



Merchant Menu User's Guide

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION TO AUTHORIZE.NET	4
OVERVIEW	4
PURPOSE OF THE MERCHANT MENU USER GUIDE	4
ENTITIES INVOLVED IN THE PAYMENT PROCESS	5
THE TRANSACTION PROCESS	6
THE CREDIT CARD SETTLEMENT PROCESS	7
CHAPTER 2 GETTING STARTED	8
MERCHANT MENU LOGIN	8
INTERVIEW AREA	8
SECOND INTERVIEW AREA	10
AUTHORIZE.NET SERVICE AND SOFTWARE LICENSE AGREEMENT AREA	10
eCHECK.NET SERVICE AGREEMENT AREA	11
THE MERCHANT MENU HOME SCREEN	11
CHAPTER 3 SETTINGS AREA	12
GENERAL MERCHANT SETTINGS	13
MANAGE CONTACT INFORMATION	14
PAYMENT FORM/RECEIPT SETTINGS	16
MANAGE URLS	22
AUTOMATED DIRECT CONNECT (ADC) SETTINGS	26
TRANSACTION BATCH UPLOAD SETTINGS	28
ADDRESS VERIFICATION SYSTEM (AVS) FILTER	30
FRAUDSCREEN.NET	33
CVV2 AND CVC2 SETTINGS	37
TRANSACTION CUTOFF TIME	39
CHAPTER 4 VIRTUAL TERMINAL	40
PROCESSING CREDIT CARD TRANSACTIONS	40
PROCESSING eCHECK.NET TRANSACTIONS	41
ISSUING CREDITS USING THE VIRTUAL TERMINAL	41
PROCESSING AUTHORIZATION-ONLY TRANSACTIONS	43
SUBMITTING eCHECK.NET TRANSACTIONS WITHOUT CAPTURING FUNDS	43
PROCESSING CAPTURE-ONLY TRANSACTIONS	44
PARTIAL ORDER FULFILLMENT*	44
CHAPTER 5 TRANSACTION ACTIVITY AND BATCH UPLOADS	46
TRANSACTION ACTIVITY	46
CURRENT BATCH OF TRANSACTIONS	47
VIEW RETURNED ITEMS	50
DOWNLOAD TRANSACTIONS	51
VIEW STATISTICS	52

VIEWING SUMMARY STATISTICS	52
BATCH UPLOADS	53
CHAPTER 6 ACCOUNT INFORMATION	54
CHAPTER 7 SUPPORT	56
EMAILING SUPPORT FROM YOUR MERCHANT MENU	56
INDEX	57

Chapter 1 Introduction to Authorize.Net

Overview

The Internet represents a tremendous opportunity for your business—whether you're a budding entrepreneur looking to market and sell your great new idea or a large corporation searching for new ways to increase sales. But selling goods and services on the Internet presents its own set of challenges in setting up and maintaining a secure, reliable, and cost-effective system for authorizing payment and managing transactions. If you don't know what you're doing—and even if you do—that can be difficult, complicated, and expensive.

Authorize.Net removes the barriers that might prevent you from efficiently doing business on the Internet. We take care of the complex issues for you with our advanced transaction processing system. You can process and manage transactions over the Internet through the Authorize.Net payment system with as little as a credit card merchant account, a computer with a Web browser, and an Internet connection.

Purpose of the Merchant Menu User Guide

The following Merchant Menu User Guide will acquaint you with the Authorize.Net Merchant Menu and the Authorize.Net processing system. Using the Merchant Menu, you will be able to customize your Authorize.Net account and supervise your transaction activity. This will help to maximize your productivity and satisfaction as an Authorize.Net Merchant.

Entities involved in the Payment Process

Your Merchant account has multiple entities involved, including: You (the **Merchant**), the **Merchant Service Provider (MSP)**, the **Payment Processor**, and **Authorize.Net** (the Payment Gateway and Acquirer of eCheck.Net transactions).

Merchant

A Merchant is a person or entity selling goods or services. Your Merchant account enables you to accept and charge credit cards.

Merchant Service Provider

The Merchant Service Provider (MSP) is a bank or Independent Sales Organization (ISO). Usually, your Merchant Service Provider also acts as your Authorize.Net Reseller, selling you the Authorize.Net service(s). Among other things, the MSP normally does the following:

- Assigns you a Merchant Account Number.
- Sets up your Authorize.Net account.
- Assigns you a Login ID and password for use with your Authorize.Net account.
- Acts as your main point of contact for basic issues regarding your Merchant and Authorize.Net accounts.
- Enables you to add certain types of credit cards to your Merchant account.
- Activates processing capability for those cards on your Authorize.Net account (if the Merchant Service Provider is also your Authorize.Net Reseller).
- Deposits credit card funds to your Merchant account.

Authorize.Net

Authorize.Net is your electronic gateway to the payment-processing network, allowing you to submit your information securely to the Payment Processor. Authorize.Net receives the results of the credit card transaction from the Payment Processor, records the results in its database, then displays the results to the merchant and/or customer. Authorize.Net also acts the acquirer of eCheck.Net (electronic check) transactions.

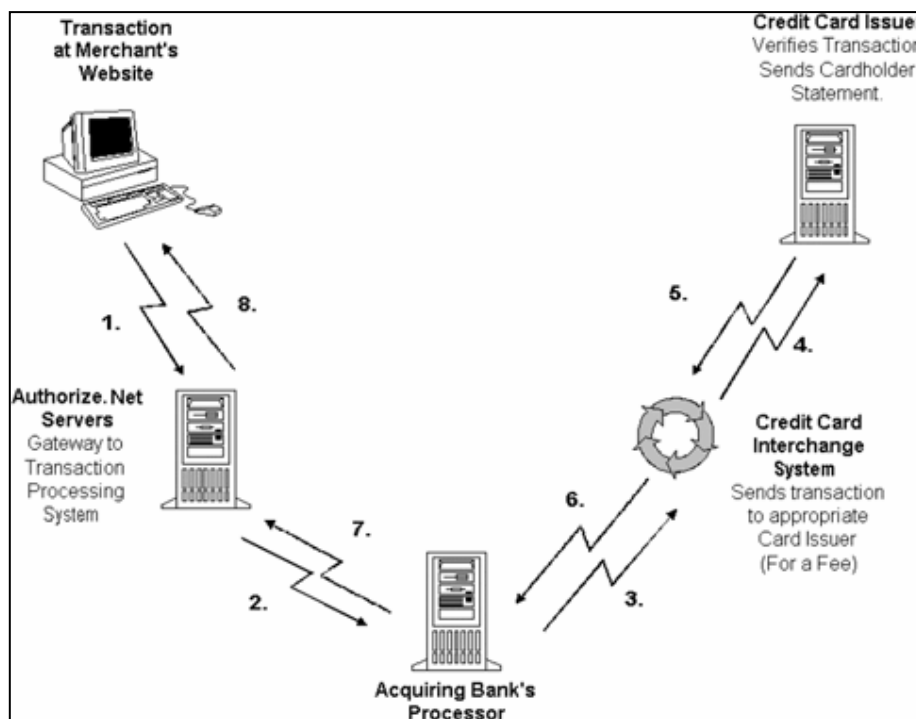
Payment Processor

The Payment Processor submits credit card information through the credit card interchange system to the cardholder's bank, returning transaction results to Authorize.Net.

The Transaction Process

The following explanation and diagram describe the interactions that occur when processing a credit card transaction through Authorize.Net.

Figure 1.1 The Transaction Process



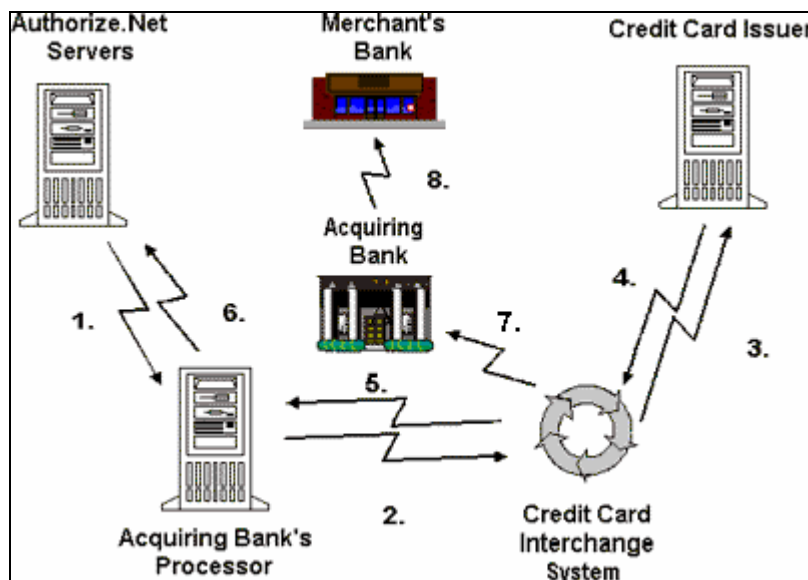
1. A transaction passes from the Merchant's website to the Authorize.Net Processing Gateway.
2. The transaction is transmitted to the Acquiring Bank's processor.
3. The Acquiring Bank's processor passes the transaction to the Credit Card Interchange system.
4. The Credit Card Interchange system queries the appropriate Card Issuer database.
5. The Card Issuer approves or declines the transaction, places hold on funds, and passes result/authorization code back through the Credit Card Interchange system.
6. The Credit Card Interchange system relays the transaction result to the Acquiring Bank's processor.
7. The Acquiring Bank's processor relays the transaction result to Authorize.Net servers.
8. Authorize.Net servers store the results and transmit them back to the customer and/or Merchant.

Note: On average, these steps typically take place in 3 to 4 seconds!

The Credit Card Settlement Process

The following explanation and diagram explain what takes place during the settlement process, which is the means by which funds are actually transferred from the customer's bank to yours.

Figure 1.2 Credit Card Settlement Process



1. Authorize.Net servers automatically transmit batches of transactions to the Acquiring Bank's processor.
2. The Acquiring Bank's processor passes the transaction batches to the Credit Card Interchange system.
3. The Credit Card Interchange system routes to the appropriate Card Issuer database.
4. The Card Issuer verifies transactions, passes results through the Credit Card Interchange system, and passes funds to the Interchange system.
5. The Interchange system relays transaction process results to the Acquiring Bank's processor, and passes funds to the Acquiring Bank. The Acquiring Bank passes remaining funds to the Merchant's bank account.
6. The Acquiring Bank's processor passes transaction results to Authorize.Net servers.

Billing

There are fees associated with your use of Authorize.Net services, as explained in your agreement(s) with Authorize.Net. You can view your fees in the **Account Information** section of your Merchant Menu. More information about this section of your Merchant Menu is located in **Chapter 6 Account Information**.

Chapter 2 Getting Started

Merchant Menu Login

As soon as you receive your Merchant Login ID and password, log in to your Merchant Menu. To log in to your Merchant Menu, you must have access to the World Wide Web on the Internet (such as through Microsoft Internet Explorer, Netscape, etc.). Type <https://secure.authorize.net/> in the browser's address bar. At this site, you will be prompted to enter your Login ID and password. Your Reseller (usually the same as your merchant service provider) will provide you with your Login ID and password once your account has been created on the system. Your account will not be "live" (ready to process real transactions) until your merchant account is active. Upon logging in for the first time, we strongly recommend that you change your password to an alphanumeric value at least seven digits in length. Keep the password in a secure place and refrain from distributing it to anyone who does not need access to your merchant account interface.

NOTE: Your account will be locked out after five failed attempts at login. You may reattempt to login after 15 minutes.

Figure 2.1 Login Screen



The screenshot shows the Authorize.Net login interface. At the top left is the Authorize.Net logo, which consists of a blue diamond shape with horizontal lines, followed by the text 'Authorize.Net™' and the tagline 'Where the world does business on the Web'. Below the logo are two text input fields. The first is labeled 'Login ID:' and the second is labeled 'Password:'. Below the password field is a button labeled 'Log In'.

Interview Area

When you log in for the first time, you will see a screen prompting you to verify information that the Reseller provided to Authorize.Net while setting up your Authorize.Net account. If this information is *incorrect*, you should email Authorize.Net at support@authorize.net with the correct information, and Authorize.Net will make necessary changes. If the information is *correct*, click **Next** to continue to the next screen.

Figure 2.2 Example First Interview Screen

Welcome to Authorize.Net!

Please verify the information shown below that your Merchant Service Provider provided our system about your business. Incorrect information on this screen may delay or prevent transferring funds to you once transactions have been processed. Accordingly, if any of the following information is incorrect, please immediately email any corrections, along with your Authorize.Net loginID (failure to include your loginID will prevent us from effecting a change in information to your account), to support@Authorize.Net BEFORE CONTINUING. Allow 24 hours for this corrected information to be updated in our system, after which you may re-attempt your login.

Merchant Business Information

Name Joe Merchant
Address 1234 Elm Street
City, State, Zip Anywhere, MyState, 12345
Phone 888-555-5555
Fax 888-555-5556

Owner or Principal Information

Full Name Joe Merchant
Title Owner
Home Address 1234 Elm Street
City, State, Zip Anywhere, MyState, 12345
Home Phone 888-555-5555

Figure 2.3 Example Second Interview Screen

It is strongly suggested that you change the password on your account now. (Note: your new password will not be posted until the end of this survey)

Current Password

New Password

Retype New Password

The credit card number is for secondary collection purposes only. Under normal circumstances your card will never be charged.

Credit Card Number

Expiration Date (mm/yyyy)

The following items of information are required for you to be able to process transactions.

Website Homepage URL (g.e. http://www.myhomepage.com)

Brief Description Of Your Business

Please specify your Time Zone and whether or not you observe Daylight Savings Time. This information is used for keeping all of your receipts and reports in your local time.

Time Zone Pacific Time

Daylight Savings

The following questions will allow us to better serve you in future releases and product offerings.

How Internet savvy are you? Select One

How are you personally connected to the Internet? Select One

Which web browser do you use? Select One

Which operating system do you use? Select One

What is your #1 concern about doing business on the Internet? Select One

What percentage of your business is Internet based? Select One

How many employees do you have? Select One

Second Interview Area

The next screen will request the following:

- Your current and new passwords.
- Credit card information (for backup billing purposes).
- Your website homepage URL (your web address) and a brief description of your business.
- Your time zone and whether or not you observe Daylight Savings Time.
- Basic information about your interaction with the Internet and computer technology.

