

# **iTransact Gateway Account Settings Guide**

---

# iTransact Gateway Account Settings Guide

---

---

---

---

## Table of Contents

1. Version and Legal Information .....	1
2. The Account Settings Interface .....	2
The Account Settings .....	2
3. The Welcome Section .....	3
The Welcome Section .....	3
4. The General Information Section .....	4
The General Information Section .....	4
5. The Email Settings Section .....	5
The Email Settings Section .....	5
6. The Advanced Features Settings Section .....	6
The Advanced Features Settings Section .....	6
7. The Test Transaction Settings Section .....	7
The Test Transaction Settings Section .....	7
8. The Customer Confirmation Email Settings Section .....	8
The Customer Confirmation Email Settings Section .....	8
9. The Fraud Control Settings Section .....	9
The Fraud Control Settings .....	9
10. The Card Acceptance Section .....	14
The Card Acceptance Section .....	14
11. The Check Processing Information Section .....	15
The Check Processing Information Section .....	15
12. Style Settings Section .....	16
Style Settings .....	16

---

## List of Figures

3.1. Account Settings Welcome Example .....	3
4.1. Account Settings General Section Example .....	4
5.1. Account Settings Email Section Example .....	5
6.1. Account Settings Advanced Features Section Example .....	6
7.1. Account Settings Test Section Example .....	7
8.1. Account Settings Customer Email Section Example .....	8
9.1. Account Settings Fraud Controls Example .....	9
9.2. IP Filter Settings Example .....	10
10.1. Account Settings Card Acceptance Section Example .....	14
11.1. Account Settings Check Section Example .....	15
12.1. Account Settings Style Settings Example .....	16
12.2. Account Settings Style Color Bar Example .....	16

---

# Chapter 1. Version and Legal Information

**iTransact Gateway Account Settings Guide**

*iTransact Account Settings Guide*

Version: *1.11*

Date: *5/5/10*

Copyright: *iTransact, Inc. 2010*

---

# Chapter 2. The Account Settings Interface

## The Account Settings

The Account Settings interface is used to update contact information, anti-fraud features, email settings, and general transaction functions. It can be accessed through the Control Panel.

**Please remember, any changes to data in this interface require the user to click the "UPDATE" button at the bottom of the Account Settings interface.**

---

# Chapter 3. The Welcome Section

## The Welcome Section

**Figure 3.1. Account Settings Welcome Example**

CLOSE	Account Settings
NAME: ACC Live Test Co.	PASSWORD CHANGE: <input type="button" value="go"/>
GATEWAY ID: 66646	PIN UPDATE: <input type="button" value="go"/>

This section lists the Business Name and the Gateway ID (*See Figure 3.1*). Your gateway ID number will never change. To change the way your business name is listed here, please submit the request through your sales rep. This section also houses the following security code interfaces:

- **Password Change** - This interface allows a merchant to change their password. Click on the GO button to open the interface. The new desired password must meet the following requirements:

- 1) Minimum length: 8 characters
- 2) Maximum length: 30 characters
- 3) Must include at least two different character groups (lowercase letters, uppercase letters, digits, punctuation)
- 4) Cannot include the same character repeated three times (like aaa or 555) or a sequence of three characters (like xyz or 789)
- 5) Cannot include dictionary words, including common names.

To change the password, enter your then-current password into the "Current Password", and then enter your new desired password in the other two fields.

- **PIN Update** - This interface allows a merchant to setup or change their PIN number for the Transaction By Telephone system. To change the PIN code, click on the GO button to open the interface, enter your then-current PIN code into the "Current PIN", and then enter your new desired PIN code in the other two fields. All PIN codes must be six numeric digits.

---

# Chapter 4. The General Information Section

## The General Information Section

This section contains contact information for a Merchant to be used by the gateway (*See Figure 4.1*). The HELP command explains that the fields should be modified if any of the information changes.

**Figure 4.1. Account Settings General Section Example**

The screenshot displays a form titled "GENERAL INFORMATION" with the following fields and values:

GENERAL INFORMATION	
FIRST NAME:	Merchant
LAST NAME:	Name
ADDRESS:	4567 Merchant St
CITY:	Merchantville
STATE:	CA
ZIP:	90210
COUNTRY:	USA
PHONE:	8885551234
FAX:	8885551234
WEB SITE:	http://www.domain.com

A "HELP" button is located in the bottom right corner of the form area.

