Payment Card Industry (PCI) Data Security Standard. If your business needs the ability to submit this transaction type from a custom application, please use AIM. For more information about AIM, please see the *AIM Developer Guide* at http://developer.authorize.net/guides/AIM/.

Void

This transaction type is used to cancel an original transaction that not yet settled and prevents it from being sent for settlement. A Void can be submitted against any other transaction type.

Note:	If you are unsure of whether a transaction is settled, you can attempt to submit a Void first. If the Void errors, the original transaction is likely settled, in which case you can submit a Credit for the transaction.

The payment gateway accepts Voids if the following conditions are met:

- The transaction is submitted with the valid transaction ID of an original, successfully authorized transaction.

- The original transaction is not already settled, expired or errored.

If this transaction type is required, we recommend you process the transactions by logging on to the Merchant Interface directly, or by using a desktop application that uses AIM. The merchant can search for the transaction by Transaction ID, then open the Transaction Details page for that transaction.

Using the Merchant Interface

The Merchant Interface allows you to manage transactions, capture Authorization Only transactions, void transactions, and issue refunds. These transaction types can also be managed automatically using AIM or SIM if you are integrating a custom application to the payment gateway. However, for most integrations, these transaction types can be more conveniently and easily managed in the Merchant Interface.

Unsettled Transactions

On the Unsettled Transactions page you can select a single or multiple Authorization Only transactions to capture. You can also void transactions from the Unsettled Transactions page. For more information on how to submit these transaction types, click **Unsettled Transactions** under Search in the Merchant Interface main menu and then click the **Help** link in the top right corner of the Unsettled Transactions page.

Virtual Terminal

Refunds (Credit and Unlinked Credit) and Capture Only transactions can be submitted through the Virtual Terminal feature of the Merchant Interface. For information on how to use the Virtual Terminal, click **Virtual Terminal** under Tools in the Merchant Interface main menu and then click the **Help** link in the top right corner of the Virtual Terminal page.

Refunds submitted through the Virtual Terminal for original transactions processed through the payment gateway require the Transaction ID of the original transaction. You can obtain this information by searching for the original transaction on the Search Transactions page of the Merchant Interface and viewing the transaction details. For information on how to search transactions, click **Transactions** under Search in the Merchant Interface main menu and then click the **Help** link in the top right corner of the Transaction Search page.

If ECC is enabled for your account and you would like to submit a refund through the Virtual Terminal that is associated with a transaction that was **not** originally processed on the payment gateway, you must **not** provide a transaction ID. If a transaction ID is submitted, the payment gateway will attempt to apply the credit to an original payment gateway transaction.

Section 3
Integration Settings

Most integration settings in the Merchant Interface apply to both Server Integration Method (SIM) and Advanced Integration Method (AIM). However, some are specific to the connection method you are using. This section details all the settings you should be aware of in the Merchant Interface that will help you achieve and maintain a strong connection to the payment gateway.

Access Settings

In order to connect a website or proprietary business application to the payment gateway, you should be familiar with the API Login ID and Transaction Key. These values authenticate you as an authorized merchant when submitting transaction requests.

API Login ID

The API Login ID is a complex value that is at least eight characters in length, includes uppercase and lowercase letters, numbers, and/or symbols and identifies your account to the payment gateway. It is *not* the same as your login ID for logging into the Merchant Interface. The two perform different functions. The API Login ID is a login ID that your website uses when communicating with the payment gateway to submit transactions. It is only used for your website or other business application's connection to the payment gateway.

The API Login ID for your account is available in the Settings menu of the Merchant Interface.

IMPORTANT: The API Login ID is a sensitive piece of account information and should only be shared on a need-to-know basis, for example with your Web developer. Be sure to store it securely.

To obtain your API Login ID:

1. Log on to the Merchant Interface at https://account.authorize.net
2. Select **Settings** under Account in the main menu on the left
3. Click **API Login ID and Transaction Key** in the Security Settings section
4. If you have not already obtained an API Login ID and Transaction Key for your account, you will need to enter the secret answer to the secret question you configured at account activation.
5. Click **Submit**.

The API Login ID for your account is displayed on the API Login ID and Transaction Key page.

It is highly recommended that you reset your API Login ID regularly, such as every six months, to strengthen the security of your payment gateway account. To reset your API Login ID you need to contact Authorize.Net Customer Support. You will then need to communicate the new API Login ID to your Web developer immediately to update your website integration code. Failure to do so will result in a disruption in transaction processing.

Note: The above directions apply when Multiple User Accounts is activated for your account. If this feature is not enabled for your account, you will need to activate it in order to generate and view the API Login ID in the Merchant Interface. Otherwise your current login ID is the same as the API Login ID for your account.

Transaction Key

The Transaction Key is a 16-character alphanumeric value that is randomly generated in the Merchant Interface. It works in conjunction with your API Login ID to authenticate you as an authorized user of the Authorize.Net Payment Gateway when submitting transactions from your website.

Like the API Login ID, the Transaction Key is a sensitive piece of account information that should only be shared on a need-to-know basis.

To obtain a Transaction Key:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Select **Settings** under Account in the main menu on the left

3. Click **API Login ID and Transaction Key** in the Security Settings section

4. Enter the secret answer to the secret question you configured when you activated your user account

5. Click **Submit**

The Transaction Key for your account is displayed on a confirmation page.

IMPORTANT: Be sure to record your Transaction Key immediately in a secure manner or copy it immediately to a file in a secure location, since it is not always visible in the Merchant Interface like the API Login ID. Once you navigate away from the confirmation page, there is no other way to access the Transaction Key in the Merchant Interface. You would have to generate a new Transaction Key.

It is highly recommended that you create a new Transaction Key regularly, such as every six months, to strengthen the security of your payment gateway account. You then need to communicate the new Transaction Key to your Web developer immediately to update your website integration code. Failure to do so will result in a disruption in transaction processing.

General Settings

The following settings are important for all connections to the Authorize.Net Payment Gateway and should be configured for your account to achieve optimal performance and security. You might need to contact your Web developer to be sure that your website is coded to interact properly with these settings.

Test Mode

Test Mode allows you to test your website connection to the payment gateway without actually processing live transactions. Once activated, your account is already in Test Mode by default. While in Test Mode, the payment gateway will accept test transactions as a simulation of how actual transactions would be accepted or declined, but **payment data will not actually be submitted for processing**. Test transactions will not be stored and cannot be retrieved from the payment gateway.

IMPORTANT: Please contact your Web developer for help with submitting test transactions.

It is important that you leave your account in Test Mode until your connection to the payment gateway is successfully tested and ready to process live transactions. You can place your account in Test Mode at any time to test updates to your website connection, or in the event that you need to quickly turn off transaction processing.

To turn Test Mode off or on:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Select **Settings** under Account in the main menu on the left

3. Click **Test Mode** in the Security Settings section

4. Click **Turn Test OFF** to take your account out of Test Mode. Click **Turn Test ON** to place your account in Test Mode

Transaction Cut-Off Time

The Transaction-Cut-Off Time is the time of day that your transactions are batched and submitted by the payment gateway to the processing network for settlement. You can specify the time that your batch should be submitted for settlement each day. The default Transaction Cut-Off Time for your account is 3:00 PM Pacific time. Transactions submitted after your Transaction Cut-Off Time will be included with the next day's batch. You can contact your Merchant Service Provider for their recommendation on what time is best for your account's Transaction Cut-Off Time to optimize the settlement timeframe for your transactions.

To configure the transaction cut-off time for your account:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Select **Settings** under Account in the main menu on the left

3. Select **Transaction Cut-Off Time** in the Business Settings section

4. Select the desired cut-off time from the drop-down lists

5. Click **Submit**

Transaction Details API

Enabling this feature allows you to set up applications to retrieve information about your transactions and settled batches. Security is maintained by sending your API Login ID and Transaction Key with the API calls.

For example, enabling the Transaction Details API allows you to retrieve data such as:

- Settlement information for a batch, or batches within a date range

- Data for all transactions in a specified batch

- Detailed information about a specific transaction

All calls to the Transaction Details API require merchant authentication to ensure they originate from authorized sources. This implementation of the merchant Web services API supports authentication using the API Login ID and Transaction Key.