Figure 2.4 Authorize.Net Service and Software License Agreement

Transaction Processing Terms

This Agreement is entered into the day and year indicated on the Authorize Net Transaction Processing Terms & Software License Agreement (herein after referred to as the "Agreement") by and between Authorize Net Corporation, whose principal place of business is 3311 North University Avenue, Provo, Utah, 84604 (hereinafter referred to as "Authorize Net"), and "Merchant," whose name, complete address, business organization and type of business are stated on the Agreement. Authorize Net is a subsidiary of Go2Net, Inc., a Delaware corporation whose principal place of business is in Seattle, Washington. For purposes of this Agreement the corporate entities Authorize Net Corporation and Go2Net, Inc. shall be synonymous. In consideration of the premises set forth herein, Authorize Net and Merchant hereby agree as follows:

1. Authorize Net agrees to perform transaction processing services for Merchant. This includes the acceptance and authorization of transactions forwarded from Merchant in a timely manner, the subsequent transmission of transactions to the processing network and the detailed reporting of those transactions via Merchant's web-based Merchant Menu.
2. By signing the Agreement, Merchant understands and agrees that the Authorize Net Transaction Processing Services require additional charges, as indicated above under Schedule of Fees, to be billed directly by Authorize Net to the Merchant and payable pursuant to paragraphs 14 and 16 listed below.
3. By signing this document, Merchant will indemnify, protect, defend and hold Authorize Net, affiliates and / or subsidiaries and all of its officers, agents and / or employees, harmless from and against any and all claims, losses, demands, actions, expenses, damages, liability, and / or causes of action, including (without limitation) attorneys' fees, other costs of defense and / or collection fees, which in any way result directly or indirectly from:
 - a. Merchant breach of this Agreement or any warranty or representation made to Authorize Net;
 - b. Any damage or loss caused by negligence, fraud, dishonesty or willful behavior by Merchant or any of Merchant employees or agents;
 - c. Any contention, whether well-founded, baseless or otherwise, that Merchant violated the law or any rule or regulation;
 - d. Any damages resulting from or related to any failure or delay of Authorize Net in providing Transaction Processing services under this Agreement; or
 - e. Any delays in the performance of services hereunder or for any failure to perform same hereunder if such delays are due to strikes, inclement weather, acts of God, or other causes beyond Authorize Net's reasonable control. Authorize Net will not be liable for performance of services where delayed by war, riots, embargoes, strikes, or acts of its vendors and suppliers, concealed acts of workmen (whether of Authorize Net or others), or accidents.

The indemnifications provided for in this Article shall survive any termination of this Agreement.

4. Merchant warrants to Authorize Net all of the following:
 - a. That all representations and statements made by Merchant in this Agreement, or in any other document relating hereto, by Merchant or on Merchant's behalf are true, accurate and complete in all material respects. Merchant hereby authorizes Authorize Net to investigate and confirm the information herein. For this purpose, Authorize Net may utilize credit bureau / reporting agencies and / or its own agents. Upon Merchant's request, Authorize Net will provide Merchant with a copy of the results of such investigation.
 - b. That Merchant is engaged in the lawful business shown on the Agreement which includes the sale of merchandise and / or services, and is duly licensed to conduct such business under the laws of the state, county and city in which Merchant is located.

Authorize.Net Service and Software License Agreement Area

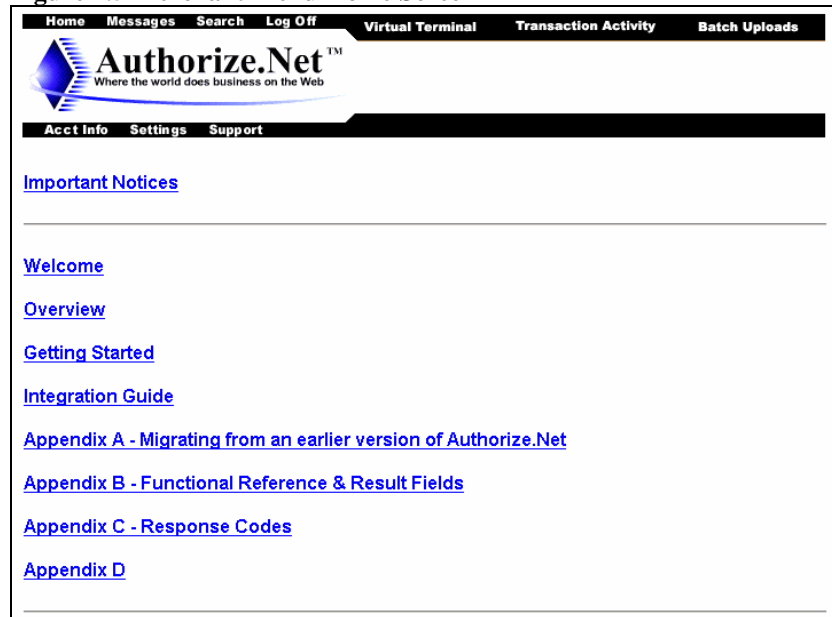
Upon completion of the interview, the **Authorize.Net Service and Software License Agreement** will be displayed. You *must* read this agreement, agree to be bound by all of its terms and conditions, and provide the social security number of the Principal/Corporate officer of your company as set up by the Reseller (for verification purposes

eCheck.Net Service Agreement Area

If you are configured to accept both credit card and eCheck.Net transactions, you will proceed to the online eCheck.Net application. Until your eCheck.Net application has been approved and your eCheck.Net ACH processing account has been activated by Authorize.Net, you will not be able to successfully process eCheck.Net transactions. The online eCheck.Net application requests basic information regarding your company and its anticipated use of the eCheck.Net service. Read the eCheck.Net Standard Terms and the eCheck.Net Operating Procedures carefully before printing and mailing a completed and signed eCheck.Net Application and Signature Card to Authorize.Net for consideration. Authorize.Net will notify you via e-mail of the results of your application to use the eCheck.Net service.

Warning: You will have one chance to print the online eCheck.Net Application and Signature Card, after which it will no longer appear. It is very important to print this application **the first time you log in.**

Figure 2.5 Merchant Menu Home Screen



The Merchant Menu Home Screen

The Merchant Menu home screen is the first screen displayed when you log in to the Merchant Menu (except for the first time, when you are prompted to read and agree to the terms of the Authorize.Net Service and Software License Agreement. See preceding paragraphs for information regarding that agreement.)

The black menu bars at the top of the screen remain constant while you navigate the Merchant Menu. You can access most features available in the Merchant Menu by clicking one of the choices embedded in the two black menu bars.

Chapter 3 Settings Area

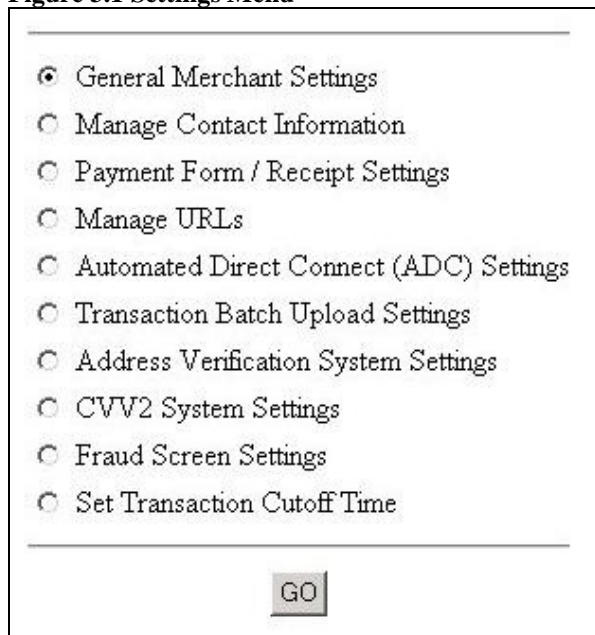
The Settings Area allows you to customize your Authorize.Net account. Features explained for the settings area include:

- Changing your account to and from **Test Mode**.
- Designating your **contact information** (including email, telephone number, etc.).
- Controlling which information is required for a **transaction** done through your website.
- Designating your **web site addresses** for interaction with the Authorize.Net payment processing network.

You can enter **Settings** by doing the following:

- Log in to your Merchant Menu at <https://secure.authorize.net/>.
- Click **Settings**.

Figure 3.1 Settings Menu



General Merchant Settings

Manage Contact Information

Payment Form / Receipt Settings

Manage URLs

Automated Direct Connect (ADC) Settings

Transaction Batch Upload Settings

Address Verification System Settings

CVV2 System Settings

Fraud Screen Settings

Set Transaction Cutoff Time

GO

General Merchant Settings

You may do the following in the General Merchant Settings:

- Put your account in test mode.
- Adjust the time zone for your account, as well as indicate if you observe Daylight Savings Time.
- View your Merchant Login ID.
- Change your password.
- Modify the response string version. (The response string is a set of data that includes the results of a given transaction. Data from the response string is seen in Batch Download Files and when using either ADC Relay Response or ADC Direct Response. Please consult your web developer before changing this value. For more information on the response string, please see Appendix B of the Developer's Guide.)

Figure 3.2 General Settings

General Settings	
Test Mode	<input checked="" type="checkbox"/>
Time Zone	Eastern Time ▾
Daylight Savings	<input checked="" type="checkbox"/>
<i>(Changing the Response String Version will change the ADC Responses and Batch Download file. Version 3.10 includes new CVV2 Response Code.)</i>	
Response String Version	3.00 ▾
Login Settings	
Login ID	testdrive
Current Password	<input type="text"/>
New Password	<input type="text"/>
Retype New Password	<input type="text"/>

To enter **General Merchant Settings**, do the following:

- Click **Settings**.
- Select **General Merchant Settings**.
- Click **Go**.

Test Mode

Test Mode allows you to test your linking integration with Authorize.Net, without having to process real credit card transactions. This is especially helpful if you or your web developer are still integrating your website with Authorize.Net.

Putting Your Account in Test Mode

To put your account in Test Mode, do the following:

- Click **Test Mode**.
- To save the changes, scroll down to the bottom of the page and click **Submit**.

Note: You must log in to the Merchant Menu and execute the Authorize.Net Service and Software License Agreement to process test transactions. When you process **test** transactions, no transactions are passed to the payment processor; thus, no information about test transactions is stored on Authorize.Net payment servers. When in test mode, properly formatted transactions will show as approved, but will not actually be processed or recorded (for details regarding test mode transactions, consult our Developer's Guide).

Time Zone

To designate your **Time Zone**, do the following:

- Click the **Time Zone** drop-down box.
- Select the time zone in which you live.
- To save the changes, scroll down to the bottom of the page and click **Submit**.

Login ID and Password

You can view your Login ID at the top of the **Login Settings** portion of this page.

Changing Your Password

We strongly recommend that when you change your password, you make it an alphanumeric value at least seven digits in length. You may change your password by doing the following:

- Type your current password in the box labeled **Current Password**.
- Type your new password in the box labeled **New Password**.
- Retype in your new password in the box labeled **Retype New Password**.
- To save the changes, scroll down to the bottom of the page and click **Submit**.

Note: Unlike your password, your Merchant Login ID is **unchangeable**.

Tip: If you begin typing a password, but decide that you want to keep your current password or type in a different password, simply click **Cancel** and the changes will be canceled.

Warning: Because your password allows you to log into your Merchant Menu, customize your account, and most importantly, process transactions, **you must exercise extreme caution in sharing your password with others**.

Manage Contact Information

You may customize your account so that Authorize.Net sends email confirmation about successful transactions, daily settlement reports, and other important information. In **Manage Contact Information**, you may do the following:

- Add a contact to your List of Contacts.
- Designate which emails a contact will receive.
- Designate one of the contacts as the reply-to address that will appear on your customers' Authorize.Net email receipts.
- Edit an existing contact.
- Delete a contact.

Figure 3.3 Example Manage Contact Information Screen

The following are the contacts that are currently specified on your account. You may add a contact by pressing the "Add Contact" button or you may edit or delete a contact by selecting the contact and pressing the appropriate button.

Name	E-Mail	Customer Receipt ReplyTo Address	Select
Joe Merchant	joe@merchant.com	x	⊙

To enter **Manage Contact Information**, do the following:

- Click **Settings**.
- Select **Manage Contact Information**.
- Click **Go**.

Figure 3.4 Example Add Contact Screen

Contact Information

Personal Name

Title

Phone, Ext. ,

E-Mail Address

E-Mails To Send This Contact

- Transaction Receipt
- Batch-Uploaded Transaction Receipt
- Uploaded Batch File Summary Report
- Credit Card Settlement Report
- eCheck Settlement Report
- Developer Announcements
- Administrative Notices
- Newsletter

Make this E-Mail the Customer Receipt ReplyTo Address

Adding a Contact

To **Add** a contact, do the following:

- Click **Add Contact**.
- Fill out the following:
 - Personal Name
 - Title
 - Phone and Extension
 - Email Address
- Click the box next to any email that you would like this contact to receive.
- If you would like the customer to see this contact's email address on their receipt, click the box **Make this Email the Customer Receipt Reply-To Address**.
- Click **Submit Contact** to save the changes.

Note: Only *one* email address can be designated as the reply-to address for the customer receipt email.

Tip: If you decide you do not want to make those changes, click **Cancel** and the Manage Contact Information page will appear, canceling the changes.

Figure 3.5 Example Edit Contact Screen

The screenshot shows a web form titled "Contact Information". It contains the following fields and options:

- Personal Name:
- Title:
- Phone, Ext:
- E-Mail Address:
- E-Mails To Send This Contact: Transaction Receipt, Batch-Uploaded Transaction Receipt, Uploaded Batch File Summary Report, Credit Card Settlement Report, e-Check Settlement Report, Developer Announcements, Administrative Notices, Newsletter
- Make this E-Mail the Customer Receipt Reply-To Address:
- Buttons:

Editing a Contact

To **Edit** a contact, do the following:

- Click under **Select** next to the contact that you would like to edit.
- Click **Edit Contact**.
- Change or add information as desired.
- Click **Submit** to save the changes.

Deleting a Contact

To **Delete** a contact, do the following:

- Click under **Select** next to the contact that you would like to delete.
- Click **Delete Contact**.
- The selected contact will automatically be deleted.

