

## How To Manage Fraud Settings

The PaySimple Solution 2.0 provides a number of fraud settings to limit your risk on the transactions processed through your system. Each fraud setting is described in detail below, and each can be enabled and configured to your specifications.

### Enable and Configure Fraud Settings:

1. Access the fraud settings configuration page by selecting **System Management** from main navigation, then **Fraud Settings** from secondary navigation.
2. Any module that is on will have the **Enabled** radio button selected and the **Configure** link visible. Any module that is off will have the **Disabled** radio button selected and the **Configure** link will not be visible.
3. To configure a module, make sure it is **Enabled** and click its **Configure** link. It will expand a configuration section with program settings for the fraud module. Once changes are made to the configuration screen, click the **Close** icon at the top right of the expanded section.
4. Click the **Save** button at the bottom of the page. Settings will not be saved by closing the configuration section.

Note: The system saves your custom configurations even if you need to disable a module for a period of time.

The Fraud Settings screen is divided into three sections: **ACH Settings**, **Credit Card Settings**, and **Account Settings**. You will always see the **Account Settings** section. Depending on the type of payments your account is set up to process, you will see the **ACH Settings** section, the **Credit Card Settings** section, or both.

# Configuring Credit Card Fraud Settings

## AVS Fraud Settings

An AVS query determines whether the street address and/or zip code entered in the billing address fields match the billing address the issuer has on file for the credit card holder. Performing an AVS check is required to obtain the lowest qualified rate on a MOTO transaction. However, to get the qualified rate you only need to perform an AVS check, you do not need to obtain an exact match, or any other specific response.

The default setting for AVS is **Enabled** and programmed to process for every possible response. ***There is no need to change this configuration***, unless you want to increase the security of your system (which may result in more declined transactions, because even slight variations in addresses could cause a failure result).

To turn off the **AVS** module, select the **Disabled** radio button.

To change **AVS** configuration settings:

1. Click the **Configure** link for **AVS** and the configuration screen expands
2. Uncheck any boxes for responses you want to reject (Decline the transaction if this AVS response is received).
3. Click the **Save** button at the bottom of the page.

## CVV2 Fraud Settings

The CVV2 number is a three digit (4 digit for AMEX) security code printed on a credit card (as shown below), and is used to help ensure the person authorizing a card-not-present (mail, telephone, or web payment) transaction has physical possession of the card. Having received CVV2 match verification can help you defend yourself in the event a card holder initiates a chargeback .



The CVV2 fraud module is **Enabled** and programmed to process on all responses by default. ***There is no need to change this configuration***. However, for an additional layer of security, it is a good idea to uncheck the **No Match** box, so that you do not process a transaction where you know the CVV2 is invalid (the number provided by your customer does not match the one on record for the card). See below for how to make this change.

If you want to turn off the **CVV2** module entirely, select the **Disabled** radio button. But, note that you can bypass the CVV2 check on any individual transaction by leaving the CVV2 field blank, or selecting the **CVV2 not available** radio button.

To change **CVV2** configuration settings:

1. Click the **Configure** link for **CVV2** and the configuration screen expands
2. Uncheck any boxes for responses you want to reject (Decline the transaction if this CVV2 response is received).
3. Click the **Save** button at the bottom of the page.

## Multiple Credit Cards

The **Multiple Credit Cards** setting can prevent your system from being used to test stolen credit card numbers. It works by limiting the number of different credit card numbers that can be submitted to the system for processing in a specified time frame from a specific IP Address. This module is **Disabled** by default.

**Important note for Web Payment Form users:** It is possible for criminals to direct a software program at your web form that tests thousands of stolen credit card numbers in order to find one that is valid. This can happen very quickly and without your knowledge. Each time a credit card transaction is submitted from your form, whether it is successful or declined, you are charged an inquiry fee. To prevent fraudulent activity from costing you inquiry fees, we strongly suggest enabling the **Multiple Credit Cards** module, and configuring it as detailed below. Doing so will stop this kind of attack before it can generate large amounts of fraudulent transactions.

