Authorize.Net™
Where the world does business on the Web

3.0 Merchant Menu User Guide

TABLE OF CONTENTS

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 3.0 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 services).

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. 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.
- If the Merchant Service Provider is also your Authorize.Net Reseller, they activate processing capability for those cards on your Authorize.Net account.
- Deposits credit card funds to your 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 trans-action 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 explain the interactions that occur when processing a transaction through Authorize.Net.

Figure 1.1 The Transaction Process
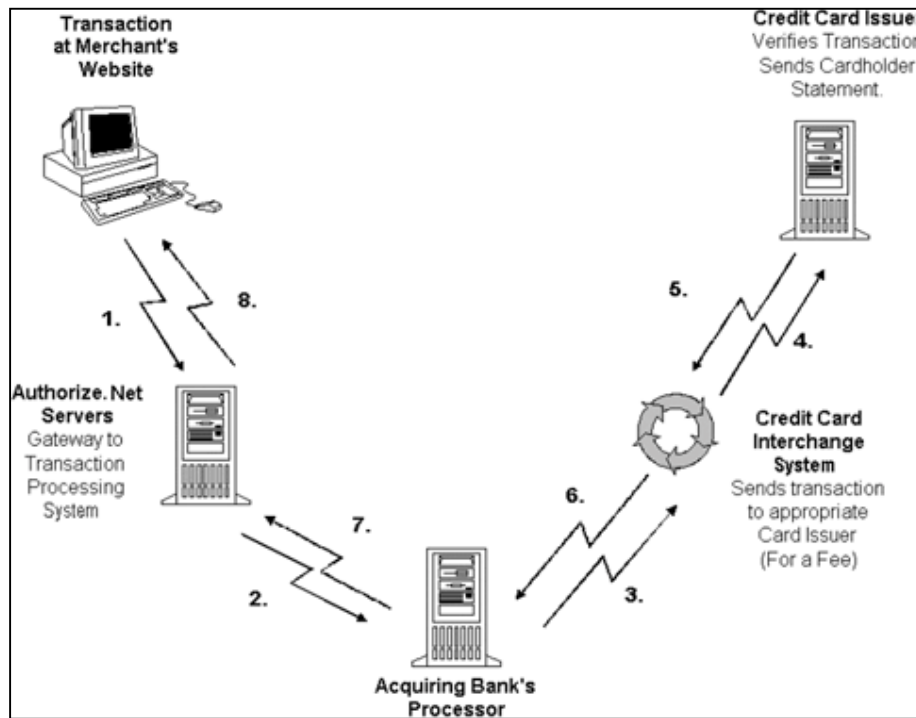
1. A transaction passes from the Merchant's website to the Authorize.Net Processing Gateway.
2. The transaction is transmitted to the Acquiring Bank's processor.
3. The Acquiring Bank's processor passes the transaction to the Credit Card Interchange system.
4. The Credit Card Interchange system queries the appropriate Card Issuer database.
5. The Card Issuer approves or declines transaction, places hold on funds, and passes result/authorization codes back through the Credit Card Interchange system.
6. The Credit Card Interchange system relays 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 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
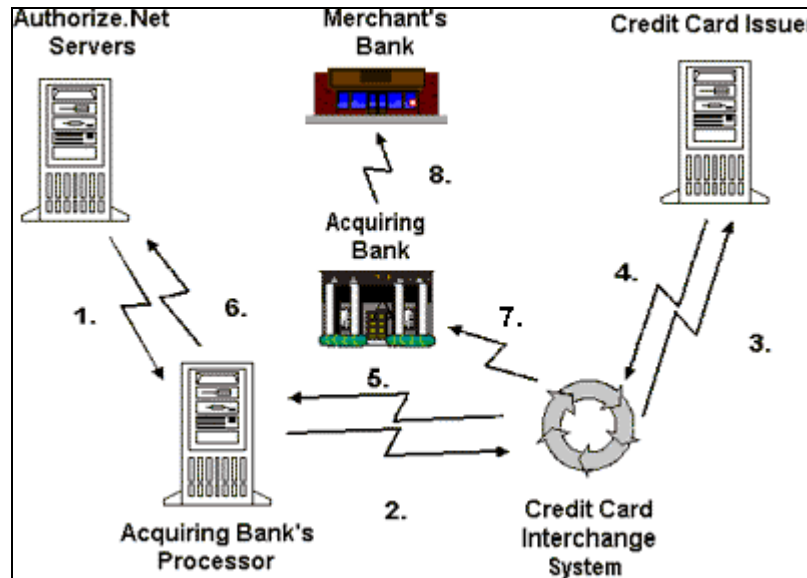
1. Authorize.Net servers automatically transmit batches of transactions to the Acquiring Bank's processor.
2. The Acquiring Bank's processor passes the transaction batches to the Credit Card Interchange system.
3. The Credit Card Interchange system routes to the appropriate Card Issuer database.
4. The Card Issuer verifies transactions, passes results through 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 (7). The Acquiring Bank passes remaining funds to the Merchant's bank account (8).
6. The Acquiring Bank's processor passes transaction results to Authorize.Net servers.