---

# Chapter 5. The Email Settings Section

## The Email Settings Section

Figure 5.1. Account Settings Email Section Example

The screenshot shows a web interface titled "EMAIL SETTINGS". It contains several input fields and a checkbox. The fields are: "CONTACT EMAIL:" with the value "email@domain.com", "ORDER EMAIL:" with the value "email@domain.com", "RECEIVE FAILURE EMAILS?" with a checked checkbox and the text "Yes", "ERROR EMAIL:" with the value "email@domain.com", and "CUSTOMER REPLY EMAIL:" with the value "email@domain.com". At the bottom, there is a link that says "CLICK TO JOIN THE MERCHANT UPDATES EMAIL LIST" and a "HELP" link in the bottom right corner.

This interface allows a merchant to change where the gateway sends emails concerning sales, settlements, order form errors and billings (*See Figure 5.1*). These emails may only be sent to one address. If you would like several individuals to receive these emails, please have your Network Administrator/Email Manager setup a multi-recipient alias address and use that to populate these fields. This interface also allows merchants to opt-in to the failure emails and the MerchantUpdates email list. Here is a more in depth explanation of each of these settings:

- **Contact Email Address** - This address will be sent account activation information and settlements..
- **Order Email Address** - This address will receive email confirmations of all sales, voids, credits, forces, pre-authorizations, post-authorizations, recurring billings, and failure emails (if selected). There is no way to turn off these emails (except for the failures). The gateway is required to send these confirmations to a merchant for that merchant's records. If a merchant decides not to do anything with these emails, they may want to setup a "garbage" email account and enter that address as the Order Email Address.
- **Receive Failure Emails Checkbox** - A merchant should select this feature if they would like to be sent an email anytime that a customer attempts to pay them but is rejected for some reason. The email will explain the reason for the failure by listing the response from the credit card processing network.
- **Error Email Address** - This address will be sent messages when there is an error in the order form script on a merchant's website. Generally, emails are only sent there as a merchant is first integrating the Gateway Software with their website and working to get the integration correct.
- **Customer Reply Email Address** - This address will be listed in the customer's copy of the email confirmation receipt as a contact address for the merchant.
- **The Merchant Updates Email List** - This link opens a window the interface that allows a merchant to subscribe to the opt-in MerchantUpdates email list. The MerchantUpdates mailing list is used to notify merchants of system maintenance, feature additions and other important information.
- **The HELP Menu** - This link provides a list of the functions of each of the email settings.

---

# Chapter 6. The Advanced Features Settings Section

## The Advanced Features Settings Section

Figure 6.1. Account Settings Advanced Features Section Example

The screenshot shows a web interface titled "ADVANCED FEATURES". It contains the following fields and controls:

- RECURRING POST-BACK URL:** A text input field containing "https://www.domain.com/c" and an unchecked "ACTIVATE" checkbox.
- SETTLEMENT TIME:** A dropdown menu currently set to "Auto" and a "MOUNTAIN TIME" button.
- ORDER FORM UID:** A text input field containing "7GxzWeDks37Q3fEPW7X" and a "RESET" link.
- API ACCESS:** A text input field containing "merchant\_business\_and\_XeNvE5Z8 N43A7zR74Q9ute6kGqx5" and a "RESET" link.

A "HELP" link is located in the bottom right corner of the form area.

- **The Recurring Post-Back URL** - If a merchant uses the recurring transaction features of the gateway, the merchant may specify a URL to receive transaction postback information generated at the time the transaction recurs. The "ACTIVATE" checkbox must be checked for this feature to function. For complete details concerning the Recurring Billing system and the Recurring Post-Back feature, please see the full gateway documentation.
- **The Settlement Time Selector** - By default, this setting is "AUTO", meaning that the software will cycle through all of the gateway accounts for settlement each night beginning at midnight. If a merchant would like their batch settlement to take place at a specific time each day, that merchant can select the appropriate time. "MANUAL" should be selected by merchants who want to settle each of their own batches using the "Settle Now" tool in the Settlement Options area of the Control Panel.
- **The Order Form UID Value** - This is the preferred option to be used as the value for the "vendor\_id" field in an order form or shopping cart. You can change this value by clicking the "RESET" link. NOTE: If your forms are using the UID instead of the Gateway ID and you reset this value, you MUST update the "vendor\_id" value in your order form or shopping cart or your transactions will not process.
- **The API Username** - This the username for people using the XML Connection Method. You can change this value by clicking the "RESET" link. NOTE: You must update your scripts generating the XML requests if you reset the API Access information.
- **The API Key** - This is used to help generate the payload signature for people using the XML Connection Method. You can change this value by clicking the "RESET" link. NOTE: You must update your scripts generating the XML requests if you reset the API Access information.