Warning: The contact will be irreversibly erased, so be certain that you would like to delete a contact before clicking **Delete Contact**.

Payment Form/Receipt Settings

The **Authorize.Net Secure Payment Form** is a secure form located on the Authorize.Net secure site, and is available to Merchants as part of the standard Authorize.Net service. If a Merchant needs a secure site for processing transactions through its web site, this form may be used to submit information for a transaction.

The **Authorize.Net Receipt Page** is displayed to the customer after a successful transaction. On this page, there can be a link to a site of your choosing. The **Authorize.Net Email Receipt** can be sent to a customer following a successful transaction.

The **Payment Form/Receipt Settings** allow you to control the appearance of your payment form and receipt page, designate required information for a transaction, and designate whether, and in what manner, a customer returns to your website after a transaction.

Figure 3.6 Payment Form/Receipt Settings Menu

General Payment Form / Receipt Settings
 Payment Form / Weblink Field Settings
 Virtual Terminal Field Settings

GO

To enter **Payment Form/Receipt Settings**, do the following:

- Click **Settings**.
- Select **Payment Form/Receipt Settings**.
- Click **Go**.

Figure 3.7 Changing Receipt/Payment Form Text, Link, or Background Colors

Color Settings

(to enter a HEX value, choose "HEX Color Code" from the drop down list)

Text Color or hexadecimal

Link Color or hexadecimal

Background Color or hexadecimal

Changing Colors for Receipt Text, Link, or Background

To change the **Text**, **Link** or **Background Color** settings for your payment form and/or receipt page, do the following:

- Select **General Payment Form/Receipt Settings**.
- Click **Go**.
- Click the arrow next to the boxes for the **Text Color**, **Link Color**, or **Background Color**.
- Select the desired color **or** select **Hex Color Code** to enter the hexadecimal value for another color.
- If you have selected **Hex Color Code**, enter the hexadecimal code in the adjacent box.
- Scroll down to the bottom of the page and click **Submit**.

Adding a Header to the Payment Form

To add a **Header** to your Payment Form, do the following:

- Select **General Payment Form/Receipt Settings**.
- Click **Go**.
- Click the box labeled **Payment Form Header**.
- Enter the desired text (either plain text or HTML).
- Scroll down to the bottom of the page and click **Submit**.

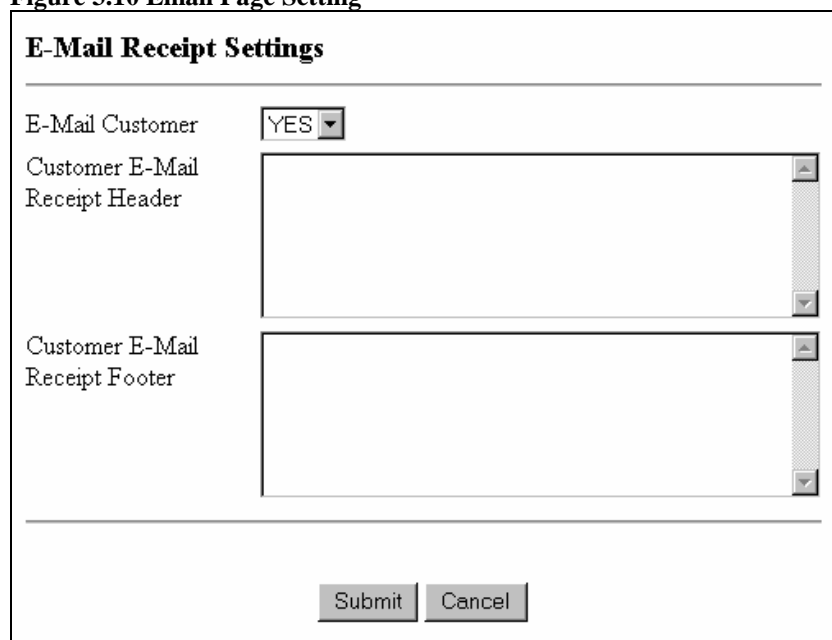
Changing the Receipt Page Settings

To change your **Receipt Page Settings**, do the following:

- Click **Receipt Link Method** and select **Link, Get, or Post**
- Click the box labeled **Receipt Link Text** and type the desired message.
- Click the box labeled **Receipt Page Header** and type the desired header (255 characters or less allowed in each header/footer).
- Click the box labeled **Receipt Page Footer** and type the desired footer.
- Scroll down to the bottom of the page and click **Submit**.

Note: The **Link** method simply links the customer to the designated address (for more information on how to designate your **Receipt Link URL**, see **Manage URLs** in this chapter). The **POST** and **GET** methods cause Authorize.Net to send information from the transaction in an HTTP form post to your designated URL. If you have any questions regarding these types of links, consult your webmaster. The vast majority of Merchants using the Authorize.Net receipt page will use **Link**.

Figure 3.10 Email Page Setting



The screenshot shows a web form titled "E-Mail Receipt Settings". It contains the following elements:

- A label "E-Mail Customer" followed by a dropdown menu currently set to "YES".
- A label "Customer E-Mail Receipt Header" followed by a large text input area with a vertical scrollbar on the right.
- A label "Customer E-Mail Receipt Footer" followed by another large text input area with a vertical scrollbar on the right.
- At the bottom of the form, there are two buttons: "Submit" and "Cancel".

Changing Email Receipt Settings

To change your **Email Receipt Settings**, do the following:

- To designate whether or not a customer receives an Authorize.Net-generated email receipt for their transaction, click **Email Customer** and select either **Yes** or **No**.
- Click the box labeled **Customer Email Receipt Header** and type the desired header for your Authorize.Net customer email (255 characters or less allowed in each header or footer).

- Click the box labeled **Customer Email Receipt Footer** and type the desired footer for your Authorize.Net customer email.
- Scroll down to the bottom of the page and click **Submit**.

Controlling the Information on your Payment Form

Within the **Settings** area, you may decide and designate which fields of information you would like to be required for a transaction to be processed through your web site. For example, you could designate the customer address as a required field. If a customer doesn't enter information in that field, submission of a transaction would cause an error indicating which field(s) was not provided. Likewise, you could choose to include certain fields of information while excluding others (e.g. designating customer address as required while excluding the customer's company name).

Figure 3.11 Example Payment Form Field Settings

Description	Viewable	Editable	Required
Invoice #	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Description	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer ID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customer First Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Last Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Company	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer City	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer State	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Zip	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Country	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Fax	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer E-Mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping First Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Last Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Company	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping City	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping State	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Zip	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Country	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Level 2 Tax	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 Duty	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 Freight	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 Tax Exempt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 PO Number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Currency Code	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recurring Billing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CVV2 Code	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Selecting Information Fields for your Payment Form

You may control whether or not a field is viewable, editable, and/or required in the **Payment Form** by doing the following:

- Select **Payment Form/Weblink Field Settings**.
- Click **Go**.
- Select those fields that you would like to be viewable, editable, and/or required.
- Deselect those fields that you would like to **not** be viewable, editable, and/or required.
- To keep the fields in their former state, click **Cancel**.
- To save the changes, scroll down to the bottom and click **Submit**.

Note: A field is designated as **viewable** if it can be viewed on the payment form. A field is designated as **editable** if it can be changed on the payment form. A field is designated as **required** if that field must be provided for a transaction to take place.

Figure 3.12 Example Virtual Terminal Field Settings

Virtual Terminal Field Settings			
Description	Viewable	Editable	Required
Invoice #	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Description	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Amount	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer First Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Last Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Company	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer City	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer State	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Zip	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Country	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Phone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer Fax	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Customer E-Mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping First Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Last Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Company	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Address	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping City	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping State	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Zip	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shipping Country	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Level 2 Tax	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 Duty	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 Freight	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 Tax Exempt	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Level 2 PO Number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Currency Code	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Recurring Billing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CVV2 Code	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Selecting Information Fields for Your Virtual Terminal

To control whether or not a field is viewable, editable, and/or required in the **Virtual Terminal**, do the following:

- Select **Virtual Terminal Field Settings**.
- Click **Go**.
- Select those fields that you would like to be viewable, editable, and/or required.
- Deselect those fields that you would like to not be viewable, editable, and/or required.
- To cancel the changes, click **Cancel**.
- To save the changes, scroll down to the bottom and click **Submit**.

Note: When customizing the field settings for your Virtual Terminal, you should always designate a field as viewable *and* editable if it is required. Likewise, you should always designate a field as *editable* if you would like it to be present on your Virtual Terminal Payment Form.

Manage URLs

The **Manage URLs** Section allows you to designate web addresses that are used in interaction with Authorize.Net. In these settings, you can add, edit, or delete the following URLs:

- Receipt Link Address
- Receipt Link Default URL
- Valid Referrer URLs
- ADC Relay Response Default URL
- Silent Post Default URL (only for merchants using Authorize.Net version 2.5)

Note: Each of these URLs will be defined and explained in the following paragraphs. Also, note that both HTTP (non-secure) as well as HTTPS (secure) URLs may be used.

Figure 3.13 Manage URLs Screen

The following are the URLs that are currently specified on your account.
 You may add a URL by pressing the "Add URL" button or you may edit or delete a URL by selecting the URL and pressing the appropriate button.

URL	Valid Browser Referrer URL	Valid ADC or Receipt Link URL	Receipt Link Default URL	ADC Relay Response Default URL	ADC Silent Response Default URL	Select
http://www.authorizenet.com		x				⊗

To enter **Manage URLs**, do the following:

- Click **Settings**.
- Select **Manage URLs**.
- Click **Go**.

Receipt Link URL

Except with the ADC methods of interaction, a Receipt Link URL is the address for the site to which your customer goes from the receipt page. In other words, the customer will link from the secure payment form to the receipt page and finally to the site designated by the Receipt Link URL. The address that Authorize.Net will normally use for the receipt link URL is called the **Receipt Link Default URL**.

Note: Authorize.Net will use your Receipt Link Default URL for the receipt link unless otherwise specified in the HTML form sent during the transaction (for information regarding the HTML necessary to specify receipt links on a per-transaction basis, consult our Developer's Guide).

Figure 3.14 Add Receipt Link URL Screen

URL Information	
URL	<input type="text" value="http://www.merchant.com"/>
Add To List Of Valid Referrers	<input type="checkbox"/>
Add To List Of Valid ADC / Receipt Link URLs	<input type="checkbox"/>
Not A Default URL	<input type="radio"/>
Receipt Link Default URL	<input checked="" type="radio"/>
ADC Relay Response Default URL	<input type="radio"/>
ADC Silent Response Default URL	<input type="radio"/>
<input type="button" value="Submit URL"/> <input type="button" value="Cancel"/>	

Adding a Receipt Link URL

To add a **Receipt Link URL**, do the following:

- Click **Add URL**.
- Click the box labeled **URL** and type in the *exact* web address of the place you would like your customer to go to after they see the Authorize.Net receipt page.
- Click the box labeled **Add to List of Valid ADC/Receipt Link URLs**.
- Click **Receipt Link Default URL** if you would like this to be the URL that your customer automatically goes to from the Authorize.Net receipt page.
- Scroll down to the bottom and click **Submit**.

Valid Referrer URL

A Valid Referrer URL is any address from which your site processes its Authorize.Net transactions. In other words, if your customer links to Authorize.Net's Secure Payment Form from a certain page on your site, you could designate the URL *for that particular page* on your site as a Valid Referrer URL. Authorize.Net would check each transaction to see that it was coming from one of the Valid Referrer URLs. You may also designate the general website as a Valid Referrer URL, thus encompassing all URLs beginning with that prefix.

Note: This feature is for Weblink connection method only. Do not use Valid Referrer URL with ADC connections. (Note: When using the Valid Referrer URL feature with a shopping cart, please contact your shopping cart provider to verify that they are not using ADC to connect to Authorize.Net.)

Adding a Valid Referrer URL

To add a URL as **Valid Referrer URL**, do the following:

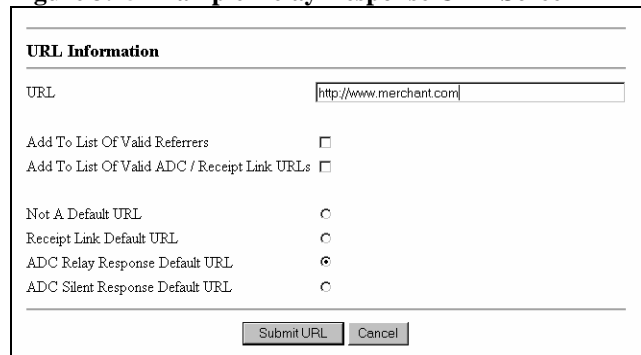
- Click **Add URL**.
- Click the box labeled **URL** and type in the *exact* web address of the Valid Referrer URL.
- Click the box labeled **Add to List of Valid Referrers**.
- Scroll down to the bottom of the page and click **Submit**.

Tip: Once you have added one or more Valid Referrer URLs to your settings, any transaction done from a URL *not* listed as a Valid Referrer URL will be **rejected**, so make sure that you have either all Valid Referrer URLs in your settings, or none.

ADC Relay Response URL

During a transaction done with the ADC Relay Response Method, Authorize.Net sends transaction response codes to the ADC Relay Response Default URL unless otherwise specified in the HTML form post (for more information on how to specify the ADC Relay Response URL in your HTML post on a per-transaction basis, or for information regarding the ADC methods of interaction, consult our Developer's Guide). This setting only pertains to those merchants using the ADC Relay Response Method.

Figure 3.15 Example Relay Response URL Screen



The screenshot shows a web form titled "URL Information". It contains a text input field for "URL" with the value "http://www.merchant.com". Below this are several options:

Add To List Of Valid Referrers	<input type="checkbox"/>
Add To List Of Valid ADC / Receipt Link URLs	<input type="checkbox"/>
Not A Default URL	<input type="radio"/>
Receipt Link Default URL	<input type="radio"/>
ADC Relay Response Default URL	<input checked="" type="radio"/>
ADC Silent Response Default URL	<input type="radio"/>

At the bottom of the form are two buttons: "Submit URL" and "Cancel".

Adding a Relay Response URL

To add a URL as an ADC Relay Response URL, do the following:

- Click **Add URL**.
- Click the box labeled URL and type in the *exact* web address of the Relay Response URL.
- Click the box labeled **Add to List of Valid ADC/Receipt Link URLs**.
- Select **ADC Relay Response Default URL** if you would like this to be the URL to which response codes are automatically sent after a customer submits a transaction for processing.
- Scroll down to the bottom of the page and click **Submit**.