Billing

There are fees associated with your use of the Authorize.Net service. Fees for the Authorize.Net account are established by your Authorize.Net Reseller. 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.

Figure 2.1 Login Screen

Interview Area

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

Figure 2.2 Example First Interview Screen

Figure 2.3 Example Second Interview Screen

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 Internet and computer technology.

Figure 2.4 Transaction Processing Agreement

Licensing Agreement Area

Upon completion of the interview, you will be shown a **Transaction Processing Agreement**. You *must* read this agreement and provide the social security number of the Principal/Corporate officer as set up by the Reseller (for verification purposes).

eCheck.Net 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 the eCheck.Net service has been activated by Authorize.Net, your account will not be able to successfully process eCheck.Net transactions. The online application requests basic information and out-lines regulations associated with use of the eCheck.Net account. Read this information carefully and follow the directions for printing this agreement and mailing it to Authorize.Net for approval. Authorize.Net will notify you of the results of your application to use the eCheck.Net service.

Warning: You will have one chance to print the eCheck.Net online application, 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 complete the Merchant agreements. See preceding paragraphs for information regarding those agreements.)

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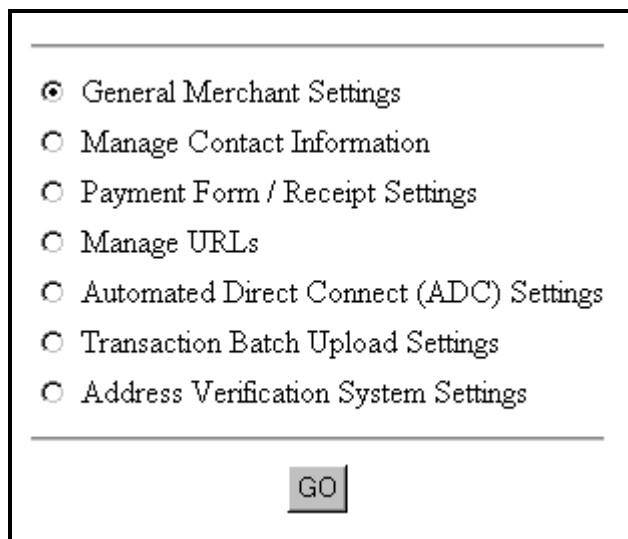
The Settings Area allows you to customize your Authorize.Net account. Features explained for the settings area include:

- 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
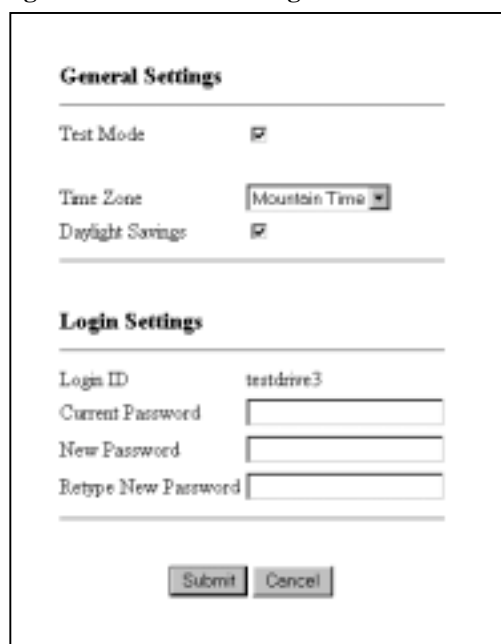
General Merchant Settings

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.