---

# Chapter 7. The Test Transaction Settings Section

## The Test Transaction Settings Section

This feature allows a merchant to test their order forms and ordering system to make sure that they have integrated their website with the gateway system correctly - without actually charging an account (See *Figure 7.1*). These settings can also be modified in the Testing Your Forms interface.

**Figure 7.1. Account Settings Test Section Example**

The screenshot shows a dark grey header bar with the text "TEST TRANSACTION SETTINGS" in white. Below the header, there are two main sections. The first section is labeled "TEST MODE:" and contains a checkbox that is currently unchecked, followed by the text "Check to turn ON.". The second section is labeled "FIRST NAME:" and contains a text input field with the value "Test123". Below these sections, there is a label "DEMO ACCOUNT INFORMATION" in a smaller font.

- **The Test Mode Checkbox** - This should only be selected if a merchant wants all transactions processed as TEST transactions. By default, this is unchecked. When checked, any transactions will run as TEST transactions and will not be processed or charged. Any transactions submitted as TEST transactions will not show up in the Transaction Listing or Transaction Detail interfaces.
- **The Test User First Name** - When the entry in this field is passed as the customer's first name, the transaction will be processed as a TEST transaction. Do not use a real name, instead use something like "Test123".

---

# Chapter 8. The Customer Confirmation Email Settings Section

## The Customer Confirmation Email Settings Section

This feature allows a merchant to select/deselect which emails are sent to the email provided by the customer at the time of the transaction (*See Figure 8.1*). Many merchants who use a shopping cart system prefer that the shopping cart sends a confirmation, rather than the gateway. In that case, they remove the check marks. All emails are set to be sent by default, except for the AVSOnly and Pre-Auth emails. The HELP menu reminds a merchant what each of the emails indicate.

**Figure 8.1. Account Settings Customer Email Section Example**



---

# Chapter 9. The Fraud Control Settings Section

## The Fraud Control Settings

These settings are provided as additional protection against potential fraud (See Figure 3.32). Each of these features are optional. A merchant may use as many of these features as they desire. None of these features can completely prevent all types of fraud, but these are some of the most powerful anti-fraud options available on any gateway software available today.

Figure 9.1. Account Settings Fraud Controls Example

- **Allow Credits With No Prior Sale** - When this is selected, a merchant can log into the Control Panel and utilize the Post A Credit interface to put money into the credit card account of a customer. The interface does not function correctly unless this checkbox is marked. For more information on the Post A Credit feature, please see [THIS](#)
- **Allow Refunds Via The Transaction Listing** - This should be enabled if a merchant wants to be able to refund past transactions without having to enter the customer's information in the Transaction Listing or Transaction Detail Options area.
- **Refunds Greater Than Sale** - This checkbox, when selected, allows a merchant to generate refunds for a larger amount than the original payment made by the customer.
- **Resubmit Greater Than Sale** - This allows a merchant to generate a charge to a past customer without having to re-enter the customer's information. This should be enabled if a merchant would ever possibly "re-bill" a past customer for an amount larger than the original sale. The feature does not effect Recurring transactions, only Resubmit transactions.
- **IP Filter Settings Interface** - This allows a merchant to access the IP Filter Management window (See Figure 3.33). This interface allows a Merchant utilizing the HTML or XML connection methods to limit transaction submissions to the IP address/range of a specific server. This is required for

XML connection users and optional for HTML users. If used with HTML, be sure to activate the "Restrict Order By IP" feature. The HTML Transproc Module is used for HTML based transactions. The XMLTrans module is used for XML. The status must be set to Active. To delete an IP address, click the "GO" button in the Delete Column.