Silent Response Default URL

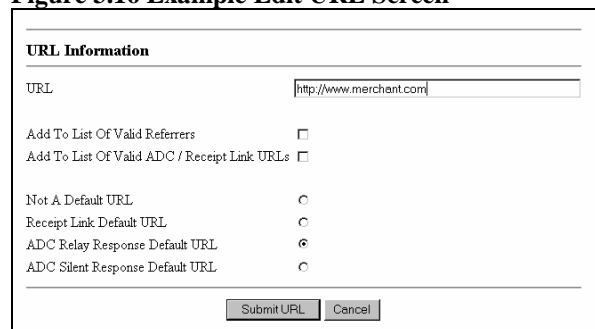
The Silent Response function is only available as a backwards compatibility tool for Merchants using Authorize.Net version 2.5, and should not be used by Merchants using Authorize.Net 3.0 or higher.

Edit URL

Some of the reasons you may need to edit your URLs in the settings include:

- You have adjusted the location of your pages.
- You would like to switch methods of interaction (e.g. switch from WebLink to ADC Relay Response).
- You would like to have a different Receipt Link Default URL.

Figure 3.16 Example Edit URL Screen



The screenshot shows a form titled "URL Information". It contains a text input field for the URL with the value "http://www.merchant.com". Below this are several checkboxes and radio buttons for configuration options:

Option	Control
Add To List Of Valid Referrers	<input type="checkbox"/>
Add To List Of Valid ADC / Receipt Link URLs	<input type="checkbox"/>
Not A Default URL	<input type="radio"/>
Receipt Link Default URL	<input type="radio"/>
ADC Relay Response Default URL	<input checked="" type="radio"/>
ADC Silent Response Default URL	<input type="radio"/>

At the bottom of the form are two buttons: "Submit URL" and "Cancel".

Editing a URL

To **edit** one of the URLs already provided in your settings, do the following:

- Select the URL that you would like to edit.
- Click **Edit URL**.
- Make desired changes.
- To cancel changes made to the URL, click **Cancel**.
- To save the changes, scroll down to the bottom of the page and click **Submit**.

Deleting a URL

To **delete** a URL, do the following:

- Select the URL that you would like to delete.
- Click **Delete URL**.

Warning: The URL will be irreversibly erased from your settings, so be certain that you would like to delete a URL before clicking **Delete URL**.

Automated Direct Connect (ADC) Settings

If your site uses the ADC Methods of interaction in processing transactions with Authorize.Net, you can use the **Automated Direct Connect (ADC) Settings** to customize the format for sending and receiving information. In this section, you can also enter your ADC Secret for use with the MD5 Hash field (consult our Developer's Guide for more information regarding the ADC methods).

Figure 3.17 Example ADC Settings Page

ADC Direct Response Settings

Delimited Response or

Default Field Separator or

Default Field Encapsulation Character or

General ADC Settings

(The ADC Secret is the private key used in the creation of the MD5 Hash field included in all ADC responses)

Current Secret (case-sensitive)

New Secret (case-sensitive)

Retype New Secret

Related Settings

(Only set "Require Password" to "YES" if ALL TRANSACTIONS are to be submitted via ADC Direct Response and/or Virtual Terminal and/or Batch Uploads)

Require Password for ALL Transactions

To enter **Automated Direct Connect (ADC) Settings**, do the following:

- Select **Automated Direct Connect (ADC) Settings**.
- Click **Go**.

Customizing the ADC Direct Response Settings

To customize your ADC Direct Response Settings, do the following:

- To specify whether or not you would like a delimited response, click **Delimited Response** and select either **YES** or **NO**.
- Click **Default Field Separator** and select your desired separator.
- Click **Default Field Encapsulation Character** and select either the desired encapsulation character or select **None** if you would like to send and receive your responses without an encapsulation character.
- If desired, you can change your ADC Secret (only necessary if using the MD5 Hash field) by entering your current ADC Secret, then providing your New Secret and providing it again in **Retype New Secret**.
- To cancel the changes made, click **Cancel**.
- To save the changes, scroll down to the bottom of the page and click **Submit**.

Note: The MD5 Hash field is part of an extra security feature available when using the ADC methods for transaction processing. The use of this feature is not mandatory, and using your payment processing system without it will **not** negatively affect the security of your transaction processing.

Password-Required Mode

The Password-Required mode is a great security feature for any Merchant who uses the ADC Direct Response method and/or Virtual Terminal exclusively. When an account is designated as Password Required, no transaction can be processed without initially providing the password. This mode prevents transactions from being done with only the login ID.

Password-Required Mode is available to the following types of Merchants:

1. Merchants who use *only* ADC Direct Response; that is, they securely transmit their passwords over an SSL connection during interaction with Authorize.Net. Other forms of interaction with the Authorize.Net Payment Gateway, such as the WebLink and Relay Response methods, should not be used with the Password-Required Mode.
2. Merchants who use *only* the Virtual Terminal (When using the Virtual Terminal, the Merchant provides their login ID and password to access their Merchant Menu. Therefore, the Virtual Terminal can still be used when an account is designated as Password Required.)
3. Merchants who use both Direct Response *and* Virtual Terminal.

The use of the password is safe with ADC Direct Response because all interactions with Authorize.Net are done over an SSL connection. When in Password-Required mode, the following form field must be provided with the usual transaction fields:

```
<INPUT TYPE="HIDDEN" NAME="x_PASSWORD" VALUE="Your Password Here">
```

Turning on Password-Required Mode

Authorize.Net strongly recommends that each Merchant who meets the above requirements implement this security feature. Any Merchant may designate their account as Password Required by doing the following:

- Click on **Settings**.
- Select **Automated Direct Connect (ADC) Settings**.
- Under Related Settings, Set Require Password for ALL Transactions to **YES**.

Transaction Batch Upload Settings

A batch upload is a delimited file used to send multiple transactions to Authorize.Net for automatic processing. You can use this function for submitting multiple transactions without having to submit each transaction individually. You can use the Transaction Batch Upload Settings to designate the format in which you are sending your batch upload files. (Consult our Developer’s Guide for more details on how to configure a batch upload file).

Figure 3.18 Example Transaction Batch Upload Settings Page

Transaction Batch Upload Settings

E-Mail Customer

Apply AVS Filter

Apply CVV2 Filter

Default Field Separator or

Default Field Encapsulation Character or

Field Inclusion And Order Settings

Field Description	Order
Invoice #	<input type="text" value="1"/>
Description	<input type="text" value="2"/>
Amount	<input type="text" value="3"/>
Payment Method (Credit Card or eCheck)	<input type="text" value="4"/>
Transaction Type	<input type="text" value="Exclude"/>
Authorization Code	<input type="text" value="Exclude"/>
Transaction ID	<input type="text" value="Exclude"/>
Credit Card Number	<input type="text" value="5"/>
Credit Card Expiration Date	<input type="text" value="6"/>
Bank Account Number	<input type="text" value="Exclude"/>
Bank Account Type	<input type="text" value="Exclude"/>
Bank ABA Routing Code	<input type="text" value="Exclude"/>
Bank Name	<input type="text" value="Exclude"/>

To enter **Transaction Batch Upload Settings**, do the following:

- Click on **Settings**.
- Select **Transaction Batch Upload Settings**.
- Click on **Go**.

Configuring Batch Upload Settings

To configure your **Batch Upload Settings**, do the following:

- To specify whether or not you would like your customer to receive an email notification for a transaction processed as part of a batch upload, click on the **E-Mail Customer** box and choose either **YES** or **NO**.
- Click on the **Default Field Separator** and select your desired separator.
- Click on the **Default Field Encapsulation Character** box and select your desired field encapsulation character.

Figure 3.19 Example Transaction Batch Upload Settings
Page cont'd

Customer ID	Exclude
Customer First Name	7
Customer Last Name	8
Customer Company	9
Customer Address	Exclude
Customer City	10
Customer State	11
Customer Zip	Exclude
Customer Country	12
Customer Phone	Exclude
Customer Fax	Exclude
Customer E-Mail	Exclude
Shipping First Name	Exclude
Shipping Last Name	Exclude
Shipping Company	Exclude
Shipping Address	Exclude
Shipping City	Exclude
Shipping State	Exclude
Shipping Zip	Exclude
Shipping Country	Exclude
Level 2 Tax	Exclude
Level 2 Duty	Exclude
Level 2 Freight	Exclude
Level 2 Tax Exempt	Exclude
Level 2 PO Number	Exclude
Currency Code	Exclude
Recurring Billing	Exclude
CVV2 Code	Exclude

Designating Field Order for Batch Upload File

To customize the order of information in which your batch upload file is sent, do the following:

- From the list of field types, click the field that you would like to send first.
- Select the number **1** from the drop-down box.
- Click your second field and select the number **2**.
- Continue this process until you have all fields in the desired order.
- Click any fields that you are not going to include, designating each as **Exclude**.
- To save changes, scroll down to the bottom of the page and click **Submit**.

Note: Transaction ID must be included when uploading a batch containing credits.

Note: More information on how to upload a batch is located in **Chapter 5 Transaction Activity and Batch Uploads**.

Address Verification System (AVS) Filter

(Please read the section on AVS Filter Risks below before making any changes to AVS Filter settings.)

Purpose of the AVS System

Bankcard processors provide the Address Verification System to aid in the detection of fraud. In the Internet context, customers fill out an online payment form on the Merchant's website with their credit card information including the card billing address. The processing network (e.g., FDC, Vital, Nova, GPS, Paymentech) compares the billing address supplied online with the billing address on file at the credit card issuing bank. From this comparison, the processing network sends an AVS response code to Authorize.Net.

Authorize.Net takes the AVS response code from the processing network and reports it to the Merchant. Depending upon the response, the Merchant may wish to approve the transaction, reject the transaction, or follow other lines of logic. With so many possible reasons as to why an address and zip code may not match, a Merchant is not required to refuse a transaction because the AVS response is a mismatch. With most banks and Merchant Service Providers, use of the AVS system is required in order to avoid non-qualified transaction surcharges (typically an additional 1%). There are two main reasons for voiding transactions that have an AVS mismatch:

- (1) Accepting a transaction involving an AVS mismatch response may or may not cause a non-qualified transaction surcharge according to your Merchant agreement with your bank or Merchant Service Provider.
- (2) The AVS mismatch may indicate fraud.

Note: Failure to activate required AVS data fields in the **Settings** area may result in "downgrading" of transactions causing an increase in the discount rate for those transactions.

AVS Response Code Explanations

The following is a list of possible AVS response codes, and their corresponding meanings. Each code is unique; no AVS response code will ever overlap another in meaning.

AVS Response Codes and Meanings:

- A = Address (Street) matches, ZIP does not
- B = Address information not provided for AVS check
- E = AVS error
- G = Non U.S. Card Issuing 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

A = Address (Street) matches, ZIP does not

This response code signifies a perfect match between the street address entered by the customer and the billing address on file with the card-issuing bank, and a mismatch between zip codes.

B = Address information not provided for AVS check

This response code signifies that the transaction was submitted to Authorize.Net without address information, so the AVS check could not be performed.

E = AVS error

This response code signifies that an error occurred on the processing network while processing the AVS request, so AVS information is not available for this transaction.

G = Non U.S. Card Issuing Bank

The credit card issuing bank is of non-U.S. origin, and does not support the AVS system.

N = No Match on Address (Street) or ZIP

Neither the street address nor the zip code provided by the customer matches the billing address and zip code on file with the card-issuing bank.

P = AVS not applicable for this transaction

This response code is returned when address information is not checked against the AVS system. Examples of this would be eCheck.Net transactions, credits, voids, prior auth capture transactions, capture only transactions, declines, and other transactions that do not involve address checking.

R = Retry – System unavailable or timed out

AVS was unavailable on the processing network, or the processor did not respond.

S = Service not supported by issuer

The issuing bank does not support AVS.

U = Address information is unavailable

Address information is not available for the customer's credit card at the processor.

W = 9 digit ZIP matches, Address (Street) does not

The nine-digit zip code provided matches the billing zip code on file with the issuing bank, and the street address provided does not match.

X = Address (Street) and 9 digit ZIP match

The nine-digit zip code and street address provided match the billing address on file with the issuing bank.

Y = Address (Street) and 5 digit ZIP match

The five-digit zip code and street address provided match the billing address on file with the issuing bank.

Z = 5 digit ZIP matches, Address (Street) does not

The five-digit zip code provided matches the billing zip code on file with the issuing bank, and the street address provided does not match.

AVS Filter Risks

It is important to note that when the AVS filter declines a transaction as the result of an AVS mismatch, the transaction is voided, but the authorization remains. **The preauthorized amount**

reserved against the credit limit of the customer's card will remain for a predefined period of time until it is expired by the card issuer. (See your Merchant Service Provider for the exact length of this period.) For example, if a customer repeatedly enters an incorrect zip code, and you have chosen to decline all zip code mismatches, the preauthorized amounts may sum up to reach or exceed the credit card's credit limit.

Even though the customer has not actually made a purchase with his credit card, future transactions will be declined regardless of the AVS response because the credit limit has been reached. Merchants should be aware that normal transaction fees apply for all resubmitted transactions.

Default AVS Filter Settings

Authorize.Net has initiated standard default AVS settings to your account in order to better protect you against fraud. The default settings will be set to reject all transactions as described below.

Defaulted to Reject:

B = Address information not provided for AVS check

E = AVS error

G = Non U.S. Card Issuing Bank

N = No Match on Address (Street) or ZIP

R = Retry - System unavailable or timed out

S = Service not supported by issuer

U = Address information is unavailable

This means that all transactions will require a street address and/or zip code match to be approved. Any transaction that receives an AVS response code as listed above will result in a decline. If you wish to allow transactions that receive any of these AVS responses to be approved, you will need to manually uncheck the boxes next to the desired code in the Address Verification System Settings area. This is a very important consideration if you are performing recurring billing and do not include address and zip code data with transactions. See below for specific instructions on how you can make this change.