To enable the Transaction Details API:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Select **Settings** under Account in the main menu on the left

3. Click the **Transaction Details API** link in the Security Settings section. The Transaction Details API screen opens.

4. Enter the answer to your Secret Question, then click **Enable Transaction Details API**.

5. When you have successfully enabled the **Transaction Details API**, the **Settings** page displays.

Standard Transaction Security Settings

The following standard transaction security settings are recommended for all payment gateway accounts as a general way to identify and prevent suspicious transactions.

Address Verification Service (AVS) Filter

Bankcard processors implemented the Address Verification Service (AVS) to aid merchants in the detection of suspicious transaction activity. The payment processing network compares the billing address provided in the transaction with the cardholder's address on file at the credit card issuing bank. The processing network returns an AVS response code that indicates the results of this comparison to the payment gateway. You can configure your account to reject certain transactions based on the AVS code returned. For example, the AVS code "A" indicates that the street address matched, but the first five digits of the ZIP Code did not.

The following result codes are possible.

AVS CODE	DESCRIPTION
A	The street address matches, but the 5-digit ZIP code does not
B	Address information was not submitted in the transaction information, so AVS check could not be performed
E	The AVS data provided is invalid, or AVS is not allowed for the card type submitted
G	The credit card issuing bank is of non-U.S. origin and does not support AVS
N	Neither the street address nor the 5-digit ZIP code matches the address and ZIP code on file for the card
P	AVS is not applicable for this transaction
R	AVS was unavailable at the time the transaction was processed. Retry transaction
S	The U.S. card issuing bank does not support AVS
U	Address information is not available for the customer's credit card
W	The 9-digit ZIP code matches, but the street address does not match
Y	The street address and the first 5 digits of the ZIP code match perfectly
Z	The first 5 digits of the ZIP code matches, but the street address does not match

Note: AVS responses **B**, **E**, **R**, **G**, **U**, **S** and **N** are the default payment gateway AVS transaction rejection settings, meaning that when these codes are returned, transactions are automatically rejected by the payment gateway. These default settings can be modified in the Merchant Interface.

To configure transaction rejection settings based on the AVS response code:

1. Log on to the Merchant Interface at https://account.authorize.net
2. Select **Settings** under Account in the main menu on the left

3. Click **Address Verification Service** in the Security Settings section

4. Click to select the check box(es) next to the AVS codes for which the payment gateway should reject transactions

5. Click **Submit**

Transactions will be processed against your rejection criteria immediately.

Note: In order to use the AVS filter, you need to require the billing address and ZIP code fields when collecting payment information from your customers. Please communicate these requirements to your Web developer.

Tips for using AVS:

- AVS response code **N** (neither the street address nor the ZIP code matches the address and ZIP code on file for the card) is the most fundamental AVS check. Select **N** to implement the most basic AVS protection from suspicious transaction activity.

- If you choose not to select **N**, then there is no need to select the following response codes: **B**, **E**, **R**, **G**, **U**, and **S**. These codes indicate that the address could not be verified by the card issuer. If transactions are NOT being rejected when they are returned with an **N** response, then it is unnecessary to reject transactions that could not be verified with the issuer.

- To avoid errors when accepting gift credit cards (stored-value cards with a Visa, MasterCard, Discover or American Express logo), you will need to deselect the **U** response code. For this type of transaction, the customer's billing address will most likely not be associated with the gift card, or will not exist on file at the issuing bank.

- Not all banks outside the United States will return the **G, U** and **S** response codes. Therefore, this code is not absolutely effective for limiting suspicious transactions from outside of the United States.

- If you want to accept International payments, you must deselect the **G**, **U** and **S** response codes.

- The desired response code in most cases is **Y** (the street address and the first 5 digits of the ZIP code match perfectly). Select this response code to reject transactions **only** after very careful consideration, because legitimate matches might be rejected when **Y** is selected.

The AVS filter is designed to provide a basic level of protection from suspicious transactions. However, the AVS filter is not intended for use as an absolute protection nor is it intended for use in all processing scenarios, because there are many reasons why an address and ZIP code might not match. You are not required to reject a transaction due to an AVS mismatch, but it is recommended that you enable some level of address verification. However, most banks and Merchant Service Providers require use of the AVS system in order to avoid non-qualified transaction surcharges (typically an additional 1%). For this reason, it is recommended that you enable some level of address verification to avoid non-qualified transaction surcharges. Please note, however, that you are responsible for applicable transaction fees incurred for transactions declined due to an AVS mismatch (as with any other declined transaction).

If your business has a low risk factor, or if potentially paying a non-qualified discount rate will not adversely affect your business, you might consider being lenient in your application of the AVS filter. Conversely, if you anticipate a high frequency of suspicious transaction activity or if you are incurring abnormally high discount rate charges, the AVS filter might be an appropriate method of protection.

To obtain the transaction's Authorization Code:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Transactions** under Search in the main menu on the left

3. Enter the applicable search criteria to look up the transaction, for example, the payment gateway settlement date or customer name. If you have the Transaction ID, simply enter that value in the **Transaction ID** field

4. Click **Search** at the bottom of the page

5. Click on the Transaction ID for the declined transaction to view the details

6. The Authorization Code is located in the Authorization Information section of the Transaction Detail page

To perform a Capture Only transaction:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Tools** from the tool bar at the top of the page

3. Select **Capture Only** from the Select Transaction Type section of the Virtual Terminal page

4. Enter the required transaction information (indicated with an asterisk) including the Authorization Code

5. Click **Submit**

Note: Because a Capture Only transaction requires the customer's full credit card number and expiration date, you might need to contact the customer to collect this information. In addition, your transaction processing rates for Capture Only transactions might be downgraded (increased). Please contact your Merchant Service Provider for more information.

If you would like to void the authorization for the transaction so that the customer's funds can be released back to their card, you will need to call the credit card issuing bank, since the payment gateway does not allow a Void transaction for a decline. You must have the Authorization Code for this request and you must know the credit card type that was used, and your Merchant Number associated with that Card Association (for example, Visa). If you don't know your Merchant Number, please call your Merchant Service Provider.

Credit Card Verification (CCV) Filter

The Credit Card Verification Code, or Card Code, is a three- or four-digit security code that is printed on the back of credit cards (or on the front for American Express cards) in reverse italics in the card's signature panel.

Figure 1. Finding the card code on a credit card
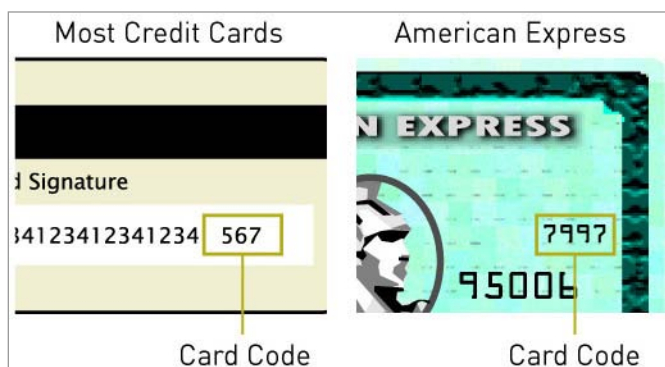
You can choose to collect this information from the customer and submit the data to the payment gateway, as another method for authenticating credit card transactions submitted through your

account. The payment gateway will pass this information to the credit card issuer along with the credit card number. The credit card issuer will determine if the value matches the value on file for the customer's credit card and return a code to the payment gateway indicating whether the code matched, in addition to indicating whether the card was authorized. You can configure the payment gateway to reject transactions based on the code returned.

CARD CODE RESPONSE	DESCRIPTION
N	The Card Code does not match
P	The Card Code was not processed
S	The Card Code was not indicated
U	Card Code is not supported by the card issuer

Note: There are no default payment gateway settings for the Card Code filter. To use this feature, you need to configure the appropriate rejection settings.