Figure 3.2 General Settings

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 complete the Merchant 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 3.0 Developer's Guide).

Figure 3.3 General Settings Page

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

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 in to your Merchant Menu, customize your account, and most importantly, process transactions, **you must exercise extreme caution in sharing your password with others**. By doing so, and by correctly using the Authorize.Net system, your password will remain confidential.

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 3.4 Example Manage Contact Information Screen

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

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

Figure 3.5 Example Add Contact Screen

Adding a Contact

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

- Click **Add Contact**.
- Fill out the following:
    - o Personal Name
    - o Title
    - o Phone and Extension
    - o 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 3.6 Example Edit Contact Screen

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 Authorize.Net service. If a Merchant needs a secure site for processing transactions through their 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 3.7 Payment Form/Receipt Settings Menu
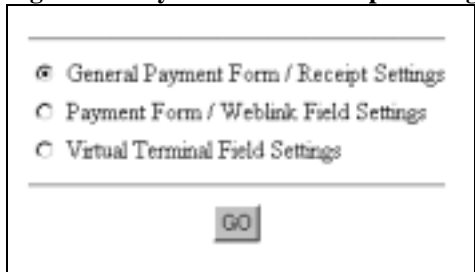
Figure 3.8 Changing Receipt/Payment Form Text, Link, or Background Colors

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

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

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:
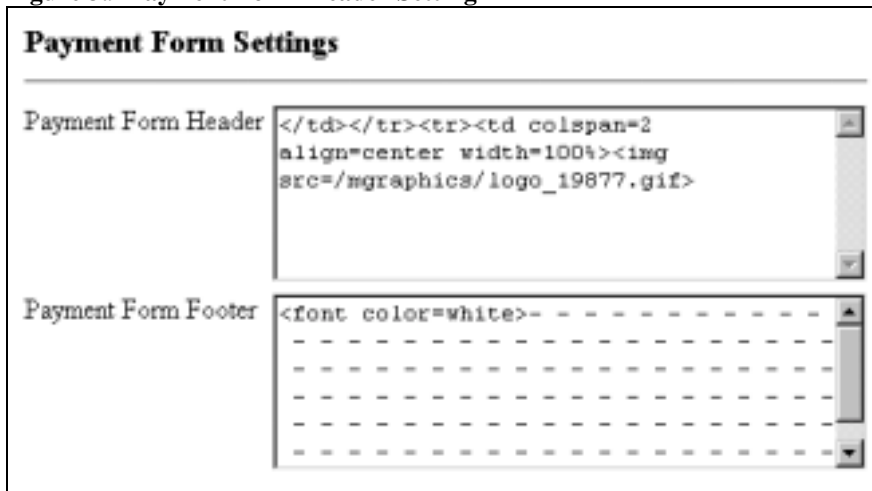
- Select **General Payment Form/Receipt Settings**.
- Click **Go**.
- Click the arrow next to the boxes for the **Text Color**, **Link Color**, or **Background Color**.
- Select the desired color **or** select **Hex Color Code** to enter the hexadecimal value for another color.
- If you have selected **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**.

Figure 3.9 Payment Form Header Setting

Payment Form Settings

Payment Form Header
```
</td></tr><tr><td colspan=2
align=center width=100%><img
src=/mgraphics/logo_19877.gif>
```