Figure 3.20 Example AVS Interface

Address Verification System Settings		
AVS Code	Description	Reject Transaction
A	Street Address: Match -- First 5 Digits of Zip: No Match	<input type="checkbox"/>
B	Address Information Not Provided for AVS Check	<input type="checkbox"/>
E	AVS Error	<input type="checkbox"/>
G	Non U.S. Card Issuing Bank	<input type="checkbox"/>
N	Street Address: No Match -- First 5 Digits of Zip: No Match	<input type="checkbox"/>
R	Retry, System Is Unavailable	<input type="checkbox"/>
S	AVS Not Supported by Card Issuing Bank	<input type="checkbox"/>
U	Address Information For This Cardholder Is Unavailable	<input type="checkbox"/>
W	Street Address: No Match -- All 9 Digits of Zip: Match	<input type="checkbox"/>
X	Street Address: Match -- All 9 Digits of Zip: Match	<input type="checkbox"/>
Y	Street Address: Match -- First 5 Digits of Zip: Match	<input type="checkbox"/>
Z	Street Address: No Match -- First 5 Digits of Zip: Match	<input type="checkbox"/>

*Note: To apply these settings to batch uploaded transactions, go to the "Transaction Batch Upload Settings" area and set the "Apply AVS Filter" setting to "YES".

AVS Interface

To access the AVS filter interface, do the following:

- Click the **Settings** button.
- Click **Address Verification System Settings**.
- Click **Go**.

Setting AVS functionality

To select the AVS filters you wish to apply to transactions:

- Select the AVS response codes you would like to automatically reject. Click **Submit**.

FraudScreen.Net

The FraudScreen.Net functionality enables Merchants who have enrolled in the FraudScreen.Net service to set a rejection threshold for transactions based on a real-time score returned from the Authorize.Net fraud-screening engine. Authorize.Net utilizes the eFalcon technology from HNC, the industry leader in transaction fraud scoring. HNC's technology utilizes dozens of online, offline, and positive and negative databases to score each transaction (0 - 1000) for the probability of fraud. The FraudScreen.Net service is particularly appealing to Merchants with:

- High average ticket items
- High cost of goods sold
- Concerns about Merchant credit worthiness associated with high charge back occurrence.

If you are interested in using the FraudScreen.Net service, please see [Chapter 7](#) for information on how to contact Authorize.Net. A link to the documentation and application for the FraudScreen.Net Service is also available on the main page of the Merchant Interface. Click here to login:

<https://merchant.authorize.net/>.

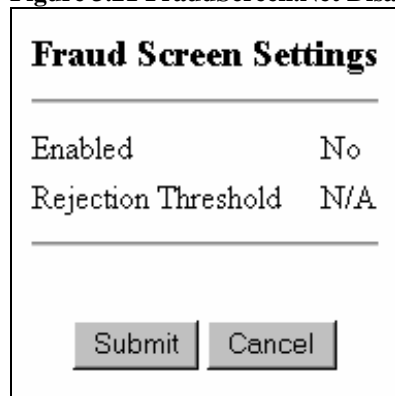
Using the FraudScreen.Net Service

To access the FraudScreen.Net settings, do the following:

- Click the **Settings** button.
- Select **Fraud Screen Settings**.
- Click **Go**.

Before the FraudScreen.Net service has been enabled, the settings screen looks like this:

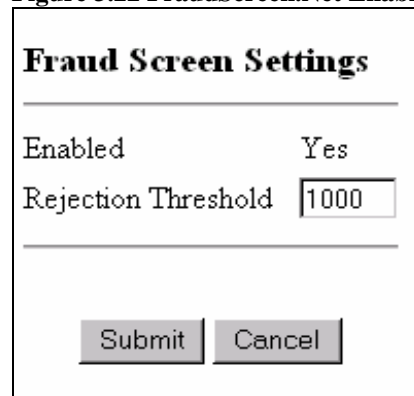
Figure 3.21 FraudScreen.Net Disabled Screen



The screenshot shows a form titled "Fraud Screen Settings". It contains two rows of text: "Enabled" with "No" to its right, and "Rejection Threshold" with "N/A" to its right. At the bottom of the form are two buttons: "Submit" and "Cancel".

After the FraudScreen.Net service has been enabled, the settings screen looks like this:

Figure 3.22 FraudScreen.Net Enabled Screen



The screenshot shows a form titled "Fraud Screen Settings". It contains two rows of text: "Enabled" with "Yes" to its right, and "Rejection Threshold" with a text input field containing "1000" to its right. At the bottom of the form are two buttons: "Submit" and "Cancel".

Managing Transactions Using the Fraud Score

The fraud score is a measure of the probability that a particular transaction is fraudulent. A larger fraud score indicates a greater probability that the transaction is fraudulent. A fraud score is based upon the transaction information along with other factors related to the Merchant, Merchant's industry, and cardholder.

FraudScreen.Net is designed to detect fraudulent transactions in real time. It uses powerful statistical models that enable it to identify the majority of the fraudulent transactions as they occur. Because FraudScreen.Net is a statistical product, however, it cannot be expected to detect all frauds. You should exercise caution before setting a rejection threshold for your account.

A typical approach to using the FraudScreen.Net score is to use two thresholds. The first threshold is set through the Merchant Menu Interface (see Using the FraudScreen.Net Service above) by the Merchant. Transactions that score above the first threshold are automatically rejected. These transactions have an extremely high likelihood of fraud, so this threshold should be set at a very high score (depending on the type of goods sold).

The second threshold is not set through an interface, but rather is a level the Merchant determines while reviewing fraud scores of transactions in the current batch. Transactions that score above the second threshold are reviewed manually. Upon manual review, the Merchant may decide to void a transaction or allow it to be captured. Typically, this second threshold is somewhere between 500 and 800. Over time, the Merchant will learn what the best second threshold is for their business.

Sample Rules Using the Cutoff Score

The following is an example of how the first and second fraud thresholds function (as described above). If, in the Merchant Menu, the Merchant chooses to set 900 as their first rejection score threshold, then all transactions scoring greater than 900 will be declined automatically by FraudScreen.Net. If the Merchant wishes to manually review transactions scoring between 500 and 900, then 500 would be considered the *second* threshold. All transactions scoring greater than 500 but less than 900 would be left in the current batch until the Merchant has satisfactorily performed a manual review (manual fraud analysis). After reviewing these transactions, the Merchant may choose to do one of the following: first, in the case that the transaction is found to be “good”, the Merchant may allow it to be captured and processed; second, in the case that the transaction is found to be suspicious of fraud, the Merchant may choose to void it. All transactions scoring less than 500 would be approved by FraudScreen.Net and processed as legitimate transactions.

Optimizing Fraud Detection

With any fraud detection system that ranks transactions by risk, the optimal strategy is to investigate the riskiest transactions (those with the highest fraud score) first. This will maximize the number of frauds caught per customer contacted. Investigation should proceed down the list through successively less risky transactions, and continue until the incremental cost of detecting the next fraud outweighs the expected fraud savings. The optimal threshold varies depending upon the investigation cost, the marginal cost of the goods, and expected fraud savings. Each distinct type of Merchant will have a different optimal threshold. Note that, when you are evaluating risk, you should also take into account the amount of money at risk. In other words, Merchants selling high-priced items with high resale potential (e.g., jewelry, electronics), will want to be more careful than those selling lower-priced items not typically resold (e.g., books, t-shirts).

For much of its detection capability, FraudScreen.Net relies upon usage profiles that track the historical use of card numbers, e-mail addresses, and other data in the order. When a transaction is sent, these profiles are updated, even if the information in the transaction is phony. Since the score is highly dependent upon the usage profiles, “testing” the system with bogus transactions can compromise the future performance of the system. We strongly encourage you to not “test” the system by sending fake transactions.

Note: The rejection threshold will affect *all* transactions processed through your account including batch uploads.

Important: Transactions that are declined due to a fraud score that exceeds the rejection threshold will *not* appear in the current or past batches viewable from the Merchant Menu. In order to see the

transactions rejected by FraudScreen.Net, you must download the batch following the steps outlined in Chapter 5. FraudScreen.Net rejected transactions will not include a fraud score, but will have a response code of 3, and a reason code of 41. (For more information on what these codes mean, consult the Integration Guide available from the Developer's Guide within the Merchant Menu.)

CVV2 and CVC2 Settings

What is CVV2 or CVC2?

The CVV2/CVC2 is a three-digit security code that is printed on the back of credit cards. The value appears in reverse italic at the top of the signature panel. The additional numbers provide an extra measure of security against credit card fraud. Would-be fraudsters must be capable of providing both the credit card number as well as the card validation value in order to successfully complete a transaction. All MasterCard cards, both credit and debit, were required to contain CVC2 (Card Validation Code 2) by January 1, 1997 and all Visa cards were required to contain CVV2 (Card Verification Value 2) by January 1, 2001. For simplicity, we will refer to CVV2/CVC2 as CVV2.

How does CVV2 work?

Merchants may request the CVV2 value from the customer when processing a card-not-present transaction. The cardholder reads this code directly from the back of the credit card and enters it in the appropriate field. Authorize.Net then verifies the CVV2 value during the authorization process and relays the decline/approval results. By using the CVV2 program along with the Address Verification Service (AVS), Merchants are able to make a more informed decision about whether to accept a particular credit card transaction.

Where is the CVV2 located on a credit card?

The CVV2 three-digit value is printed on the signature panel on the back of credit cards immediately following the Visa or MasterCard account number. Previously, the three-digit CVV2 value followed the 16-digit account number. In newer cards, the 16-digit account number is truncated to the last four digits on the signature panel.

How do I use CVV2 with Authorize.Net?

The CVV2 security program is a free service available to all Authorize.Net Merchants. You may customize your account so that Authorize.Net rejects transactions where the CVV2 code provided by the cardholder is invalid. Within the CVV2 Settings area, you may choose to reject transactions that have any one of the following responses:

- No match
- Not Processed
- Should be on card but not so indicated
- Issuer Not Certified and/or has not provided encryption key

You may control whether or not a particular transaction is declined based on the CVV2 response by doing the following:

- Select **CVV2 Settings**.
- Click **Go**.
- Select the CVV2 response codes that you would like to be rejected.
- To save the changes, click **Submit**.

Figure 3.23 CVV2 Settings Screen

CVV2 System Settings		
CVV2 Resp Code	Description	Reject Transaction
N	No Match	<input type="checkbox"/>
P	Not Processed	<input type="checkbox"/>
S	Should be on card but not so indicated	<input type="checkbox"/>
U	Issuer Not Certified and/or has not provided encryption key	<input type="checkbox"/>

*Note: To apply these settings to batch uploaded transactions, go to the "Transaction Batch Upload Settings" area and set the "Apply CVV2 Filter" setting to "YES".

Note: Transactions with a valid CVV2 code will return a response that indicates a match and will be processed through the system as normal. Transactions with invalid CVV2 codes will only be rejected if you select the corresponding box in the CVV2 Settings area.

Caution: The FDC and Paymentech processors will ignore CVV2 and AVS fields if a transaction is flagged as a recurring billing. Because the CVV2 field is ignored, the CVV2 response code returned is "Not Processed." If the Merchant has turned on the AVS or CVV2 filter for "Not Processed" responses, the Authorize.Net system will reject the transaction.

How do I get the CVV2 field to show up on my payment form or in the Virtual Terminal?

To add the CVV2 security code field to your Virtual Terminal or payment form, you must select the fields as viewable from within the Virtual Terminal Field Settings and Payment Form / Weblink Field Settings areas. For more information, please see **Chapter 3: Controlling the Information on your Payment Form.**

Can I use CVV2 with transaction batch uploads?

Yes. For more information, please see **Chapter 3: Transaction Batch Upload Settings.**

Transaction Cutoff Time

What is Transaction Cutoff Time?

Transaction Cutoff Time is a feature that allows Merchants the opportunity to specify the time for a batch of transactions to be closed and sent to the processor. All transactions authorized and set to capture by the specified time will be included in the current batch for settlement. Previously, the transaction cutoff time was fixed at the system default of 6:00 PM EDT. With Transaction Cutoff Time, Merchants may now specify any time as the time at which the last transaction is picked up for settlement for a particular day. This flexibility provides Merchants the opportunity to simplify bookkeeping by specifying a batch closure time which best suits their business needs.

What else should I know about Transaction Cutoff Time?

Several key factors should be considered before modifying your transaction cutoff time, including:

- The transaction cutoff time will apply to all credit card and eCheck.Net transactions.
- If you choose to edit the transaction cutoff time after you have already settled a batch for the day, the new transaction cutoff time will apply to the next settlement day. (You may not settle twice in one day.)
- Transaction cutoff time is not the same as settlement time. Whereas Authorize.Net will send all transactions authorized (and set to capture) by the cutoff time to the processor for settlement, Authorize.Net cannot specify the time at which the transactions are actually settled by the processor. Given this consideration, it is possible that late transaction cutoff times may result in transactions settling during the next settlement day.
- You may specify any time as the transaction cutoff time; however, it is your responsibility to verify that the specified transaction cutoff time will correspond with the cutoff times of your acquiring bank and processor.
- For some window of time between the transaction cutoff time and the time the batch is actually picked up for settlement, you will see transactions in the current batch that will settle with the day's current batch as well as transactions that will not be sent for settlement until the next settlement day.
- Unless otherwise modified, the Authorize.Net system will close batches for settlement at the system default time of 6:00 PM EDT.

How do I set the Transaction Cutoff Time?

You may set the transaction cutoff time by doing the following:

- Select **Set Transaction Cutoff Time for Settlement**.
- Click **Go**.
- Read the system notice, and then click **Edit** to modify the cutoff time.
- Select the desired cutoff time using the drop down menus.
- Click **Submit** to save changes.

Chapter 4 Virtual Terminal

The Virtual Terminal is your online transaction terminal. From the Virtual Terminal, you can do the following:

- Process credit card charges and credits.
- Receive authorization for a transaction without capturing the funds (called Authorization-Only).
- Capture funds from a previously authorized transaction.
- Process eCheck.Net debits and credits (subject to approval: contact your Merchant Service Provider for details regarding configuration and approval for eCheck.Net service).

To enter the **Virtual Terminal**, do the following:

- Log in to your Merchant Menu at <https://secure.authorize.net/>
- Click **Virtual Terminal**.