To configure transaction rejection settings based on the Card Code response:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Select **Settings** under Account in the main menu on the left

3. Click **Card Code Verification** in the Security Settings section

4. Click to select the check box(es) next to the Card Code responses for which the payment gateway should reject transactions

5. Click Submit

Note: In order to use the CCV filter, you need to require the Card Code field either on the payment gateway hosted payment form or your own custom payment form. Please communicate these requirements to your Web developer.

Overriding a CCV Decline

If you would like to accept a transaction that was declined by the payment gateway due to CCV filtering, you can submit a Capture Only transaction in the Virtual Terminal. This is possible because the transaction was declined by the payment gateway *after* the transaction was successfully authorized and the funds placed on hold at the credit card issuing bank. The Authorization Code issued for the transaction can be obtained in the Merchant Interface.

Note: The Authorization Code is required for submitting a Capture Only transaction.

-Required Mode

Password-Required Mode is a security setting that requires the account Transaction Key to be submitted with all transactions for authentication purposes. This setting is enabled for all payment gateway accounts by default and should always be on for SIM and AIM merchants.

To verify that Password-Required Mode is enabled for your account:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **Password-Required Mode** in the Security Settings section

4. If it is unchecked, click to select the check box labeled **Require Password for ALL Transactions**

5. Click **Submit**

Server Integration Method (SIM) Settings

If you are connecting to the payment gateway using SIM, this section describes the integration settings you will need to understand in order to configure them properly in the Merchant Interface.

IMPORTANT: Please be aware that connection settings that can be configured in the Merchant Interface can also be hard coded in your website code. To maintain a robust connection to the payment gateway, it is highly recommended that you work closely with your Web developer or third-party solution provider to identify those settings that should be hard coded in your website code versus those settings that you might need to configure yourself from time to time in the Merchant Interface.

Form Settings

SIM merchants use the payment gateway hosted payment form for collecting and submitting customer payment information. You can customize the hosted payment form to include additional transaction fields and to match the look and feel of your website.

Fields on the Payment Form

By default, the payment gateway hosted page will always display the fields required to post a transaction, which are:

For credit card transactions:

- Amount

- Credit Card Number

- Expiration Date

For eCheck.Net® transactions:

- Amount

- ABA Routing Number

- Bank Account Number

- Bank Account Type

- Bank Name

- Bank Account Name

Note: eCheck.Net® fields only appear on the hosted payment form if the eCheck.Net service is enabled for your payment gateway account. eCheck.Net® is Authorize.Net's exclusive electronic check processing solution. For more information on how eCheck.Net can help you potentially increase sales and how to sign up, visit http://www.authorize.net/echeck.

To configure additional fields that you would like to appear on your payment form:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **Payment Form** in the Transaction Format Settings section

4. Click **Form Fields**

5. Click to select the checkbox(es) in the **View** column next to the fields you would like to display on your payment form

6. For each field you are adding, click to select the check boxes in the **Edit** and **Required** columns if you would also like to configure either or both of these attributes for the field

- **View** – The customer can view but not edit the information. For example, if you would like to display an invoice number. Information that is **View** only should be submitted with the transaction information to the payment gateway. Contact your Web developer for more information.

- **Edit** – The customer can view and/or edit the information but the field is not required to submit the transaction. For example, if you would like to collect but not require the customer's email address, configuring the field as **View** and **Edit** allows the customer to provide this information with the transaction.

- **Required** – The customer must provide the information in order to submit the transaction. For example, if you would like to require the customer's card code. When requiring this field, the **View**, **Edit** *and* **Required** attributes must be configured.

7. Click **Submit**

Be sure to test your payment form any time you update fields and their attributes to be sure that it meets your requirements.

IMPORTANT: If you choose to use the Address Verification Service (AVS) and Card Code Verification (CCV) transaction security features, you must collect billing address and Card Code information from the customer on the payment gateway hosted payment form.

The following table lists the additional payment form fields you can configure for the hosted payment form in the Merchant Interface.

Note: Payment form field settings can also be submitted to the payment gateway as a part of your website's integration code. To be sure that payment form settings included in your website integration code do not conflict with payment form settings you configure in the Merchant Interface, it is recommended that you discuss your payment form field requirements with your Web developer.

FIELD	VALUE	NOTES
PAYMENT INFORMATION		
Recurring Billing Transaction	The recurring billing status	Indicates whether the transaction is a recurring billing transaction.
Card Code	The customer's card code	The three- or four-digit number on the back of a credit card (on the front for American Express). This field is required if you would like to use the Card Code Verification (CCV) security feature.
eCheck Type	The type of eCheck.Net transaction	Applicable only when eCheck.Net is enabled for the payment gateway account. For more information about eCheck.Net, visit http://www.authorize.net/echeck. Indicates the type of eCheck.Net payment request.
ORDER INFORMATION		
Invoice Number	The merchant assigned invoice number for the transaction	The invoice number must be created dynamically on the merchant server or provided on a per-transaction basis. The payment gateway does not perform this function. Also, in order to be included on the hosted

FIELD	VALUE	NOTES
		payment form, the attribute **View** must be configured for this field in the Merchant Interface payment form settings.
Description	The transaction description	The description must be created dynamically on the merchant server or provided on a per-transaction basis. The payment gateway does not perform this function. Also, in order to be displayed, the attribute **View** must be configured for this field in the Merchant Interface payment form settings.
BILLING INFORMATION		
First Name	The first name associated with the customer's billing address	
Last Name	The last name associated with the customer's billing address	
Company	The company associated with the customer's billing address	
Address	The customer's billing address	Required if the merchant would like to use the Address Verification Service filter.
City	The city of the customer's billing address	
State	The state of the customer's billing address	
ZIP Code	The ZIP code of the customer's billing address	Required if the merchant would like to use the Address Verification Service filter.
Country	The country of the customer's billing address	
Phone	The phone number associated with the customer's billing address	
FAX	The fax number associated with the customer's billing address	
Email	The customer's valid email address	The email address to which the customer's email receipt is sent. The email is sent to the customer only if the email address format is valid.
Customer ID	The merchant-assigned customer ID	The unique identifier to represent the customer associated with the transaction. Also, in order to be displayed, the attribute **View** must be configured for this field in the Merchant Interface payment form settings.
SHIPPING INFORMATION		
First Name	The first name associated with	

FIELD	VALUE	NOTES
	the customer's shipping address	
Last Name	The last name associated with the customer's shipping address	
Company	The company associated with the customer's shipping address	
Address	The customer's shipping address	
City	The city of the customer's shipping address	
State	The state of the customer's shipping address	
ZIP Code	The ZIP code of the customer's shipping address	
Country	The country of the customer's shipping address	
ADDITIONAL SHIPPING INFORMATION (Level 2 Data)		
Tax	The valid tax amount	The tax amount charged. When configured in the integration code, this field can also include a tax item name and description. Contact your Web developer for more information. The total amount of the transaction must *include* this amount.
Freight	The valid freight amount	The freight amount charged. When configured in the integration code, this field can also include a freight item name and description. Contact your Web developer for more information. The total amount of the transaction must *include* this amount.
Duty	The valid duty amount OR delimited duty information	The duty amount charged. When configured in the integration code, this field can also include a duty item name and description. Contact your Web developer for more information. The total amount of the transaction must *include* this amount.
Tax Exempt	The tax exempt status	Indicates whether the transaction is tax exempt.
Purchase Order Number	The merchant assigned purchase order number	The purchase order number must be created dynamically on the merchant server or provided on a per-transaction basis. The payment gateway does not perform this function. Also, in order to be displayed, the attribute **View** must be configured for this field in the Merchant

FIELD	VALUE	NOTES
		Interface payment form settings.

Note: The hosted payment form can be configured to submit either Authorization and Capture or Authorization Only transactions. Please communicate any preferences regarding which of these credit card transaction types should be used for your website transactions to your Web developer.

Customizing the Hosted Payment Form

When using the payment gateway hosted payment form, you can also configure the following settings to match the look of your website:

- The color of the text

- The color of link text

- The font style, font size and color of body text and heading text

- The background color for the form, and for headings

- The header text (this can include HTML)

- The footer text (this can include HTML)

To configure the look of the payment gateway hosted payment form:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **Payment Form** in the Transaction Submission section

4. Click on any of the provided links to configure the different elements of the payment form

For specific instructions, click the **Help** link at the top right corner of each Merchant Interface page.