Payment Form Footer
```
<font color=white>- - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - -
```
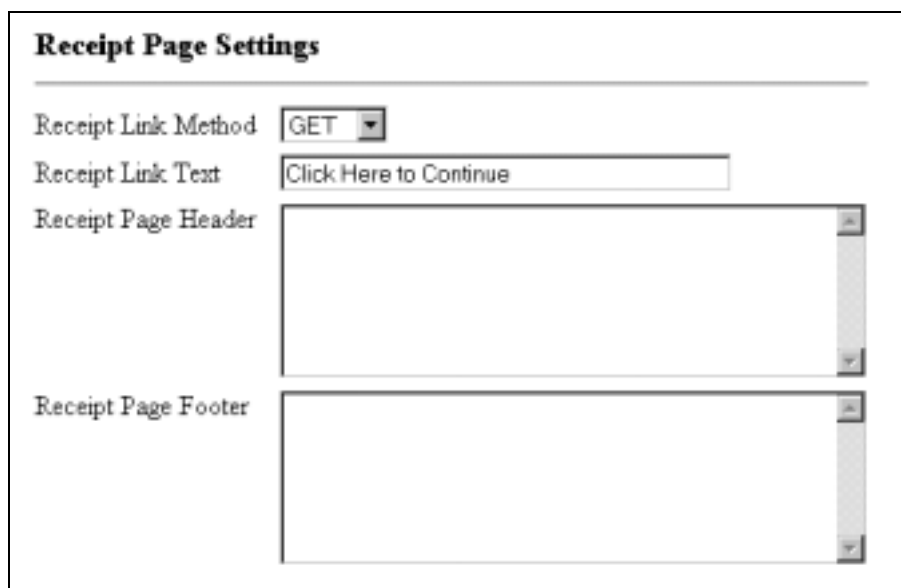
Adding a Footer to the Payment Form

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

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

Note: Due to page size, only 255 characters may be entered for each header/footer. All characters over 255 will be omitted.

Figure 3.10 Receipt Page Setting

Receipt Page Settings

Receipt Link Method   [GET ▼]

Receipt Link Text   [Click Here to Continue]

Receipt Page Header   [   ]

Receipt Page Footer   [   ]

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 3.11 Email Page Setting

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 3.12 Example Payment Form Field Settings

Payment Form / Weblink Field Settings

Description	Viewable	Editable	Required
Invoice #	☑	☐	☑
Description	☑	☐	☑
Customer ID	☑	☐	☐
Customer First Name	☑	☑	☑
Customer Last Name	☑	☑	☑
Customer Company	☑	☑	☐
Customer Address	☑	☑	☑
Customer City	☑	☑	☑
Customer State	☑	☑	☑
Customer Zip	☑	☑	☑
Customer Country	☑	☑	☐
Customer Phone	☑	☑	☑
Customer Fax	☐	☐	☐
Customer E-Mail	☑	☑	☑
Shipping First Name	☐	☐	☐
Shipping Last Name	☐	☐	☐
Shipping Company	☐	☐	☐
Shipping Address	☐	☐	☐
Shipping City	☐	☐	☐
Shipping State	☐	☐	☐
Shipping Zip	☐	☐	☐
Shipping Country	☐	☐	☐
Level 2 Tax	☐	☐	☐
Level 2 Duty	☐	☐	☐
Level 2 Freight	☐	☐	☐
Level 2 Tax Exempt	☐	☐	☐
Level 2 PO Number	☐	☐	☐
Currency Code	☐	☐	☐

Submit   Cancel

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 3.13 Example Virtual Terminal Field Settings

Virtual Terminal Field Settings

Description	Viewable	Editable	Required
Invoice #	☑	☑	☐
Description	☑	☑	☐
Amount	☑	☑	☑
Customer ID	☑	☑	☐
Customer First Name	☑	☑	☐
Customer Last Name	☑	☑	☐
Customer Company	☑	☑	☐
Customer Address	☑	☑	☐
Customer City	☑	☑	☐
Customer State	☑	☑	☐
Customer Zip	☑	☑	☐
Customer Country	☑	☑	☐
Customer Phone	☑	☑	☐
Customer Fax	☑	☑	☐
Customer E-Mail	☑	☑	☐
Shipping First Name	☑	☑	☐
Shipping Last Name	☑	☑	☐
Shipping Company	☑	☑	☐
Shipping Address	☑	☑	☐
Shipping City	☑	☑	☐
Shipping State	☑	☑	☐
Shipping Zip	☑	☑	☐
Shipping Country	☑	☑	☐
Level 2 Tax	☐	☐	☐
Level 2 Duty	☐	☐	☐
Level 2 Freight	☐	☐	☐
Level 2 Tax Exempt	☐	☐	☐
Level 2 PO Number	☐	☐	☐
Currency Code	☑	☑	☐