Figure 4.1 Example Virtual Terminal Screen

Order Information	
Transaction Type	<input checked="" type="radio"/> Charge A Credit Card / Debit A Checking Account <input type="radio"/> Credit Money Back To A Credit Card / Checking Account <input type="radio"/> Authorize An Amount / Do Not Capture Funds Yet <input type="radio"/> Capture Funds Only (requires Authorization Code) (Credit Card Only)
Invoice #	<input type="text"/>
Description	<input type="text"/>
Amount	<input type="text"/>
RefTransaction Id	<input type="text"/> (for Credit transactions)
Credit Card Information (if Payment Method is Credit Card)	
Accepted Cards	Visa MasterCard Amex Discover DinersClub EnRoute JCB
Card Number	<input type="text"/>
Exp. Date	<input type="text"/> (mm/yy)
CVV2 Code	<input type="text"/>
Authorization Code	<input type="text"/> (for Capture Only transactions)
Customer Billing Information	
First Name	<input type="text"/>
Last Name	<input type="text"/>
Zip Code	<input type="text"/>
E-Mail	<input type="text"/>
<input type="button" value="Submit Transaction"/> <input type="button" value="Clear Form"/>	

Processing Credit Card Transactions

To process a credit card transaction, do the following:

- From among the choices displayed in the category **Transaction Type**, select **Charge a Credit Card/Debit a Checking Account**.
- Provide customer information as shown on your Virtual Terminal Screen (please see this chapter's section **Payment Form/WebLink Field Settings** to find out how to designate which fields appear on your Virtual Terminal Payment Form).
- Provide customer credit card information, including the card number and the expiration date.
- To submit the transaction, scroll down to the bottom of the page and click **Submit**.

Notes: To process a normal transaction, you do **not** need to provide an authorization code. If you do not see a type of credit card and you would like to add that credit card capability, contact your Merchant Service Provider, who can enable certain types of credit cards for your Merchant Account. Once the MSP enables those types of credit cards on your Merchant Account, your Authorize.Net Reseller can add processing capability for those types of cards to your Authorize.Net account.

Processing eCheck.Net Transactions

eCheck.Net transactions differ from credit card transactions in that they are not processed in real time. Thus, an eCheck.Net transaction can only be submitted initially; the success of the transaction is not known until later.

To process a transaction using eCheck.Net, do the following:

- From among the choices displayed in the category **Transaction Type**, select **Charge a Credit Card/Debit a Checking Account**.
- Provide customer information as shown on your Virtual Terminal Screen.
- Provide **Checking Account** information, including the checking account number and the ABA routing number.
- To submit the transaction, scroll down to the bottom of the page and click **Submit**.

Note: The ABA routing number corresponds to your customer's bank, is listed on the customer's check, and is necessary for an eCheck.Net transaction to successfully take place. Please refer to the [eCheck.Net Operating Procedures](#) for more information regarding the eCheck.Net service.

Issuing Credits Using the Virtual Terminal

All credits issued through the Virtual Terminal must adhere to the following criteria. Credits can only be issued to a credit card used for a previous settled transaction where the credit card was charged for purchases through your Authorize.Net payment gateway account. You cannot issue credits against transactions that failed, were declined, or were submitted as Authorization-Only transactions. The sum total of the credits issued to a credit card cannot exceed the amount of the transaction originally charged to that card. Credits are not processed in real time, but are submitted at settlement time with other transactions.

To issue a credit using your Virtual Terminal, do the following:

- Log in to your Authorize.Net Account.
- Click on Virtual Terminal located on the Menu Bar.
- From among the choices displayed in the category **Transaction Type**, select **Credit Money Back to a Credit Card/Checking Account**.
- Provide customer information as requested on the Virtual Terminal screen.
Note: When issuing a credit for a transaction, you must include the transaction ID assigned to the original transaction. Transaction ID's can be located by viewing the transaction details or by downloading the transaction. See chapter 5 for more information on viewing transaction details and downloading transactions.
- Provide the **Customer's Credit Card/Checking Account Information**.

Note: When a credit card number is viewed in transaction details, only the first four and last four digits of the credit card number are *not* masked. Only those numbers which are *not* masked must be included when issuing a credit through the Virtual Terminal.

- To submit the credit, scroll down to the bottom of the page and click **Submit**.

Note: eCheck.Net credits do not require an original transaction ID to be issued. Because of the risks involved with ACH (eCheck.Net) credits, extreme caution should be taken when issuing them (for more information regarding these risks, please consult the [eCheck.Net Operating Procedures](#)).

Processing Authorization-Only Transactions

Authorization-Only credit card transactions are those which are authorized by the payment processor but the funds of which are not immediately captured. If you use these types of transactions, you must later designate these authorizations for capture in order to finish the transaction.

To receive authorization for a credit card transaction without capturing the funds for the transaction, do the following:

- From among the choices displayed in the category **Transaction Type**, select **Authorize an Amount/Don't Capture Funds Yet**.
- Provide customer information as shown on your Virtual Terminal Screen (please see [Controlling the Information on your Payment Form](#) for more information on how to customize the fields present on your Virtual Terminal).
- Provide customer credit card information.
- To submit the transaction, scroll down to the bottom of the screen and click **Submit**.

Note: Authorization codes are valid for a limited time period. Transactions classified as Authorization-Only should not remain in the current batch for more than one week.

Submitting eCheck.Net Transactions without Capturing Funds

Note: Because eCheck.Net transactions are **not** processed in real time, immediate authorization for an eCheck.Net transaction is **not** possible. That is, unlike credit cards, which can be immediately authorized for a transaction, eCheck.Net transactions require a lengthier processing time. Thus, if you submit an eCheck.Net transaction using the Authorization-Only method, the transaction will remain in our payment processing database, but will not be submitted to the ACH network for processing.

The transactions can later be submitted by following the same process that is used to capture Authorization-Only credit card transactions processed using (see preceding section: Processing Authorization-Only Transactions. Also see Chapter 5 Transaction Activity: Selecting Authorization-Only Transactions for Capture).

Processing Capture-Only Transactions

You should use the Capture-Only method if you have received authorization for a credit card transaction from any source **other than** Authorize.Net. For example, if you received a voice authorization for a transaction, and want to capture the funds from that transaction, you could do this using the Capture-Only method. You must provide the authorization code in order to process a Capture-Only transaction.

Figure 4.2 Example Virtual Terminal Screen

The screenshot shows a web form with the following sections:

- Order Information:**
 - Transaction Type: Radio buttons for Charge A Credit Card / Debit A Checking Account (selected), Credit Money Back To A Credit Card / Checking Account, Authorize An Amount / Do Not Capture Funds Yet, and Capture Funds Only (requires Authorization Code) (Credit Card Only).
 - Invoice #: Text input field.
 - Description: Text input field.
 - Amount: Text input field.
- Credit Card Information (if Payment Method is Credit Card):**
 - Accepted Cards: Radio buttons for Visa, MasterCard, Amex, and Discover.
 - Card Number: Text input field.
 - Exp. Date: Text input field with a "(mm/yy)" placeholder.
- Customer Information:**
 - Buttons: "Submit Transaction" and "Clear Form".
 - Customer ID: Text input field.
 - First Name: Text input field.
 - Last Name: Text input field.
 - Company: Text input field.
 - Address: Text input field.
 - City: Text input field.
 - State/Province: Text input field.
 - Zip Code: Text input field.
 - Country: Text input field.
 - Phone: Text input field.
 - Fax: Text input field.
 - E-Mail: Text input field.
- Customer Shipping Information (if different from above):**
 - First Name: Text input field.
 - Last Name: Text input field.
 - Company: Text input field.
 - Address: Text input field.
 - City: Text input field.
 - State/Province: Text input field.
 - Zip Code: Text input field.
 - Country: Text input field.
- Bottom Buttons:** "Submit Transaction" and "Clear Form".

To process a transaction using the Capture-Only method, do the following:

- From among the choices displayed in the category **Transaction Type**, select **Capture Funds Only**.
- Provide customer information as shown on your Virtual Terminal Screen **including amount**.
- Provide customer credit card information, **including Authorization Code**.
- To submit the transaction, scroll down to the bottom of the screen and click **Submit**.

Partial Order Fulfillment*

Merchants may only settle and bill cardholders for the goods and services that will be shipped within a 48-hour period from the time the cardholder is charged. This may present a problem when a Merchant takes an order and obtains an authorization for the total order amount prior to checking inventory for availability. The transaction amount and the authorization amount must correspond for the transaction to clear at an incentive interchange rate (the Merchant’s stated base discount rate).

We recommend the use of an inventory management system that prevents overstating an initial authorization amount and encourage Merchant “best practices” that keep authorization and settlement transaction procedures in sync.

If circumstances require that a preliminary order be completed as two partial orders, then the original transaction should be voided and the partial orders authorized and settled for the correct amounts. The consumer’s spending limit may be tied up if a preliminary authorization request goes unfilled and subsequent authorizations are initiated, however, transactions will not clear at the incentive interchange rate if the authorized and settled amounts do not correspond. A sample transaction will be used here in order to illustrate the steps that must be taken in order to perform partial order fulfillment. In this example, a Merchant has taken an order for \$500, of which the Merchant only has \$300 available for delivery within the 48-hour period. Adherence to this procedure is important as it will eliminate unnecessary chargebacks from customers whose credit card statements reflect amounts that do not match received orders. To process a partial order, the Merchant should follow these guidelines:

- The original transaction must be voided (in the full amount: i.e., \$500) prior to settlement of the day’s batch. **Caution:** see note following this paragraph.
- After voiding the original transaction, a new transaction (Auth-Capture) must be processed via the Virtual Terminal in the amount of the order that the Merchant wishes to fulfill (i.e., the \$300 which is available for shipment).
- When the remainder of the order is available for fulfillment (i.e., the last \$200), an additional Auth-Capture transaction may be processed to complete the original order.

Note: The Merchant should be aware that although a transaction is voided, the fund authorization remains against the cardholder’s account. **The preauthorized amount reserved against the credit limit of the customer’s card will remain for a predefined period of time until it is expired by the card issuer—typically seven days.** For example, the original \$500 transaction authorized in the scenario above was voided and a new transaction in the amount of \$300 was processed. However, because the \$500 authorization remains on the cardholder’s credit card account, it is possible that the separate preauthorized amounts may exceed the credit card’s credit limit. Even though the customer did not actually make a \$500 purchase with his credit card, the \$300 purchase will be declined because the credit limit may have been reached.

*Merchants who process transactions via ADC Relay Response, ADC Direct Response, or Batch Uploads may process a Partial Capture in place of what is required for Partial Order Fulfillment. Partial Capture allows Merchants to capture an amount that is less than the original authorized amount without voiding the original transaction. The transaction will still be considered a prior-auth-capture but, provided the issuing bank supports Partial Captures, the Authorize.Net system will automatically reverse the uncaptured funds and notify the processor that a Partial Capture has taken place. Partial Captures are limited to Visa card transactions on the Vital and FDC networks and do not include multi-currency. These transactions must be processed through the system via ADC Relay Response, ADC Direct Response, or by way of a Batch Upload.

Chapter 5 Transaction Activity and Batch Uploads

The **Transaction Activity** and **Batch Uploads** areas of the Merchant Menu provide you with tools to effectively access and analyze your transaction information.

You can do the following in these areas of your Merchant Menu:

- **View transactions** and their details.
- **Void** a transaction that has not yet been settled.
- **View transactions** according to the **type** for a given batch.
- **Select** previously authorized transactions **for capture** (see **Chapter 4 Virtual Terminal: Processing Authorization-Only transactions**).
- **Download** transaction **details** for personal record keeping.
- **View** transaction **statistics**.
- **Upload** a batch.
- **View** the **status** of an uploaded batch.

Figure 5.1 Transaction Activity/Batch Uploads Screen

The screenshot shows a web interface with two main sections. The first section, titled "Settlement Batches:", contains a dropdown menu with "Current Batch" selected and a "GO" button. Below this are five radio button options: "View Transactions" (selected), "View Returned Items", "Download Transactions", "View Statistics", and "View Summary Statistics for all Batches". The second section, titled "Uploaded Transaction Batch Files:", contains a dropdown menu with "None Uploaded" selected and a "GO" button. Below this are two radio button options: "Status Check" (selected) and "Upload a batch of new transactions".

Transaction Activity

To enter **Transaction Activity**, do the following:

- Log in to your Merchant Menu at <https://secure.authorize.net/>
- Click on **Transaction Activity**.

Current Batch of Transactions

Your Current Batch consists of all transactions that have not yet been settled, including voided transactions that have not yet been settled. Transactions that have been declined will not appear in your Current Batch, but are included in the **Download Transactions** section. Transactions that fail initial validation before being sent to the processor and are declined are not recorded in the database and cannot be seen in the batch download. Transactions that travel to the processor but are declined are recorded, and thus do appear in the batch download.

Within the **Current Batch**, you can do the following:

- **View** transaction details.
- **Void** transactions.
- **Select** previously authorized transactions for settlement.
- **Review** the fraud score for each transaction (if your account is Fraud Screen enabled). For more information on Fraud Screen, please see the [Fraud Screen](#) section in Chapter 3.

Note: If you do not capture or void them, transactions may remain in the current batch for up to 30 days. Any transaction left in the current batch for a period of 30 days will automatically expire. These authorizations are no longer valid at the processing networks and are automatically voided and removed from your current batch. This procedure prevents the current batch from becoming congested with outdated transactions and protects your customers as well as yourself from faulty billing.

Figure 5.2 Example Current Batch Screen

****Note:** In order to commit any changes to the transactions below, one of the buttons must be clicked.

View Filter : All Payment Methods ▾ Apply Filter

Next >> Details ...

<u>Result</u>	<u>Date/Time</u>	<u>Name</u>	<u>Invoice #</u>	<u>Cust ID</u>	<u>Payment Method</u>	<u>Payment Amount</u>	<u>Settlement Amount</u>	<u>Fraud Score</u>	<u>Details</u>
Settled	08-Dec-2000 11:01:16 AM MDT	Joe Merchant	11115	Merchant	eCheck	USD 160.00	USD 160.00	164	⊙
Settled	08-Dec-2000 11:01:16 AM MDT	Jane Wholesaler	11116	Wholesaler	eCheck	USD 75.00	USD 75.00	612	○

Next >> Details ...

Page 1 of 2

****Note:** In order to commit any changes to the transactions below, one of the buttons must be clicked.

Viewing Unsettled Transactions

The settlement process takes place once every day. All transactions that are approved and that have not yet been settled are located in the Current Batch.