Basic HTML guide

When customizing headers and/or footers for your hosted payment form and receipt page, you can use the following basic hypertext markup language (HTML) tags and codes to specify font and paragraph formatting and create hyperlinks. Simply use the following tags around your text, as shown in the examples.

FORMAT	HTML TAGS OR CODES	EXAMPLE	RENDERING
Bold	Opening tag: `<b>` Closing tag: `</b>`	`<b>Your text here</b>`	**Your text here**
Italic	Opening tag: `<i>` Closing tag: `</i>`	`<i>Your text here</i>`	*Your text here*
Bold Italic	Opening tags: `<b><i>` Closing tags: `</i></b>`	`<b><i>Your text here</i></b>`	***Your text here***
Line Break	Opening tag: ` ` Closing tag: Not needed	`Your text here`	Your text here

FORMAT	HTML TAGS OR CODES	EXAMPLE	RENDERING
Horizontal Rule	Opening tag: `<hr />` Closing tag: Not needed	`Your<hr>text<hr>here`	Your ——————— text ——————— here
Paragraph	Opening tag: `<p>` Closing tag: `</p>`	`Your<p>paragraphs</p>` `<p>here</p>`	Your paragraphs here

Hyperlink	Opening tag: `<a href="URL here">`
	
	Closing tag: `</a>`
		`<a href=`
		`"http://www.yourURL.com"`
		`> Link text here</a>`
			[Link text here]()

Email Link	Opening tag: `<a href= "mailto:email address here">`
	
	Closing tag: `</a>`
		`<a href="mailto:your@`
		`emailaddress.com">your@e`
		`mailaddress.com</a>`
			your@emailaddress.com

Single Quote	Left single quote: `‘` Right single quote: `’`	`‘Your text` `here’`	'Your text here'
Double Quote	Left double quote: `“` Right double quote: `”`	`“Your text` `here”`	"Your text here"

There are many ways to use HTML code in the payment form and receipt page headers and footers. You can reference a cascading style sheet (CSS). A CSS is a separate HTML document that defines formatting styles such as font and text color and size. Please contact your Web developer with any questions you have about using HTML tags and codes, or about using a CSS in your form headers and footers.

Logos and background images

If you would like to use a logo and/or background image on the hosted payment form, image files must be uploaded to the payment gateway server in order to be displayed properly. The location of the logo and background images on the payment gateway server must be referenced in the header or footer.

To upload a logo or background image to the payment gateway:

1. Save the file in any of the following formats: .gif, .jpg, .or png (other file formats will not be accepted).

2. If needed, rename the logo or background image according to the following Authorize.Net naming convention:

   • Only use letters, numbers and/or the underscore character

   • Do not use spaces

   • You must include your merchant ID and one of the following prefixes for identification purposes: logo_, background_, header_, footer. (If you do not know your merchant ID, refer to the Merchant Profile page in the Account menu of the Merchant Interface.)

Good Examples:	Bad Examples:
logo_*merchantIDhere*.jpg	logo.jpg
background_*merchantIDhere*.png	background.jpg
header_*merchantIDhere*.jpg	online forms.png
footer_*merchantIDhere*.gif	

3. Send the logo and/or background file in an email to support@authorize.net with the subject line "Payment Form Image Upload." The images are then uploaded to a secure payment gateway server.

4. To reference the logo or background image, add the following HTML to the payment form and/or receipt page header or footer. Replace *filename.ext* with the name of your image file:

```
<img src="https://account.authorize.net/mgraphics/filename.ext">
```

Note: The maximum character length allowed when configuring header or footer text in the Merchant Interface is 255. If you are including a lot of text, links or graphics, you need to arrange with your Web developer to include the header information as part of the integration code. There is no character limit when configuring payment form header text in the integration code.

If you are not comfortable uploading an image to the payment gateway or adding HTML to the form header or footer yourself, ask your Web developer for help.

Receipt page options

In addition to the secure hosted payment form, SIM also provides two options for communicating the transaction results to the customer: the payment gateway hosted receipt page OR Relay Response.

- The hosted receipt page is a brief transaction summary that is displayed in the customer's Web browser from the secure payment gateway server. It can be configured to match the look and feel of your website.

- The Relay Response feature of SIM allows you to create a custom receipt page using transaction results information returned by the payment gateway. The custom receipt page is then relayed by the payment gateway to the customer's Web browser.

Note: Only one receipt page option should be implemented. Implementing both options can cause integration errors. Please contact your Web developer for help deciding which receipt option best meets your business needs.

Hosted Receipt Page
The formatting of the hosted receipt page is similar to the formatting configured for the hosted payment form. For example, the text and link color and background color will be the same. However, the following settings are unique to the hosted receipt page.

- The receipt link (the URL or Web address included on the hosted receipt page that will return customers to your website)

- The receipt method (the link method, for example, a regular link or a button)

> **Note:** Please contact your Web developer before changing the receipt method setting, because it might depend on how your website is integrated to the payment gateway.

- The color of the text

- The color of link text

- The font style, font size and color of body text and heading text

- The background color for the form, and for headings

- Receipt link text (the text that should be displayed for the link back to your website)

- The header text (this can include HTML)

- The footer text (this can include HTML)

To configure the payment gateway hosted receipt page:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Select **Settings** under Account in the main menu on the left

3. Click **Receipt Page** in the Transaction Response section

4. Click on any of the provided links to configure the different elements of the receipt page

For specific instructions, click the **Help** link at the top right corner of each Merchant Interface page.

Relay Response

A Relay Response configuration indicates to the payment gateway that you would like to receive the transaction response and use it to create a custom receipt page for display to the customer.

To configure Relay Response for your transactions:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **Relay Response** in the Transaction Format Settings section

4. Enter the URL to which the payment gateway should post the transaction response for custom receipt page formatting

5. Click **Submit**

Configuring this URL in effect enables Relay Response for your payment gateway account.

> **Note:** The Relay Response URL should only be configured if a Relay Response is desired. Configuring both the hosted receipt page and a Relay Response can result in a failed implementation. Contact your Web developer to verify that only one of the hosted receipt page and Relay Response options are configured for your integration.

Silent Post URL

If you would like to use transaction response information for purposes other than creating a custom receipt page, such as integration with proprietary business processes or applications, a Silent Post URL can also be configured in the Merchant Interface. The Silent Post URL is a location on your Web server where the payment gateway can "carbon copy" the transaction response. This allows you to use transaction response information for other purposes separately without affecting the amount of time it takes to respond to the payment gateway with a custom receipt page from the Relay Response URL.

Note: The Silent Post URL feature does not apply to transactions made using the Hosted Payment Form.

To configure the Silent Post URL:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **Silent Post URL** in the Transaction Format Settings section

4. Enter the secondary URL to which you would like the payment gateway to copy the transaction response

5. Click **Submit**

MD5 Hash

The MD5 Hash feature allows you to authenticate that transaction responses are securely received from Authorize.Net. The payment gateway creates the MD5 hash using the following pieces of account and transaction information as input:

-   MD5 Hash value

-   API Login ID (Use the user login ID for Virtual Terminal connections.)

-   Transaction ID

-   Transaction Amount

The MD5 Hash value is a random value that you configure in the Merchant Interface.

To configure an MD5 Hash value for your account:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **MD5-Hash** in the Security Settings section

4. Enter any random value to use for your MD5 Hash Value. Enter the value again to confirm

5. Click **Submit**

Please note that the MD5 Hash value is not displayed on the screen once submitted. You will need to store the value securely and update your Web developer any time you change the value.

ARB subscription transactions do not use a login ID when generating the hash value, they use only the Transaction ID, amount, and hash value.

Note: MD5 Hash values are generated and sent to merchants, even if you have not specified a value in the Merchant Interface.

Email Receipt

In addition to the hosted payment form and receipt page, the payment gateway also provides an email receipt. You can choose to send an email receipt to any customer who provides their email address. The email receipt includes a summary and results of the transaction. To the customer, this email appears to be sent from the merchant email address that is configured as the Email Sender in the User Profile settings of the Merchant Interface.