**Figure 9.2. IP Filter Settings Example**

<b>IP FILTER MANAGEMENT</b>						Modules: <a href="#">XML</a>   <a href="#">HTML</a>
GATEWAY ID	IP ADDRESS ENTRY	STATUS	MODULE	APPLY	DELETE	
66646	<input type="text" value="0.0.0.0"/>	Active <input type="button" value="v"/>	TRANSPROC	<input type="button" value="go"/>	<input type="button" value="go"/>	
66646	<input type="text"/>	Active <input type="button" value="v"/>	XML (xmltrans) <input type="button" value="v"/>	<input type="button" value="go"/>		

If you are allowing credit/void transactions from your software or are using the XML interface, you must specify the IP address(es) that are *allowed* to process transactions via your account. You may specify either single IP addresses or a range of allowable IP addresses. If you are processing transactions directly from the computer you are using now, you may visit [www.myipaddress.com](http://www.myipaddress.com) to view your current IP address.

**Examples of valid IP address entries:**

10.0.0.1	<i>Allows this ONE specific IP address. If you have a static IP address, enter it as shown here.</i>
10.0.0.1-10.0.0.255	<i>Allows the entire IP range specified. If you DO NOT have a static IP address, enter the range of IP addresses used by your ISP here. (You may need to contact your ISP to obtain this information.) For example, if your current IP address shows "10.0.0.15" you may want to enter a range of "10.0.0.1-10.0.0.255".</i>

[CLOSE](#)

[BACK](#)

- **Restrict Order By IP** - This feature allows a merchant to allow transactions only from specific IP addresses. This is activated and used by merchants who will be making all of their customers' order submissions from their own server directly to our system. When enabled, a merchant should also enter acceptable IP addresses into the IP Filter Management window using the HTML Transproc module. It should not be activated if customers will be posting to the gateway system.
- **Restrict Order Usage** - This fraud prevention module is specifically designed to reduce the number of 'testers' hitting merchants with credit card numbers attempting to find valid cards. If a transaction is received and is NOT approved, a restriction will be automatically enabled. For the next X minutes no transactions will be allowed from the IP address of the original unapproved transaction. To activ-

ate this, click the checkbox and enter an amount of time in the minutes box.

- **Proof of Life** - This feature is also known as "Captcha Verification". When activated, a page is displayed to the user with a dynamically generated image containing random characters after order submission. The user must enter these characters correctly to complete the transaction submission. If a merchant is logged into an open session of the Control Panel, and submits a transaction through their website, it will not prompt the merchant for the entry. However, if the merchant does not have an open session, they will be prompted for the entry - like a customer.
- **Allow Non-VT Sales** - This must be selected if you will be accepting transactions via order form. The only instance in which a merchant would disable this feature would be if the merchant was only using the Virtual Terminal or XML feature to manually enter transactions. If you are only accepting XML and Virtual Terminal transactions, please uncheck this box.
- **Require VT Customer ID** - This fraud prevention module gives merchants the ability to enforce the Customer ID value for Virtual Terminal Transactions if they wish to do so.
- **Reject Duplicates** - This feature will block duplicate transactions sent through the gateway. To be considered a duplicate transaction the following values must be identical to another successful transaction that has occurred in the last 24 hours. Currently this service only works with credit card transactions. The following fields are used to determine duplication:
  - Credit Card Number
  - Credit Card Expiration Month
  - Credit Card Expiration Year
  - Billing Street Address
  - Billing Zip/Postal Code
  - Order Total
- **Require Order Form UIDs** - This fraud prevention option gives merchants the ability to enforce the use of the Order Form UID for the value of the "vendor\_id" field on HTML based order forms. The value of the UID is listed in the Account Settings. The twenty character Order Form UID value is randomly generated and keeps fraudsters from guessing what ID you are using to process orders. This does not keep someone from looking at your order form and obtaining this value, but we have found that the majority of fraud is done using automated tools. So this setting keeps fraudsters from stumbling upon your account.
- **Maximum Sale** - This allows a merchant to place a cap on the highest amount that they will allow to process through their website. Often, a merchant will set this amount to coincide with the "maximum volume ticket limit" imposed on them by their credit card merchant processing bank. A customer who attempts to place a transaction which exceeds that amount will be shown an error which indicates that they've entered an invalid amount.
- **Minimum Sale** - This allows a merchant to place an "at least" amount. A customer who attempts to place a transaction which does not meet at least that amount, will be shown an error which indicates that they've entered an invalid amount.
- **Auto-Void Options** - These advanced features will automatically void a transaction that would otherwise be approved based on the merchant's own risk tolerance.
  - **The Address and ZIP Verification Auto-Void/AVS Auto-Void Setting** - All of the major credit card processors will accept transactions that do not pass AVS. The fact that processors do not reject non-AVS transactions is a great concern of ours. Because of this, we've introduced one of the first AVS Auto-Void systems for the Internet. Our system allows the software to void