To view those transactions, do the following:

- Click the drop down box underneath **Settlement Batches**.
- Select **Current Batch**.
- Click **Go**.

Figure 5.3 Example of Transaction Details

[Return](#)

Transaction Information

Date/Time	17-Nov-2000 10:01:41 AM MST
ID	100000000
Type	Authorization w/ Auto Capture
Current Status	Settled
Authorization Code	000000
Address Verification (AVS)	Street Address: Match -- First 5 Digits of Zip: Match

Order Information

Invoice #	11115
Description	Daily Supply of Cheer
Payment Method	Visa
Payment Amount	160.00 (USD)
Settlement Amount	160.00 (USD)

Credit Card Information

Number	40070000000027
Expiration	10/2002

Bank Information (eCheck)

ABA Routing Number	
Account Number	

Customer Billing Information

Customer ID	Merchant
First Name	Joe
Last Name	Merchant
Company	Joe Merchant & Sons
Address	1234 Elm Street
City	Anywhere
State/Province	UT
Zip Code	12345
Country	USA
Phone	555 555 5555
Fax	555 555 5556
E-Mail	joemerchant@joemerchant.com

Customer Shipping Information

First Name	Joe
Last Name	Merchant
Company	Joe Merchant & Sons
Address	1234 Elm Street
City	Anywhere
State/Province	UT
Zip Code	12345
Country	USA

[Return](#)

Viewing Transaction Details

Within any batch, you can view the details recorded by Authorize.Net for a particular transaction by doing the following:

- Click the drop-down box underneath **Settlement Batches**.
- Select the desired batch.
- Click under **Select** next to the transaction for which you would like to see the details.
- Click **Details**.

Figure 5.4 Example Transaction

**Note: In order to commit any changes to the transactions below, one of the buttons must be clicked.

View Filter:

Page 1 of 1

Capture	Void	Date/Time	Address Verification	Name	Invoice #	Cust ID	Payment Method	Payment Amount	Settlement Amount	Fraud Score	Details
<input checked="" type="checkbox"/>	<input type="checkbox"/>	13-Dec-2000 08:19:42 PM EST	Street Address: No Match -- First 5 Digits of Zip: Match	Joe Merchant	1115	merchant	American Express	USD 100.00	USD 100.00	156	<input type="button" value="Details"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	13-Dec-2000 09:40:26 PM EST	Street Address: Match -- First 5 Digits of Zip: Match	Jane Wholesaler	1116	wholesaler	MasterCard	USD 99.95	USD 99.95	223	<input type="button" value="Details"/>

Page 1 of 1

**Note: In order to commit any changes to the transactions below, one of the buttons must be clicked.

Voiding Transactions

If a transaction has not been settled and you would like to void it, you can do so within the Current Batch.

To void a transaction that has not been settled, do the following:

- Click the drop down box underneath **Settlement Batches**.
- Select **Current Batch**.
- Click **Go**.
- Find the transaction that you would like to void.
- Click the **Void** box next to the desired transaction.
- To save this change, scroll down to the bottom of the page and click **Refresh Page**.

Warning: It is impossible to void a transaction that has been settled. If you need to nullify a transaction that has already been settled, you can issue a refund (see **Chapter 4 Virtual Terminal** for details on how to process a refund).

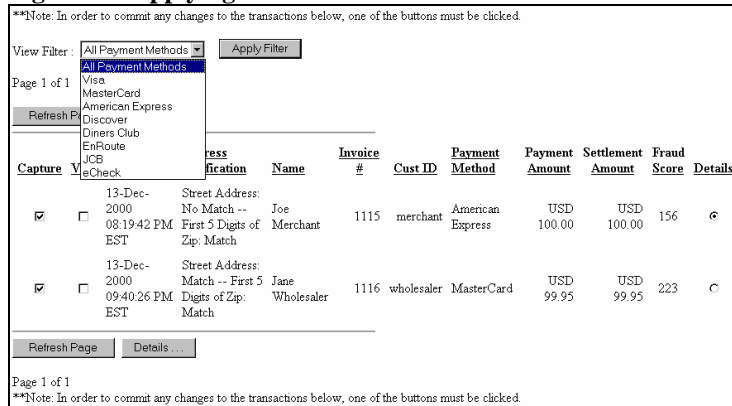
Selecting Authorization-Only Transactions for Capture

As explained in **Chapter 4: Virtual Terminal**, a transaction processed using the Authorization-Only method will not be captured until the Merchant enters the Merchant Menu and manually selects such a transaction for capture. Because the transaction remains unsettled, it also remains in the Current Batch.

To select a transaction for capture, do the following:

- Click the drop down box underneath **Settlement Batches**.
- Select **Current Batch**.
- Click **Go**.
- Find the transaction that you would like to select for capture.
- Click the **Capture** box.
- To save this change, scroll down to the bottom of the page and click **Refresh Page**.

Figure 5.5 Applying the Filter to Transaction Details



Viewing Transactions According to Card Type

If you would like to see a list of a batch’s transactions according to the type of credit card used, you can use the filter provided at the top of each page of batch listings. To filter according to credit card type, do the following:

- Click the drop down box underneath **Settlement Batches**.
- Select the desired batch.
- Click **Go**.
- Click the drop down box next to **View Filter**.
- Select the payment type (e.g. Visa, Mastercard, etc.) for the transactions that you would like to see.
- Click **Apply Filter**.

View Returned Items

When a transaction is processed through the eCheck.Net service, the transaction will either show up in the Merchant Menu as approved, or show up as rejected in the Returned Items section. ACH returns and chargebacks will be shown in the batch corresponding to the day on which the return or chargeback occurs.

Figure 5.6 Example of Returned Items

Type	Reason	Received Date/Time	Amount	Original Settlement Batch	Original Transaction ID
Correction Notice	Incorrect Routing Number	17-Nov-2000 12:23:45 PM MDT	\$10.00	14-Nov-2000 04:01:45 PM MDT	1111111
Chargeback	Customer Advises Not Authorized	17-Nov-2000 11:01:45 PM MDT	\$10.00	14-Nov-2000 04:01:45 PM MDT	1111111
Returned Item	Insufficient Funds	17-Nov-2000 10:56:45 PM MDT	\$10.00	14-Nov-2000 04:01:45 PM MDT	1111111

Viewing Returned Items

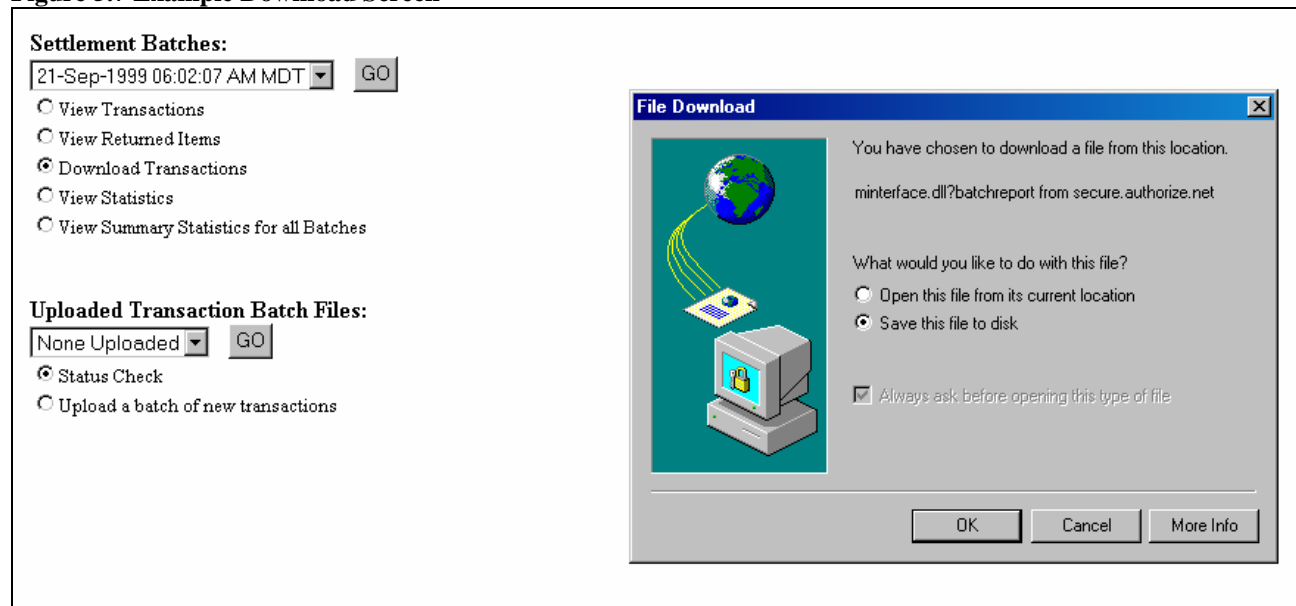
To view **Returned Items**, do the following:

- Click the drop-down box underneath **Settlement Batches**.
- Select the batch whose returned items you would like to see.
- Select the radio button next to **View Returned Items**.
- Click **Go**.

Download Transactions

You may view the details of a transaction by downloading a batch of transactions to your personal computer. Downloading a batch allows you to have a record of the transactions, both approved and declined, for any given batch. Transactions that fail initial validation before being sent to the processor but are declined are not recorded in the database and cannot be seen in the batch download. Transactions that travel to the processor but are declined are recorded, and thus do appear in the batch download.

Figure 5.7 Example Download Screen



Downloading Transactions

To **Download Transactions**, do the following:

- Click the drop down box underneath **Settlement Batches**.
- Select the batch of transactions that you would like to download.
- Select the radio button next to **Download Transactions**.
- Click **Go**.
- Follow the prompts from your computer to download that file.

View Statistics

You may want to view the breakdown of statistics for any given batch. The **View Statistics** section includes information about the number of successful transactions processed, the number of declines processed, the total dollar amounts for the batch, and other helpful information.

Figure 5.8 Example Daily Batch Statistics Screen

Batch Statistics Report												
Settlement Date/Time: 17-Nov-2000 04:44:54 PM MST												
Payment Method	Debit Count	Debit Amount	Credit Count	Credit Amount	Total Count	Total Amount	Net Amount	Decline Count	Approval Percentage	Void Count	Void Amount	Error Count
Visa (USD)	18	38,774.00	0	0.00	18	38,774.00	38,774.00	4	%81.82	0	0.00	0
MasterCard (USD)	12	16,420.00	0	0.00	12	16,420.00	16,420.00	3	%80.00	0	0.00	0
American Express (USD)	4	13,440.00	0	0.00	4	13,440.00	13,440.00	1	%80.00	0	0.00	0
Discover (USD)	7	18,630.00	1	224.55	8	18,854.55	18,405.45	1	%88.89	0	0.00	0
TOTALS	41	87,264.00	1	224.55	42	87,488.55	87,039.45	9	%82.35	0	0.00	0

Viewing Daily Batch Statistics

To **View Statistics** for a certain batch, do the following:

- Click the drop-down box underneath **Settlement Batches**.
- Select the batch of transactions whose statistics you would like to see.
- Select the radio button next to **View Statistics**.
- Click **Go**.

Figure 5.9 Example Summary Statistics Screen

Batch Statistics Report												
Settlement Date/Time: Summary of all Successfully Settled batches (excludes current batch)												
Payment Method	Debit Count	Debit Amount	Credit Count	Credit Amount	Total Count	Total Amount	Net Amount	Decline Count	Approval Percentage	Void Count	Void Amount	Error Count
Visa (USD)	7,079	10,515,236.13	417	1,054,540.36	7,496	11,569,776.49	9,460,695.77	1,918	%79.63	195	351,801.96	56
MasterCard (USD)	4,400	7,142,864.87	262	631,077.04	4,662	7,773,941.91	6,511,787.83	1,047	%81.66	114	221,997.25	49
American Express (USD)	1,394	1,919,008.65	55	136,355.43	1,449	2,055,364.08	1,782,653.22	222	%86.71	28	65,916.50	25
Discover (USD)	1,185	2,252,597.05	54	163,397.85	1,239	2,415,994.90	2,089,259.20	103	%92.32	40	89,781.50	2
eCheck (USD)	7,223	1,317,184.49	92	334,299.12	7,315	1,651,483.61	982,885.37	0	%100.00	4	1,237.62	3
TOTALS	21,281	23,146,891.19	880	2,319,609.80	22,161	25,466,500.99	20,827,281.39	3,290	%87.07	381	730,734.83	135

Viewing Summary Statistics

You may be interested to know the cumulative statistics for all the batches that have been processed through your Authorize.Net account. You can view such statistics in the **View Summary Statistics for all Batches** section.

To view summary statistics for all batches, do the following:

- Click the drop-down box underneath **Settlement Batches**.
- Select the radio button next to **View Summary Statistics for all Batches**.
- Click **Go**.

Batch Uploads

The Batch Upload feature of Authorize.Net provides you with the means to submit multiple transactions simultaneously, thus allowing you to better utilize the efficiency of the Authorize.Net payment gateway (For more information regarding how to construct a batch upload file, please consult our Developer's Guide).

Figure 5.10 Example Batch Upload Screen

Uploading a Batch

To Upload a Batch, do the following:

- Select the radio button next to **Upload a Batch of New Transactions**.
- Click **Go**.
- Click **Browse**.
- By browsing through the files on your system, locate and select the file you want to upload.
- When you have found the file that you want to upload, click **Upload Batch File**.

Figure 5.11 Example Batch Upload Status Screen

Note: Once you see that transaction processing is finished, you can view transactions for that batch in your Current Batch until after settlement (at which time that will be listed according to its day of settlement).

Checking the Status of an Uploaded Batch

After uploading a batch, you can check the status of that batch—which transactions have been settled, and the time at which they were settled.

To check the status of an uploaded batch, do the following:

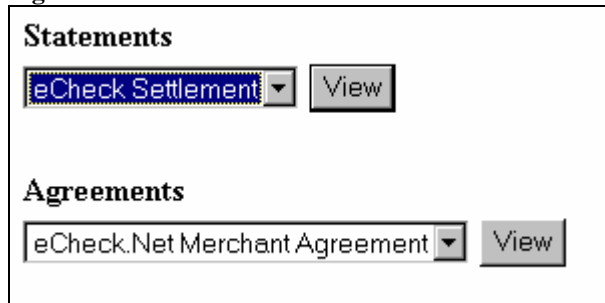
- Click the drop down box underneath **Uploaded Transaction Batch Files**.
- Select the batch whose status you would like to check.
- Select the radio button next to **Status Check**.
- Click **Go**.