To choose to send an email receipt to your customers:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under Account in the main menu on the left

3. Click **Email Receipt** in the Transaction Format Settings section

4. Click to select the check box labeled **Email transaction receipt to customer**

5. Click **Submit** to save changes

This setting also allows you to customize text for the email receipt header and footer. Add the header and footer text you would like to use for your email receipts in the appropriate text fields.

To verify or configure the Email Sender for your account:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **User Profile** under **Account** in the main menu on the left OR if this option is not available for your account, click **Settings** in the Account section

3. Click **Edit Profile Information** OR if you are in the Settings menu, click **Manage Contacts** in the **Business Settings** section and click **Edit** next to the account contact that should be configured as the Email Sender

4. Click to select the check box labeled **Use this email address as sender** in the **Specify Email Sender** section

5. Click **Submit** to save changes

You can also choose to receive a confirmation email from the payment gateway at the completion of each transaction, which includes the results of the transaction and order information.

To receive confirmation emails:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **User Profile** under Account in the main menu on the left OR if this option is not available for your account, click **Settings** in the Account section

3. Click **Edit Profile Information** OR if you are in the Settings menu, click **Manage Contacts** in the Business Settings section and click **Edit** next to the account contact that should receive confirmation emails

4. Click to select the check box labeled **Transaction Receipt** in the Transaction Emails section

5. Click **Submit** to save changes

If you are an Account Owner or Account Administrator, you can configure these settings for other users as well on the User Administration page in the Account menu.

1. Click **User Administration** under account in the Merchant Interface main menu

2. Click on the name of the user who you would like to receive the confirmation email

3. Click Edit Profile Information

4. Click to select the check box labeled **Transaction Receipt** in the Transaction Emails section

5. Click **Submit** to save changes

Advanced Integration Method (AIM) Settings

If you are connecting to the payment gateway using AIM, the following sections describe the integration settings you need to understand in order to configure them properly in the Merchant Interface.

Please be aware that connection settings that can be configured in the Merchant Interface can also be hard-coded in your website code. To maintain a robust connection to the payment gateway, it is highly recommended that you work closely with your Web developer to identify those settings that

should be hard coded in your website code versus those settings that you might need to configure yourself from time to time in the Merchant Interface.

Please keep in mind that AIM involves the collection, transmission, and storage of cardholder data on your Web server. Because of this, compliance with the PCI Data Security Standard is required by the Card Associations. For more information, please see our *Security Best Practices White Paper* at http://www.authorize.net/files/securitybestpractices.pdf and *Developer Best Practices White Paper* at http://www.authorize.net/files/developerbestpractices.pdf.

Direct Response

For AIM, the payment gateway communicates transaction response information to the merchant Web server directly and securely with a delimited text string. Delimited means that each piece of information in the string is separated by a distinct character indicating to computer programs where one piece of information ends and the next begins.

Though the payment gateway formats this information using a default field separating character (a comma), you can configure this and additional settings to ensure that information is communicated between the merchant Web server and payment gateway correctly at all times.

In addition to the field separator, you can configure an encapsulation character. An encapsulation character works similarly to the field separator and is really only necessary in the event that the field separator could potentially be included in an actual field value. For example, if the default field separator is a comma, but a piece of information in the transaction response includes a comma as part of a value, (street address or company name, etc.), it will cause an error for computer programs trying to extract information from the string. As an additional protection from this type of error, the encapsulation character wraps around each piece of information to further differentiate it from the other values. In the example below, the comma is the field separator and the quotation marks are the encapsulation character.

```
"AUTH_CAPTURE","12-98790","Jane","Doe","Jane's, Inc.","201 Center St.",
```

Depending on the computer programs that will be using the information, you might need to configure custom field separator and encapsulation characters for your transaction responses from the payment gateway. It is recommended that you use characters that are uncommon in transaction information values, for example, the pipe (|).

To configure direct response:

1. Log on to the Merchant Interface at https://account.authorize.net

2. Click **Settings** under **Account** in the main menu on the left

3. Click **Direct Response** in the **Transaction Format Settings** section

4. Click to select the radio button labeled **Yes** next to **Delimited Response**

5. Select the character you would like to use from the **Field Separator** drop-down list

6. Select the character you would like to use from the **Field Encapsulation Character** drop-down list

7. Click **Submit**

Note: Check with your Web developer before changing field separator and encapsulation characters, because it might affect the integration of transaction response information with other computer programs.

Cardholder Authentication Programs

The Authorize.Net Payment Gateway provides support for cardholder authentication information passed from third party solutions for Verified by Visa and MasterCard® SecureCode®. If you use such a service in conjunction with your website transactions, additional integration is required for your website. Contact your Web developer and refer them to the "Cardholder Authentication" section of the *Advanced Integration Method (AIM) Developer Guide* at http://developer.authorize.net/guides/AIM/.

Note: Cardholder authentication is currently supported for AIM transactions only through the Chase Paymentech, FDMS Nashville, Global Payments and TSYS processors for Visa and MasterCard transactions. If cardholder authentication information is submitted for transactions processed through any other processor, it will be ignored.

eCheck.Net® Transactions

If you are signed up for eCheck.Net®, you are required to submit the following information for electronic check transactions:

- ABA Routing Number

- Bank Account Number

- Bank Account Type

- Bank Name

- Bank Account Name

- eCheck.Net Type

Because of this, additional integration is required for your website. Contact your Web developer and refer them to the *eCheck.Net® Developer Guide* at http://developer.authorize.net/guides/echeck.pdf for more information. For more information about the eCheck.Net service, see http://www.authorize.net/echeck.

Additional Integration Features

The following sections provide information about integration features that don't involve settings in the Merchant Interface, but that do provide additional capabilities for your integration to the payment gateway and transaction processing.

Itemized Order Information

Based on your unique business requirements, you can choose to submit itemized order, or line item, information with each transaction. Itemized order information is not submitted to the processor and is not currently returned with the transaction response. However, this information is displayed on the Transaction Detail page and in the QuickBooks® download file reports in the Merchant Interface. For more information about these features, please see the Merchant Interface Online Help Files (after logging into the Merchant Interface, click the **Help** link in the top right corner of the page).

Unlike most other integration settings for your account, this feature is not configured in the Merchant Interface. Please contact your Web developer for more information on how to submit detailed order information with transactions to the payment gateway.

Merchant-Defined Fields

You can also choose to submit merchant-defined fields to further customize the information that is included with a transaction. Merchant-defined fields are any fields that are not recognized by the payment gateway as standard application programming interface (API) payment form fields. For example, you might provide a field in your checkout process where customers could provide specific shipping instructions or product color information.

Merchant-defined fields are included with the transaction response and in the merchant confirmation email for the merchant's records. However, they are *not* provided on the Transaction Detail page in the Merchant Interface. Contact your Web developer for more information on how to submit merchant-defined fields with transactions to the payment gateway.

Section 4
Transaction Response

The payment gateway will return transaction results for all Advanced Integration Method (AIM) transactions and Server Integration Method (SIM) with Relay Response transactions. The transaction response indicates whether the transaction was accepted or declined and includes information about the transaction.

The field order applies only to AIM transactions. For SIM transactions, the transaction response fields are not necessarily sent in the exact order listed here. Developers are encouraged to use the name of the field in order to locate the correct response. If your code expects transaction response fields in a particular order, future updates to the SIM API may cause unexpected results from your code

Fields included in the payment gateway response are provided in the table below.

ORDER	FIELD NAME	VALUE	FORMAT	NOTES
1	Response Code	The overall status of the transaction	1 = Approved 2 = Declined 3 = Error 4 = Held for Review	
2	Response Subcode	A code used by the payment gateway for internal transaction tracking		This field applies to CNP AIM only, and is obsolete.
3	Response Reason Code	A code that represents more details about the result of the transaction	Numeric	See the "Response Codes Details" section of this document for a listing of response reason codes.
4	Response Reason Text	A brief description of the result, which corresponds with the response reason code	Text	
5	Authorization Code	The authorization or approval code	6 characters	
6	AVS Response	The Address Verification Service (AVS) response code	A = Address (Street) matches, ZIP does not B = Address information not provided for AVS check E = AVS error G = Non-U.S. Card Issuing	Indicates the result of the AVS filter. See the "Address Verification Service (AVS) Filter" section of this document for more information.