Submit   Cancel

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 (for 2.5 merchants only)

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 3.14 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				⊙

Add URL | Edit URL | Delete URL

To enter **Manage URLs**, do the following:
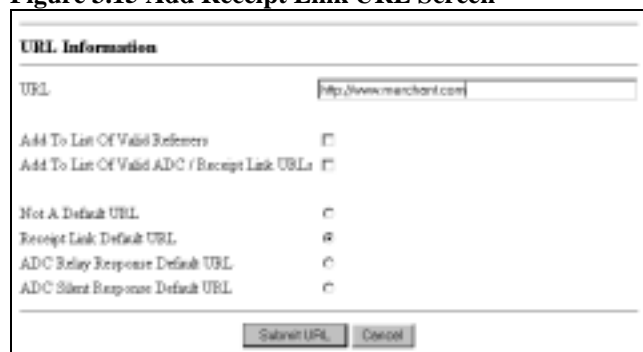
- Click **Settings**.
- Select **Manage URLs**.
- Click **Go**.

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 3.0 Developer's Guide).

Figure 3.15 Add Receipt Link URL Screen

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.

Adding a Valid Referrer URL

To add a URL as **Valid Referrer URL**, do the following:
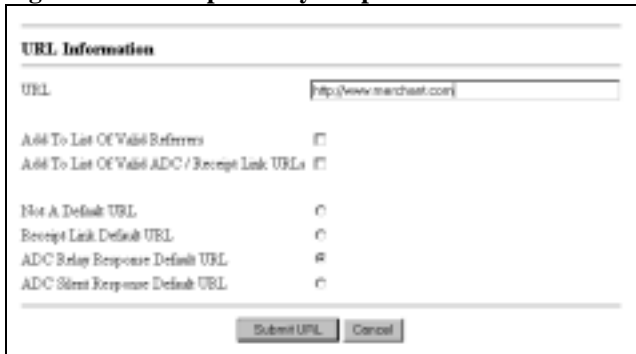
- Click **Add URL**.
- Click the box labeled **URL** and type in the *exact* web address of the Valid Referrer URL.
- Click the box labeled **Add to List of Valid Referrers**.
- Scroll down to the bottom of the page and click **Submit**.

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 3.0 Developers Guide). This setting only pertains to those merchants using the ADC Relay Response Method.

Figure 3.16 Example Relay Response URL Screen

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
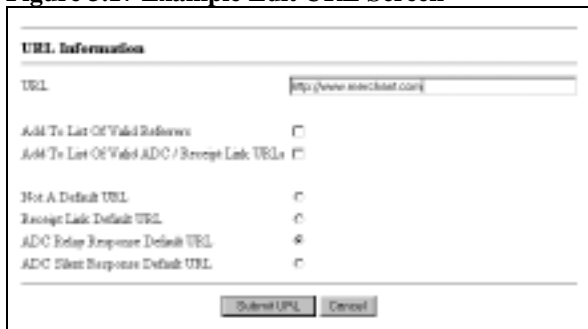
The Silent Response function is only available as a backwards compatibility tool for 2.5 Merchants, and should not be used with Authorize.Net 3.0 accounts.

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 3.17 Example Edit URL Screen

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 3.0 Developers Guide for more information regarding the ADC methods).

Figure 3.18 Example ADC Settings Page

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 3.0 Developers Guide for more details on how to configure a batch upload file).

Figure 3.19 Example Transaction Batch Upload Settings Page

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 **EMail 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 3.20 Example Transaction Batch Upload Settings Page

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: 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 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 your 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

In a recent sampling of approved transactions on the Authorize.Net system, 30% of all approvals were returned by the processor with some degree of AVS mismatch (codes A, B, E, G, N, P, R, U, W, or Z). Neglect for proper use of the AVS filter or a lack of understanding in the implications of its use may lead to confusion and lost business.