transactions that are allowed through the processor without passing AVS based upon the requirement level set by the merchant. Remember, the gateway does not provide the AVS Responses. Those responses are generated by the credit card issuing bank and reported by the credit card processor based on information located in the bank's AVS database (which may or may not match the bank's statement database). However, the gateway system will perform the Auto-Void according to the requirements set by the merchant. These settings may be modified by the merchant at any time. Keep in mind, a(n) void/auto-void of an authorized transaction cancels the charge, but does not cancel an authorization. An authorization freezes funds in an account, so that a completed charge can withdraw those frozen funds. A voided authorization may "freeze" the funds in the customer's account for up to 10 days. The following levels are available:

1. **No Auto-Void** - This will allow any approved transaction to process regardless of the address verification response.
  2. **Void Unless ZIP Matches** - This will void any approved transaction for which the processor indicates that the ZIP Code entered does not match the ZIP Code listed in the bank's AVS database (even if the street address matches).
  3. **Void Unless Addr Matches** - This will void any approved transaction for which the processor indicates that the street address entered does not match the street address listed in the bank's AVS database (even if the ZIP Code matches).
  4. **Void Unless Both Match** - This setting requires that both the address and the ZIP Code match exactly what the issuing bank's AVS database has on file for the customer. If either the address or ZIP Code, or both, come back as a non-match, that approved transaction will be voided.
- **The Recurring AVS Auto-Void Setting** - This feature provides auto-voiding of recurring transactions based on the address and ZIP Code verifications returned by the processing network. Remember, the gateway does not provide the AVS Responses. Those responses are generated by the credit card issuing bank and reported by the credit card processor based on information located in the bank's AVS database (which may or may not match the bank's statement database). However, the gateway system will perform the Auto-Void according to the requirements set by the merchant. These settings may be modified by the merchant at any time. Keep in mind, a(n) void/auto-void of an authorized transaction cancels the charge, but does not cancel an authorization. An authorization freezes funds in an account, so that a completed charge can withdraw those frozen funds. A voided authorization may "freeze" the funds in the customer's account for up to 10 days. The following levels are available:
    1. **No Auto-Void** - This will allow any approved transaction to process regardless of the address verification response.
    2. **Void Unless ZIP Matches** - This will void any approved transaction for which the processor indicates that the ZIP Code entered does not match the ZIP Code listed in the bank's AVS database (even if the street address matches).
    3. **Void Unless Addr Matches** - This will void any approved transaction for which the processor indicates that the street address entered does not match the street address listed in the bank's AVS database (even if the ZIP Code matches).
    4. **Void Unless Both Match** - This setting requires that both the address and the ZIP Code match exactly what the issuing bank's AVS database has on file for the customer. If either the address or ZIP Code, or both, come back as a non-match, that approved transaction will be voided.
  - **The CVV Verification Auto-Void Setting** - The CVV code is a security feature for 'card not present' transactions (e.g., Internet transactions), and now appears on most (but not all) major credit and debit cards. This feature is a three or four digit code which provides a cryptographic

check of the information embossed on the card. Therefore, the CVV code is not part of the card number itself. This setting allows a merchant to have sale transactions automatically voided if the processing network indicates that the CVV entered does not match the CVV database at the customer's credit card issuing bank. Most issuing banks do not require a CVV number to be entered for a transaction to process. A small group of banks do require correct CVV entry for Internet based transactions. The gateway system will perform the Auto-Void according to the requirements set by the merchant. These settings may be modified by the merchant at any time. Keep in mind, a(n) void/auto-void of an authorized transaction cancels the charge, but does not cancel an authorization. An authorization freezes funds in an account, so that a completed charge can withdraw those frozen funds. A voided authorization may "freeze" the funds in the customer's account for up to 10 days. The following levels are available:

1. **No Auto-Void** - This will allow any approved transaction to process regardless of the CVV verification response.
2. **Void Unless CVV Matches** - This setting will void any authorized transaction which is returned with a non-matching or empty CVV response.
3. **Void If CVV Not Entered** - With this setting a customer's transaction will be voided if the bank indicates that a CVV code should exist on the card, but was not entered.