ORDER	FIELD NAME	VALUE	FORMAT	NOTES
			Bank	
			N = No Match on Address (Street) or ZIP	
			P = AVS not applicable for this transaction	
			R = Retry – System unavailable or timed out	
			S = Service not supported by issuer	
			U = Address information is unavailable	
			W = 9 digit ZIP matches, Address (Street) does not	
			X = Address (Street) and 9 digit ZIP match	
			Y = Address (Street) and 5 digit ZIP match	
			Z = 5 digit ZIP matches, Address (Street) does not	
7	Transaction ID	The payment gateway assigned identification number for the transaction		This value must be used for Credit, Prior Authorization and Capture and Void transactions.
8	Invoice Number	The merchant assigned invoice number for the transaction	Up to 20 characters (no symbols)	
9	Description	The transaction description	Up to 255 characters (no symbols)	
10	Amount	The amount of the transaction	Up to 15 digits	
11	Method	The payment method	CC or ECHECK	
12	Transaction Type	The type of credit card transaction	AUTH_CAPTURE, AUTH_ONLY, CAPTURE_ONLY, CREDIT, PRIOR_AUTH_CAPTURE, VOID	
13	Customer ID	The merchant assigned customer ID	Up to 20 characters (no symbols)	
14	First Name	The first name associated with the customer's billing	Up to 50 characters (no symbols)	

35

ORDER	FIELD NAME	VALUE	FORMAT	NOTES
		address		
15	Last Name	The last name associated with the customer's billing address	Up to 50 characters (no symbols)	
16	Company	The company associated with the customer's billing address	Up to 50 characters (no symbols)	
17	Address	The customer's billing address	Up to 60 characters (no symbols)	
18	City	The city of the customer's billing address	Up to 40 characters (no symbols)	
19	State	The state of the customer's billing address	Up to 40 characters (no symbols) or a valid two-character state code	
20	ZIP Code	The ZIP code of the customer's billing address	Up to 20 characters (no symbols)	
21	Country	The country of the customer's billing address	Up to 60 characters (no symbols)	
22	Phone	The phone number associated with the customer's billing address	Up to 25 digits (no letters) Ex. (123)123-1234	
23	Fax	The fax number associated with the customer's billing address	Up to 25 digits (no letters) Ex. (123)123-1234	
24	Email Address	The customer's valid email address	Up to 255 characters	
25	Ship To First Name	The first name associated with the customer's shipping address	Up to 50 characters (no symbols)	
26	Ship To Last Name	The last name associated with the customer's shipping address	Up to 50 characters (no symbols)	
27	Ship To Company	The company associated with the customer's shipping address	Up to 50 characters (no symbols)	

ORDER	FIELD NAME	VALUE	FORMAT	NOTES
28	Ship To Address	The customer's shipping address	Up to 60 characters (no symbols)	
29	Ship To City	The city of the customer's shipping address	Up to 40 characters (no symbols)	
30	Ship To State	The state of the customer's shipping address	Up to 40 characters (no symbols) or a valid two-character state code	
31	Ship To ZIP Code	The ZIP code of the customer's shipping address	Up to 20 characters (no symbols)	
32	Ship To Country	The country of the customer's shipping address	Up to 60 characters (no symbols)	
33	Tax	The tax amount charged	Numeric	Delimited tax information is not included in the transaction response.
34	Duty	The duty amount charged	Numeric	Delimited duty information is not included in the transaction response.
35	Freight	The freight amount charged	Numeric	Delimited freight information is not included in the transaction response.
36	Tax Exempt	The tax exempt status	TRUE, FALSE, T, F, YES, NO, Y, N, 1, 0	
37	Purchase Order Number	The merchant assigned purchase order number	Up to 25 characters (no symbols)	
38	MD5 Hash	The payment gateway generated MD5 hash value that can be used to authenticate the transaction response.		See the "MD5 Hash" section of this document for more information. This feature is not necessary for AIM.
39	Card Code Response	The card code verification (CCV) response code	M = Match N = No Match P = Not Processed S = Should have been present U = Issuer unable to process request	Indicates the result of the CCV filter. See the "Card Code Verification (CCV) Filter" section of this document for more information.
40	Cardholder	The cardholder	Blank or not present =	

ORDER	FIELD NAME	VALUE	FORMAT	NOTES
	Authentication Verification Response	authentication verification response code	CAVV not validated 0 = CAVV not validated because erroneous data was submitted 1 = CAVV failed validation 2 = CAVV passed validation 3 = CAVV validation could not be performed; issuer attempt incomplete 4 = CAVV validation could not be performed; issuer system error 5 = Reserved for future use 6 = Reserved for future use 7 = CAVV attempt – failed validation – issuer available (U.S.-issued card/non-U.S acquirer) 8 = CAVV attempt – passed validation – issuer available (U.S.-issued card/non-U.S. acquirer) 9 = CAVV attempt – failed validation – issuer unavailable (U.S.-issued card/non-U.S. acquirer) A = CAVV attempt – passed validation – issuer unavailable (U.S.-issued card/non-U.S. acquirer) B = CAVV passed validation, information only, no liability shift	
41	Account Number	Last 4 digits of the card provided	Alphanumeric (XXXX6835)	This field is returned with all transactions.
42	Card Type	Visa, MasterCard, American Express, Discover, Diners Club, EnRoute, JCB	Text	
43	Split Tender ID	The value that links the current authorization request to the original authorization request. This value	Alphanumeric	This is only returned in the reply message for the first transaction that receives a partial authorization.

Last revised: 5/31/2011

ORDER	FIELD NAME	VALUE	FORMAT	NOTES
		is returned in the reply message from the original authorization request		
44	Requested Amount	Amount requested in the original authorization	Numeric	This is present if the current transaction is for a prepaid card or if a splitTenderId was sent in.
45	Balance On Card	Balance on the debit card or prepaid card	Numeric	Can be a positive or negative number. This is present if the current transaction is for a prepaid card or if a splitTenderId was sent in.

Response Code Details

The following tables describe the response codes and response reason texts that are returned for each transaction.

- **Response Code** indicates the overall status of the transaction with possible values of approved, declined, errored held for review.

- **Response Reason Code** is a numeric representation of a more specific reason for the transaction status

- **Response Reason Text** details the specific reason for the transaction status. This information can be returned to you and/or the customer to provide more information about the status of their transaction.

Response Codes

RESPONSE CODE	DESCRIPTION
1	This transaction has been approved.
2	This transaction has been declined.
3	There has been an error processing this transaction.
4	This transaction is being held for review.

Response Reason Codes and Response Reason Text

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
1	1	This transaction has been approved.	
2	2	This transaction has been declined.	
2	3	This transaction has been declined.	
2	4	This transaction has been declined.	The code returned from the processor indicating that the card used needs to be picked up.
3	5	A valid amount is required.	The value submitted in the amount field did not pass validation for a number.
3	6	The credit card number is invalid.	
3	7	The credit card expiration date is invalid.	The format of the date submitted was incorrect.
3	8	The credit card has expired.	
3	9	The ABA code is invalid.	The value submitted in the `x_bank_aba_code` field did not pass validation or was not for a valid financial institution.
3	10	The account number is invalid.	The value submitted in the `x_bank_acct_num` field did not pass validation.
3	11	A duplicate transaction has been submitted.	A transaction with identical amount and credit card information was submitted two minutes prior.
3	12	An authorization code is required but not present.	A transaction that required `x_auth_code` to be present was submitted without a value.
3	13	The merchant API Login ID is invalid or the account is inactive.	
3	14	The Referrer or Relay Response URL is invalid.	The Relay Response or Referrer URL does not match the merchant's configured value(s) or is absent. This applies only to SIM