The Merchant should note that the AVS filter is not intended for use as absolute protection against fraud, nor is it intended for use in all processing scenarios. Careful attention should be paid to ensure that the filters are implemented appropriately. If your business has a low factor of risk, or potentially paying a non-qualified discount rate will not adversely affect your business, you should consider being very lenient in your application of the AVS filter. Conversely, if you have a high frequency of fraud or if you are incurring abnormally high discount rate charges, the AVS filter may be an appropriate method of protection.

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.

Figure 3.21 Example AVS Interface

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

Submit | Cancel

*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 provides Merchants the ability 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. HNC is the industry leader in transaction fraud scoring. They utilize dozens of online, offline, and positive and negative databases to score each transaction (0 - 1000) for the probability of fraud. These services are particularly appealing to Merchants in the following areas:

- 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 FraudScreen.Net, please see Chapter 7 for information on how to contact Authorize.Net.
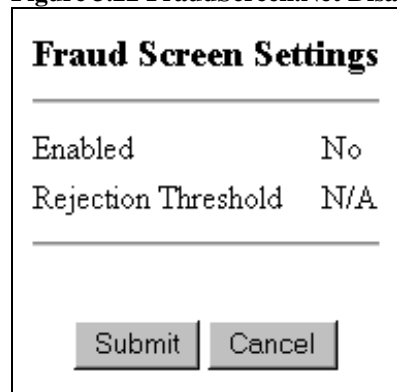
Using FraudScreen.Net

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:
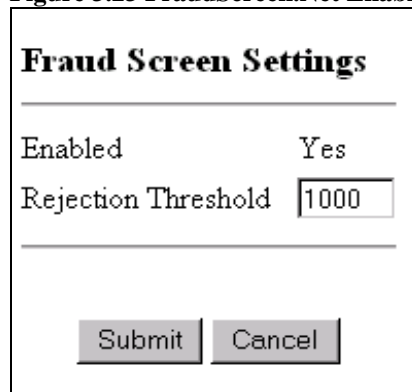
Figure 3.22 FraudScreen.Net Disabled Screen

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

Figure 3.23 FraudScreen.Net Enabled Screen

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. Since FraudScreen.Net is a statistical product, it cannot be expected to detect all frauds, however. 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. You set the first threshold through the Merchant Menu Interface (see Using FraudScreen.Net above). Transactions that score above the first threshold are automatically rejected. These transactions have an extremely high likelihood of fraud, so this threshold is usually 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 you determine while reviewing fraud scores of transactions in the current batch. Transactions that score above the second threshold are reviewed manually. Upon manual review, you may decide to void a transaction or allow it to be captured. Typically, this second threshold is somewhere between 500 and 800. You will learn over time what the best second threshold is for your business.

Sample Rules Using the Cutoff Score

For example, if 900 is your rejection score threshold (as set by you in the Merchant Menu), then all transactions scoring greater than 900 will be declined automatically by FraudScreen.Net. If you wish to manually review transactions scoring between 500 and 900, then 500 would be considered your *second* threshold. All transactions scoring greater than 500 but less than 900 would be left in the current batch until you have satisfactorily performed a manual review (manual fraud analysis). After reviewing these transactions you may choose to do one of the following: first, in the case that that you find the transaction to be "good", you may allow it to be captured and processed; second, in the case that the transaction is found to be suspicious of fraud, you 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.)

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

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**.

Notes: The ABA routing number corresponds to your customer's bank, is listed on the customer's check, and is necessary for an eCheck transaction to successfully take place.

Issuing Credits Using the Virtual Terminal

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

- From among the choices displayed in the category **Transaction Type**, Select **Credit Money Back to a Credit Card/Checking Account**.
- Provide customer information as shown on your Virtual Terminal Screen.
- Provide the **Customer's Credit Card/Checking Account Information**.
- To submit the credit, scroll down to the bottom of the page and click **Submit**.