---

# Chapter 10. The Card Acceptance Section

## The Card Acceptance Section

This area will only display if the Card Setup has been completed. If you would like the the card acceptance script to display on a Split Form, click the "Card Processing Enabled" checkbox. By default, all US based credit card merchant accounts are established to process transactions on Visa and MasterCard. If a merchant has also established "appendage" accounts (i.e. AMEX, Discover, and Diners), a merchant must provide those merchant IDs to their Visa/MC merchant provider. Once that's complete, a merchant can update the Card Type settings by clicking on the appropriate card types (*See Figure 3.34*). A merchant can disable a card type by unchecking the card type in the same area. The selected card types will display on the secure half of the split form (if a merchant uses that method).

**Figure 10.1. Account Settings Card Acceptance Section Example**

The screenshot shows a form titled "CARD PROCESSING SETTINGS". At the top, there is a checkbox labeled "CARD PROCESSING ENABLED?" which is checked and set to "Yes". Below this, there is a section titled "Card Types You Are Authorized To Accept". Under this section, there are four checkboxes, all of which are checked: "Visa/MC:", "Amex:", "Discover:", and "Diners:". Below these checkboxes, there is a note: "Acceptance of non-authorized card types may delay settlement of funds." In the bottom right corner of the form, there is a "HELP" link.

---

# Chapter 11. The Check Processing Information Section

## The Check Processing Information Section

This area will only display if the Check Setup has been completed. If you would like the check acceptance script to display on a Split Form, click the "Check Processing Enabled" checkbox. For merchants utilizing the Check system for accepting check payments, up to four email addresses can receive the daily Check Statistics emails. Please enter the desired recipients in the interface fields in the Account Settings of the Control Panel. If you are authorized to use the NACHA processing system, the NACHA Setup fields will display. Enter the necessary values provided by your NACHA processor.

**Figure 11.1. Account Settings Check Section Example**

**CHECK PROCESSING INFORMATION**

CHECK PROCESSING ENABLED?  Yes

**NACHA Setup:**

COMPANY ID:  COMPANY NAME:

IMMEDIATE DESTINATION:  IMMEDIATE DESTINATION NAME:

IMMEDIATE ORIGIN:  IMMEDIATE ORIGIN NAME:

ORIGINATING DFI:

**RediCheck Statistics Email:**

tese@test.com

HELP

---

# Chapter 12. Style Settings Section

## Style Settings

The section is used to make the secure page of the Split form to appear the way that a merchant desires it. This can be helpful in making a transaction seem more seamless. Use of any of the supported bo-dytags will supercede any setting here.

**Figure 12.1. Account Settings Style Settings Example**

STYLE SETTINGS	
BACKGROUND COLOR: 446100	BACKGROUND IMAGE:
FONT COLOR: 00c9da	HEADER BORDER COLOR: dad100
HEADER BACKGROUND COLOR: fff33c	HEADER IMAGE: https://secure.paymentclearing.com/im
<a href="#">See Demonstration Page</a>	
<a href="#">HELP</a>	
<input type="button" value="UPDATE"/>	

- **Background Color** - This can be a six digit hexadecimal value or you can use the color bar tool to select the desired color.
- **Font Color** - This can be a six digit hexadecimal value or you can use the color bar tool to select the desired color.
- **Header Background Color** - This can be a six digit hexadecimal value or you can use the color bar tool to select the desired color.
- **Background Image** - This needs to be the absolute URL of an image. You can upload this image to the secure server by submitting a ticket at <http://support.itransact.com>.
- **Header Border Color** - This can be a six digit hexadecimal value or you can use the color bar tool to select the desired color.
- **Header Image** - This needs to be the absolute URL of an image. You can upload this image to the secure server by submitting a ticket at <http://support.itransact.com>.
- **See Demonstration Page** - This will show an example of what the layout of the form will look like. This will only display settings that have been entered and submitted by the pressing of the UPDATE button at the bottom of the interface

A helpful color bar tool is displayed when a merchant clicks into one of the color entry fields. This allows a merchant to click on the desired color and it will automatically populate the corresponding field.

**Figure 12.2. Account Settings Style Color Bar Example**

BACKGROUND COLOR: 446100	BACKGROUND IMAGE:
FONT COLOR:	<input type="color" value="#00ff00"/>

**PLEASE REMEMBER TO CLICK THE "UPDATE" BUTTON AT THE BOTTOM OF THE INTERFACE WINDOW WHEN MAKING ANY CHANGES IN THE ACCOUNT SETTINGS INTERFACE.**