Last revised: 5/31/2011

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
3	15	The transaction ID is invalid.	The transaction ID value is non-numeric or was not present for a transaction that requires it (i.e., VOID, PRIOR_AUTH_CAPTURE, and CREDIT).
3	16	The transaction was not found.	The transaction ID sent in was properly formatted but the gateway had no record of the transaction.
3	17	The merchant does not accept this type of credit card.	The merchant was not configured to accept the credit card submitted in the transaction.
3	18	ACH transactions are not accepted by this merchant.	The merchant does not accept electronic checks.
3	19 - 23	An error occurred during processing. Please try again in 5 minutes.	
3	24	The Nova Bank Number or Terminal ID is incorrect. Call Merchant Service Provider.	
3	25 - 26	An error occurred during processing. Please try again in 5 minutes.	
2	27	The transaction resulted in an AVS mismatch. The address provided does not match billing address of cardholder.	
2	28	The merchant does not accept this type of credit card.	The Merchant ID at the processor was not configured to accept this card type.
2	29	The Paymentech identification numbers are incorrect. Call Merchant Service Provider.	
2	30	The configuration with the processor is invalid. Call Merchant Service Provider.	
2	31	The FDC Merchant ID or Terminal ID is incorrect. Call Merchant Service Provider.	The merchant was incorrectly set up at the processor.
3	32	This reason code is reserved or not applicable to this API.	
3	33	*FIELD* cannot be left blank.	The word *FIELD* will be replaced by an actual field name. This error indicates that a field the merchant specified as required was not filled in.
2	34	The VITAL identification numbers are incorrect. Call Merchant Service Provider.	The merchant was incorrectly set up at the processor.
2	35	An error occurred during processing.	The merchant was incorrectly set up

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
		Call Merchant Service Provider.	at the processor.
3	36	The authorization was approved, but settlement failed.	
2	37	The credit card number is invalid.	
2	38	The Global Payment System identification numbers are incorrect. Call Merchant Service Provider.	The merchant was incorrectly set up at the processor.
3	40	This transaction must be encrypted.	
2	41	This transaction has been declined.	Only merchants set up for the FraudScreen.Net service would receive this decline. This code will be returned if a given transaction's fraud score is higher than the threshold set by the merchant.
3	43	The merchant was incorrectly set up at the processor. Call your Merchant Service Provider.	The merchant was incorrectly set up at the processor.
2	44	This transaction has been declined.	The card code submitted with the transaction did not match the card code on file at the card issuing bank and the transaction was declined.
2	45	This transaction has been declined.	This error would be returned if the transaction received a code from the processor that matched the rejection criteria set by the merchant for both the AVS and Card Code filters.
3	46	Your session has expired or does not exist. You must log in to continue working.	
3	47	The amount requested for settlement cannot be greater than the original amount authorized.	This occurs if the merchant tries to capture funds greater than the amount of the original authorization-only transaction.
3	48	This processor does not accept partial reversals.	The merchant attempted to settle for less than the originally authorized amount.
3	49	A transaction amount greater than $[amount] will not be accepted.	The transaction amount submitted was greater than the maximum amount allowed.
3	50	This transaction is awaiting settlement and cannot be refunded.	Credits or refunds can only be performed against settled transactions. The transaction against which the credit/refund was submitted has not been settled, so a credit cannot be issued.
3	51	The sum of all credits against this transaction is greater than the original	

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
		transaction amount.	
3	52	The transaction was authorized, but the client could not be notified; the transaction will not be settled.	
3	53	The transaction type was invalid for ACH transactions.	If x_method = ECHECK, x_type cannot be set to CAPTURE_ONLY.
3	54	The referenced transaction does not meet the criteria for issuing a credit.	
3	55	The sum of credits against the referenced transaction would exceed the original debit amount.	The transaction is rejected if the sum of this credit and prior credits exceeds the original debit amount.
3	56	This merchant accepts ACH transactions only; no credit card transactions are accepted.	The merchant processes eCheck.Net transactions only and does not accept credit cards.
3	57 - 63	An error occurred in processing. Please try again in 5 minutes.	
2	65	This transaction has been declined.	The transaction was declined because the merchant configured their account through the Merchant Interface to reject transactions with certain values for a Card Code mismatch.
3	66	This transaction cannot be accepted for processing.	The transaction did not meet gateway security guidelines.
3	68	The version parameter is invalid.	The value submitted in x_version was invalid.
3	69	The transaction type is invalid.	The value submitted in x_type was invalid.
3	70	The transaction method is invalid.	The value submitted in x_method was invalid.
3	71	The bank account type is invalid.	The value submitted in x_bank_acct_type was invalid.
3	72	The authorization code is invalid.	The value submitted in x_auth_code was more than six characters in length.
3	73	The driver's license date of birth is invalid.	The format of the value submitted in x_drivers_license_dob was invalid.
3	74	The duty amount is invalid.	The value submitted in x_duty failed format validation.
3	75	The freight amount is invalid.	The value submitted in x_freight failed format validation.
3	76	The tax amount is invalid.	The value submitted in x_tax failed format validation.
3	77	The SSN or tax ID is invalid.	The value submitted in

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
			x_customer_tax_id failed validation.
3	78	The Card Code (CVV2/CVC2/CID) is invalid.	The value submitted in x_card_code failed format validation.
3	79	The driver's license number is invalid.	The value submitted in x_drivers_license_num failed format validation.
3	80	The driver's license state is invalid.	The value submitted in x_drivers_license_state failed format validation.
3	81	The requested form type is invalid.	The merchant requested an integration method not compatible with the AIM API.
3	82	Scripts are only supported in version 2.5.	The system no longer supports version 2.5; requests cannot be posted to scripts.
3	83	The requested script is either invalid or no longer supported.	The system no longer supports version 2.5; requests cannot be posted to scripts.
3	84 - 90	This reason code is reserved or not applicable to this API.	
3	91	Version 2.5 is no longer supported.	
3	92	The gateway no longer supports the requested method of integration.	
3	97	This transaction cannot be accepted.	Applicable only to SIM API. Fingerprints are only valid for a short period of time. This code indicates that the transaction fingerprint has expired.
3	98	This transaction cannot be accepted.	Applicable only to SIM API. The transaction fingerprint has already been used.
3	99	This transaction cannot be accepted.	Applicable only to SIM API. The server-generated fingerprint does not match the merchant-specified fingerprint in the x_fp_hash field.
3	100	The eCheck.Net type is invalid.	Applicable only to eCheck.Net. The value specified in the x_echeck_type field is invalid.
3	101	The given name on the account and/or the account type does not match the actual account.	Applicable only to eCheck.Net. The specified name on the account and/or the account type do not match the NOC record for this account.
3	102	This request cannot be accepted.	A password or Transaction Key was submitted with this WebLink request. This is a high security risk.

Last revised: 5/31/2011

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
3	103	This transaction cannot be accepted.	A valid fingerprint, Transaction Key, or password is required for this transaction.
3	104	This transaction is currently under review.	Applicable only to eCheck.Net. The value submitted for country failed validation.
3	105	This transaction is currently under review.	Applicable only to eCheck.Net. The values submitted for city and country failed validation.
3	106	This transaction is currently under review.	Applicable only to eCheck.Net. The value submitted for company failed validation.
3	107	This transaction is currently under review.	Applicable only to eCheck.Net. The value submitted for bank account name failed validation.
3	108	This transaction is currently under review.	Applicable only to eCheck.Net. The values submitted for first name and last name failed validation.
3	109	This transaction is currently under review.	Applicable only to eCheck.Net. The values submitted for first name and last name failed validation.
3	110	This transaction is currently under review.	Applicable only to eCheck.Net. The value submitted for bank account name does not contain valid characters.
3	116	The authentication indicator is invalid.	This error is only applicable to Verified by Visa and MasterCard SecureCode transactions. The ECI value for a Visa transaction; or the UCAF indicator for a MasterCard transaction submitted in the x_authentication_indicator field is invalid.
3	117	The cardholder authentication value is invalid.	This error is only applicable to Verified by Visa and MasterCard SecureCode transactions. The CAVV for a Visa transaction; or the AVV/UCAF for a MasterCard transaction is invalid.
3	118	The combination of authentication indicator and cardholder authentication value is invalid.	This error is only applicable to Verified by Visa and MasterCard SecureCode transactions. The combination of authentication indicator and cardholder authentication value for a Visa or MasterCard transaction is invalid. For more information, see the "Cardholder Authentication" section of this document.