Note: Transaction ID must be included when uploading a batch containing Credit Returns.

Chapter 6 Account Information

Account Information is the section for information regarding your billing and your eCheck.Net balances. This section provides a view of all the previous billing, a brief description of the type of billing that took place, and a record of any agreements you have executed pertaining to your gateway account and Authorize.Net services.

Figure 6.1 Account Information Screen



The screenshot shows a web interface with two main sections. The first section is titled "Statements" and contains a dropdown menu with "eCheck Settlement" selected and a "View" button to its right. The second section is titled "Agreements" and contains a dropdown menu with "eCheck.Net Merchant Agreement" selected and a "View" button to its right.

To enter **Account Information**, do the following:

- Log in to your Merchant Menu at <https://secure.authorize.net/>
- Click **Acct Info**.

Viewing eCheck.Net Settlement

To view your eCheck.Net account balance, do the following:

- Click the drop down box underneath **Statements**.
- Select **eCheck.Net Settlement**.
- Click **View**.

Note: Your eCheck.Net account balance reflects transaction submissions, transaction rejections, deposits to your account, and any fees associated with the eCheck.Net process. The top line is the latest balance for your eCheck.Net account. There is a date, amount, and description corresponding to each change in your account balance. There are separate entries for the point at which a billing is posted to your account and the point at which the billing is actually paid.

Viewing Billing Statement

To view your billing statement, do the following:

- Click the drop-down box underneath **Statements**.
- Select **Billing**.
- Click **View**.

Remember: There are separate entries for the point at which the bill is posted to your account and the point at which the bill is actually paid.

Viewing Agreements

To view the agreements pertaining to your gateway account, do the following:

- Click the drop-down box underneath **Agreements**.
- Select the agreement you wish to view from the drop-down menu.
- Click **View**.

Understanding Billing Statement Terminology

The following is a list of possible terms you might encounter as you read your billing statement:

Payment: When funds are actually taken from your account for fees associated with use of the Authorize.Net service, that transaction will be described as a “payment.”

Billing: When a bill is assessed to your virtual balance, it is described as a “billing.” This does not indicate that money has been taken out of your account. The actual charge to your account for a bill is described in a different entry as a “payment.”

Transfer: On your billing statement, this term is used to describe a transfer of funds from your Authorize.Net billing reserve in order to offset your balance.

eCheck.Net: An eCheck.Net payment is a billing to the merchant’s checking account for the outstanding balance. This payment is automatically processed by the system during the billing cycle.

***eCheck.Net Monthly Minimum Fee:** This is a monthly fee that each eCheck.Net merchant must pay Authorize.Net for access to and use of the eCheck.Net service.

****Gateway Access Fee:** This is a monthly fee paid for the right to use the Authorize.Net service.

Credit Card: This is a description of a bill that is assessed to your credit card for services (used as a means of secondary billing—eCheck.Net will usually be used.)

Intra Account: This is the “item” description for a **transfer**, and indicates a transfer from the billing reserve to offset your billing balance.

***Chargeback Fee:** This is a fee that an eCheck.Net Merchant must pay to Authorize.Net each time a Purchaser initiates a Chargeback of the amount of an eCheck.Net Transaction submitted by Merchant to Authorize.Net.

***eCheck Returned Item Fee:** This is a fee that an eCheck.Net Merchant must pay to Authorize.Net each time Authorize.Net attempts to initiate a debit to a Purchaser’s bank account on behalf of Merchant and such an attempt is unsuccessful for a reason outside of Authorize.Net’s control, such as the Merchant and/or Purchaser provided Authorize.Net with incorrect bank account information.

***eCheck Transaction Fee:** This is a fee that is assessed on a per-transaction basis for use of the eCheck.Net service.

***eCheck Discount Fee:** This is a fee that is each eCheck.Net Merchant must pay Authorize.Net for the handling and processing of each debit transaction submitted by Merchant to Authorize.Net via the eCheck.Net Service. The amount of the eCheck.Net Discount Rate Fee shall be a percentage of the total dollar amount of all debit transactions submitted by Merchant to Authorize.Net via the eCheck.Net Service in a given day.

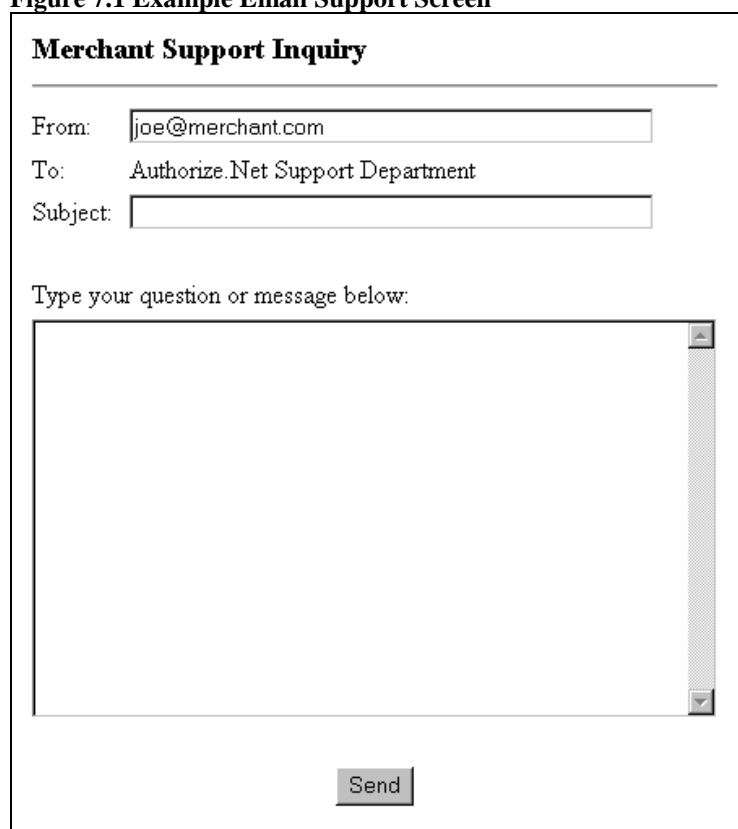
*See the eCheck.Net Standard Terms in your eCheck.Net Service Agreement for more information about these fees.

**See the Authorize.Net Service and Software License Agreement for more information about this fee and others associated with your use of the Authorize.Net credit card transaction processing and settlement payment gateway services.

Chapter 7 Support

To facilitate your success as a Merchant, we have provided outlets to help you in learning about the use of the Authorize.Net system, and overcoming any challenges regarding the use of your Authorize.Net account. Should you have further questions that are not answered either in this **Authorize.Net Merchant Menu User Guide**, the **Developer's Guide**, or in the **Support Section** of our website, feel free to contact us, either by email or by phone.

Figure 7.1 Example Email Support Screen



The screenshot shows a web form titled "Merchant Support Inquiry". It contains three input fields: "From:" with the value "joe@merchant.com", "To:" with the value "Authorize.Net Support Department", and "Subject:" which is empty. Below these fields is a text area with the prompt "Type your question or message below:" and a large empty text box with a vertical scrollbar. At the bottom center of the form is a "Send" button.

Emailing Support from your Merchant Menu

To email our Support Department from your Merchant Menu, do the following:

- Click **Support**.
- Type in the subject of your email and your questions/comments.
- Scroll down to the bottom of the screen and click **Send**.

Note: When emailing for support, please send your Login ID with your comments and/or suggestions. Please do **not** send your password, credit card information, or other sensitive information in email correspondence.

Index

A

Account Information, 7, 41, 54
Acquiring Bank, 6, 7
ADC Direct Response, 26, 27
ADC Direct Response Settings, 26
ADC methods, 22, 24, 26
ADC Methods, 26
ADC Relay Response, 22, 24, 25
ADC Relay Response Default URL, 22, 24
Adding a Contact, 15
Adding a Footer to the Payment Form, 18
Adding A Relay Response URL, 24
Address Verification System, 30, 33
Address Verification System (AVS) Filter, 30
Auth-Capture transaction, 45
authorization code, 40, 44
Authorization-Only, 43, 46, 49
Authorization-Only credit card transactions, 43
Authorize.Net, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 19, 20, 22, 23, 24, 26, 27, 28, 30, 31, 33, 37, 44, 48, 52, 53, 55
Authorize.Net account, 4, 5, 12, 40, 52, 56
Authorize.Net accounts, 5
Authorize.Net customer email, 19
Authorize.Net Email Receipt, 16
Authorize.Net Receipt Page, 16
Authorize.Net system, 56
Automated Direct Connect (ADC) Settings, 26, 27
AVS Filter Risks, 30, 31
AVS filters, 33
AVS Interface, 33
AVS mismatch, 30, 31
AVS response, 30, 32, 33
AVS response code, 30
AVS Response Code Explanations, 30
AVS System, 30

B

Batch Upload feature, 53
Batch Upload Settings, 28
Batch Uploads, 46, 53
Billing, 7, 54, 55
billing statement, 54, 55

C

Capture-Only method, 44
Capture-Only transaction, 44
card billing address, 30
Card Issuer, 6, 7
Changing Colors, 17
Changing Email Receipt Settings, 19

Changing the Receipt Page Settings, 19
Changing Your Password, 14
Chargeback Fee, 55
Checking the Status of an Uploaded Batch, 53
Configuring Batch Upload, 28
contact information, 12
Controlling the Information on your Payment Form, 20
credit card, 4, 5, 11, 13, 30, 31, 32, 40, 41, 43, 44, 45, 50, 55, 56
credit card information, 5, 30, 40, 43, 44, 56
credit card statements, 45
credit limit, 32, 45
Current Batch, 47, 48, 49, 53
Current Batch of Transactions, 47
Customer Email Receipt Footer, 20
Customer Email Receipt Header, 19
Customer Receipt, 15
Customizing the ADC Direct Response Settings, 26

D

Daylight Savings Time, 10, 13
Default Field Encapsulation Character, 26, 28
Default Field Separator, 26, 28
Deleting a Contact, 16
Deleting a URL, 25
Delimited Response, 26
Designating Field Order for Batch Upload File, 29
Developer's Guide, 14, 22, 53
Developers Guide, 24, 26, 28, 56
Download Transactions, 47, 51
Downloading a batch, 51

E

eCheck Discount Fee, 55
eCheck Returned Item Fee, 55
eCheck Transaction Fee, 55
eCheck.Net, 5, 11, 31, 40, 41, 43, 50, 54, 55
eCheck.Net application, 11
eCheck.Net Minimum Processing Fee, 55
eCheck.Net service, 11, 40, 55
Edit URL, 25
Editing a Contact, 16
Editing a URL, 25
electronic gateway, 5
Email Receipt Settings, 19
Emailing Support From Your Merchant Menu, 56

F

FDC, 30
fees, 7, 32, 54, 55
fraud score, 34, 35, 47
Fraud Screen Settings, 34

FraudScreen.Net, 33, 34, 35, 36
fraud-screening engine, 33

G

Gateway Fee, 55
General Merchant Settings, 13
GPS, 30

I

Interchange, 6, 7
Internet, 4, 8, 10, 30
Interview Area, 8, 10
Intra Account, 55
inventory management system, 45
Issuing Credits Using the Virtual Terminal, 41

L

Licensing Agreement, 10
Login ID, 5, 8, 13, 14, 56

M

Manage Contact Information, 14, 15
Manage URLs, 19, 22
Managing Transactions Using the Fraud Score, 34
MD5 Hash, 26
Merchant account, 5
Merchant Account Number, 5
Merchant Agreement, 14
Merchant Menu, 1, 4, 7, 8, 11, 12, 14, 27, 35, 40, 46,
49, 50, 54, 56
Merchant Menu Interface, 34
Merchant Menu User Guide, 1, 4, 56
Merchant Service Provider, 5, 30, 32, 40

N

Nova, 30

O

Optimizing Fraud Detection, 35

P

Partial Order Fulfillment, 44
password, 5, 8, 13, 14, 27, 56
Password-Required mode, 27
Password-Required Mode, 27
Payment Form, 16, 17, 18, 20, 21
Payment Form/Weblink Field Settings, 20, 37, 39
Payment Form/WebLink Field Settings, 40
payment processing network, 12
payment processor, 14, 43
Payment Processor, 5
Paymentech, 30
Processing Authorization-Only Transactions, 43
Processing Capture-Only Transactions, 44

Processing Credit Card Transactions, 40
Processing Gateway, 6

R

Receipt Link Address, 22
Receipt Link Default URL, 22, 23, 25
Receipt Link Method, 19
Receipt Link URL, 19, 22, 23
Receipt Page Settings, 19
Receipt Settings, 16, 17, 18
rejection threshold, 33, 34, 35
Relay Response, 24, 27

S

Sample Rules Using the Cutoff Score, 35
Secure Payment Form, 23
Selecting Authorization-Only Transactions for Capture,
43, 49
Selecting Information Fields for your Payment Form,
20
Selecting Information Fields for Your Virtual Terminal,
21
Setting AVS functionality, 33
Settings Area, 12
settlement process, 7, 48
Settlement Process, 7
Silent Post Default URL, 22
Silent Response Default URL, 24
Support Department, 56

T

test mode, 13, 14
Test Mode, 12, 13
test transactions, 14
Time Zone, 14
Transaction Activity, 29, 43, 46
Transaction Activity and Batch Uploads, 29, 46
Transaction Batch Upload Settings, 28, 29
Transaction Process, 6

U

Understanding Billing Statement Terminology, 55
Uploading a Batch, 53
Using FraudScreen.Net, 34

V

Valid Referrer URL, 23, 24
Valid Referrer URLs, 22, 23, 24
View Returned Items, 50
View Statistics, 52
Viewing Agreements, 55
Viewing Billing Statement, 54
Viewing Daily Batch Statistics, 52
Viewing eCheck.Net Settlement, 54

Viewing Returned Items, 50
Viewing Summary Statistics, 52
Viewing Transaction Details, 48
Viewing Transactions According to Card Type, 50
Virtual Terminal, 21, 27, 40, 41, 43, 44, 45, 46, 49
Virtual Terminal Field Settings, 21
Virtual Terminal Payment Form, 40

Vital, 30
Voiding Transactions, 49

W

WebLink, 25, 27
World Wide Web, 8