Notes: Credits are not processed in real time, but are submitted at settlement time with other transaction. When issuing a credit, be certain to provide the customer's credit card/checking account information. The money for a refund is taken from the same checking account that is used for your Authorize.Net transaction deposits. Because of the risks involved with ACH (eCheck.Net) refunds, extreme caution should be taken in processing eCheck.Net refunds (for more information regarding these risks, please consult the eCheck.Net Usage Guide).

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 **Chapter 3 Settings** 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

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 use of an inventory management system that prevents overstating an initial authorization amount and encourages 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 cardholders 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.

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

Transaction Activity

To enter **Transaction Activit**y, 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

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

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

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

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

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 3.0 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

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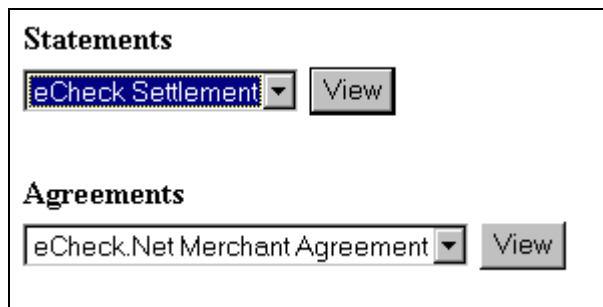
To check the status of an uploaded batch, do the following:

- 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: 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).

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 signed pertaining to your gateway account.

Figure 6.1 Account Information Screen

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 Minimum Processing Fee: This is the monthly minimum amount paid for use of eCheck.Net.
Gateway Fee: This is a 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 for a eCheck.Net chargeback, which occurs if the customer withdraws authorization for an eCheck.Net transaction.
eCheck Returned Item Fee: Should an eCheck transaction be returned by a customer's bank, a returned item fee is assessed.
eCheck Transaction Fee: This is a fee that is assessed on a per-transaction basis for use of the eCheck.Net service (such as $.20 per echeck.net transaction).
eCheck Discount Fee: This is a fee that is assessed according to total funds from eCheck.Net transactions (such as 1% of all funds processed).
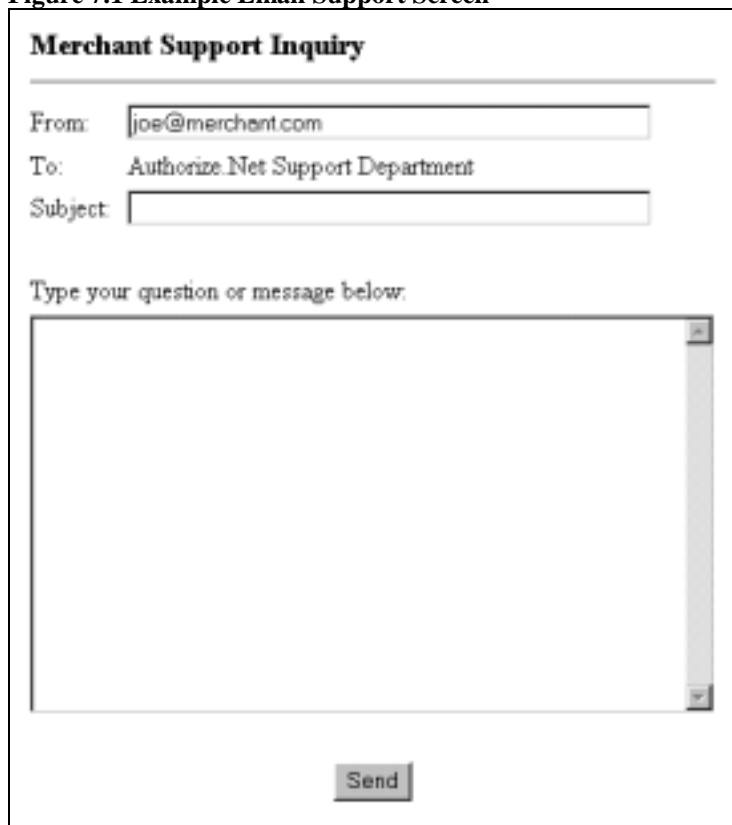
Chapter 7 Support

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 3.0 Merchant Menu User Guide**, the **3.0 Developers 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

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