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
3	119	Transactions having cardholder authentication values cannot be marked as recurring.	This error is only applicable to Verified by Visa and MasterCard SecureCode transactions. Transactions submitted with a value in x_authentication_indicator *and* x_recurring_billing=YES will be rejected.
3	120	An error occurred during processing. Please try again.	The system-generated void for the original timed-out transaction failed. (The original transaction timed out while waiting for a response from the authorizer.)
3	121	An error occurred during processing. Please try again.	The system-generated void for the original errored transaction failed. (The original transaction experienced a database error.)
3	122	An error occurred during processing. Please try again.	The system-generated void for the original errored transaction failed. (The original transaction experienced a processing error.)
3	123	This account has not been given the permission(s) required for this request.	The transaction request must include the API Login ID associated with the payment gateway account.
2	127	The transaction resulted in an AVS mismatch. The address provided does not match billing address of cardholder.	The system-generated void for the original AVS-rejected transaction failed.
3	128	This transaction cannot be processed.	The customer's financial institution does not currently allow transactions for this account.
3	130	This payment gateway account has been closed.	IFT: The payment gateway account status is Blacklisted.
3	131	This transaction cannot be accepted at this time.	IFT: The payment gateway account status is Suspended-STA.
3	132	This transaction cannot be accepted at this time.	IFT: The payment gateway account status is Suspended-Blacklist.
2	141	This transaction has been declined.	The system-generated void for the original FraudScreen-rejected transaction failed.
2	145	This transaction has been declined.	The system-generated void for the original card code-rejected and AVS-rejected transaction failed.
3	152	The transaction was authorized, but the client could not be notified; the transaction will not be settled.	The system-generated void for the original transaction failed. The response for the original transaction could not be communicated to the client.

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
2	165	This transaction has been declined.	The system-generated void for the original card code-rejected transaction failed.
3	170	An error occurred during processing. Please contact the merchant.	Concord EFS – Provisioning at the processor has not been completed.
2	171	An error occurred during processing. Please contact the merchant.	Concord EFS – This request is invalid.
2	172	An error occurred during processing. Please contact the merchant.	Concord EFS – The store ID is invalid.
3	173	An error occurred during processing. Please contact the merchant.	Concord EFS – The store key is invalid.
2	174	The transaction type is invalid. Please contact the merchant.	Concord EFS – This transaction type is not accepted by the processor.
3	175	The processor does not allow voiding of credits.	Concord EFS – This transaction is not allowed. The Concord EFS processing platform does not support voiding credit transactions. Please debit the credit card instead of voiding the credit.
3	180	An error occurred during processing. Please try again.	The processor response format is invalid.
3	181	An error occurred during processing. Please try again.	The system-generated void for the original invalid transaction failed. (The original transaction included an invalid processor response format.)
3	185	This reason code is reserved or not applicable to this API.	
4	193	The transaction is currently under review.	The transaction was placed under review by the risk management system.
2	200	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The credit card number is invalid.
2	201	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The expiration date is invalid.
2	202	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The transaction type is invalid.
2	203	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The value submitted in the amount field is invalid.
2	204	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The department code is invalid.

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
2	205	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The value submitted in the merchant number field is invalid.
2	206	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The merchant is not on file.
2	207	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The merchant account is closed.
2	208	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The merchant is not on file.
2	209	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. Communication with the processor could not be established.
2	210	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The merchant type is incorrect.
2	211	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The cardholder is not on file.
2	212	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The bank configuration is not on file.
2	213	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The merchant assessment code is incorrect.
2	214	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. This function is currently unavailable.
2	215	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The encrypted PIN field format is invalid.
2	216	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The ATM term ID is invalid.
2	217	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. This transaction experienced a general message format problem.
2	218	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The PIN block format or PIN availability value is invalid.

Last revised: 5/31/2011

48

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
2	219	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The ETC void is unmatched.
2	220	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The primary CPU is not available.
2	221	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. The SE number is invalid.
2	222	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. Duplicate auth request (from INAS).
2	223	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. This transaction experienced an unspecified error.
2	224	This transaction has been declined.	This error code applies only to merchants on FDC Omaha. Please re-enter the transaction.
3	243	Recurring billing is not allowed for this eCheck.Net type.	The combination of values submitted for x_recurring_billing and x_echeck_type is not allowed.
3	244	This eCheck.Net type is not allowed for this Bank Account Type.	The combination of values submitted for x_bank_acct_type and x_echeck_type is not allowed.
3	245	This eCheck.Net type is not allowed when using the payment gateway hosted payment form.	The value submitted for x_echeck_type is not allowed when using the payment gateway hosted payment form.
3	246	This eCheck.Net type is not allowed.	The merchant's payment gateway account is not enabled to submit the eCheck.Net type.
3	247	This eCheck.Net type is not allowed.	The combination of values submitted for x_type and x_echeck_type is not allowed.
2	250	This transaction has been declined.	This transaction was submitted from a blocked IP address.
2	251	This transaction has been declined.	The transaction was declined as a result of triggering a Fraud Detection Suite filter.
4	252	Your order has been received. Thank you for your business!	The transaction was accepted, but is being held for merchant review. The merchant can customize the customer response in the Merchant Interface.
4	253	Your order has been received. Thank	The transaction was accepted and was authorized, but is being held for

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
		you for your business!	merchant review. The merchant can customize the customer response in the Merchant Interface.
2	254	Your transaction has been declined.	The transaction was declined after manual review.
3	261	An error occurred during processing. Please try again.	The transaction experienced an error during sensitive data encryption and was not processed. Please try again.
3	270	The line item [item number] is invalid.	A value submitted in x_line_item for the item referenced is invalid.
3	271	The number of line items submitted is not allowed. A maximum of 30 line items can be submitted.	The number of line items submitted exceeds the allowed maximum of 30.
3	289	This processor does not accept zero dollar authorization for this card type.	Your credit card processing service does not yet accept zero dollar authorizations for Visa credit cards. You can find your credit card processor listed on your merchant profile.
3	290	One or more required AVS values for zero dollar authorization were not submitted.	When submitting authorization requests for Visa, the address and zip code fields must be entered.
4	295	The amount of this request was only partially approved on the given prepaid card. Additional payments are required to complete the balance of this transaction.	
3	296	The specified SplitTenderId is not valid.	
3	297	A Transaction ID and a Split Tender ID cannot both be used in a single transaction request.	
3	300	The device ID is invalid.	The value submitted for x_device_id is invalid.
3	301	The device batch ID is invalid.	The value submitted for x_device_batch_id is invalid.
3	303	The device batch is full. Please close the batch.	The current device batch must be closed manually from the POS device.
3	304	The original transaction is in a closed batch.	The original transaction has been settled and cannot be reversed.
3	305	The merchant is configured for auto-close.	This merchant is configured for auto-close and cannot manually close batches.
3	306	The batch is already closed.	The batch is already closed.
1	307	The reversal was processed	The reversal was processed

RESPONSE CODE	RESPONSE REASON CODE	RESPONSE REASON TEXT	NOTES
		successfully.	successfully.
1	308	Original transaction for reversal not found.	The transaction submitted for reversal was not found.
3	309	The device has been disabled.	The device has been disabled.
1	310	This transaction has already been voided.	This transaction has already been voided.
1	311	This transaction has already been captured	This transaction has already been captured.
2	315	The credit card number is invalid.	This is a processor-issued decline.
2	316	The credit card expiration date is invalid.	This is a processor-issued decline.
2	317	The credit card has expired.	This is a processor-issued decline.
2	318	A duplicate transaction has been submitted.	This is a processor-issued decline.
2	319	The transaction cannot be found.	This is a processor-issued decline.

Note: A very helpful tool for troubleshooting errors is available in our Developer Center at http://developer.authorize.net/tools/responsereasoncode.