To change **Multiple Credit Card** configuration settings:

- Click the **Enable** radio button for **Multiple Credit Cards**
- Click the **Configure** link for **Multiple Credit Cards** and the configuration screen expands
- Enter a value for **Time Period**. This is the number of minutes tracked in a session. Suggested Value: 5 minutes
- Enter a value for **Number of Cards**. This is the number of different credit card numbers the system allows to be tried in a single session. Suggested Value: 6 (Do not set this number too low or you will end up blocking valid customers who have made data entry errors when entering their credit card number).
- Click the **Save** button at the bottom of the page.

## ACCOUNT FRAUD SETTINGS

### Duplicate Detection

This setting is used to help prevent duplicate transactions from being generated by your customers clicking the “Process” button multiple times on your web payment forms, and by your employees mistakenly double clicking “Process” or entering the same transaction twice.

**Duplicate Detection** is “Enabled” on all systems by default, with a recommended one-minute delay. ***There is no need to change this configuration.*** If you want added protection against duplicates, you can increase the number of minutes in which duplicates are disallowed. However, do not make the time period too long, or you may end up blocking legitimate repeat orders.

It is strongly discouraged, but you can turn off the **Duplicate Detection** module by selecting the “Disabled” radio button.

To change **Duplicate Detection** configuration settings:

1. Click the “Configure” link for **Duplicate Detection** and the configuration screen expands.
2. In the **Time Period** field, enter the number of minutes in which you want to block duplicates.
3. Click the **Save** button at the bottom of the page.

### E-mail Blocker

You can block people from creating accounts and transactions via your web forms based on their e-mail address. For example, you can block customers from using free e-mail accounts such as hotmail. You can also use it to block e-mail addresses from companies with which you no longer wish to conduct business.

**Email Blocker** is “Disabled” by default.

To enable and change **Email Blocker** configuration settings:

1. Click the “Enable” radio button for **Email Blocker**.
2. Click the “Configure” link for **Email Blocker** and the configuration screen expands.
3. Enter an address or domain to block, for example, “joe@hotmail.com” would block all orders from that specific email address. “\*hotmail.com” would block all hotmail addresses. You can enter one email, or one domain per line.
4. Click the **Save** button at the bottom of the page.

## ZIP Code Verifier

The **Zip Code Verifier** module is used to determine whether a zip code is valid for the state, city and/or area code entered in the address fields. While it can only validate US addresses, it can be used with billing address and/or shipping address. This is very helpful in assisting your customers and your employees in finding data entry errors before a transaction is entered into the system for processing.

**Zip Code Verifier** is “Disabled” by default.

To enable and change **Zip Code Verifier** configuration settings:

1. Click the “Enable” radio button for **Zip Code Verifier**.
2. Click the “Configure” link for **Zip Code Verifier** and the configuration screen expands.
3. In the **Verify Billing Zip Code** column, check the boxes for the verifications you want. (Note that checking “Area Code” may result in failed validations if people provide work or cell phone numbers with area codes that do not match their billing address.)
4. In the **Verify Shipping Zip Code** column, check the boxes for the verification you want. (See note on “Area Code” above.)
5. If you want to accept orders for non-US addresses, check the “Accept orders from zip codes not in database” box.
6. Click the **Save** button at the bottom of the page.

# Configuring ACH Fraud Settings

## Routing Number Verification

All accounts set up for ACH processing have **Routing Number Verification** enabled by default, and cannot be turned off. This means that the routing number is verified for all ACH transactions automatically, ensuring that your transaction will always reach an actual bank.

## Check Verification

**Check Verification** is available for ACH merchant accounts at time of set-up. If you see this option in your **ACH Fraud Settings** section, then it is available to you. If this setting is not available and you would like it, contact your account executive to have it added to your account.

**Check Verification** is “disabled” by default. When you “enable” it, every transaction run through the system will incur an additional check verification fee. When it is disabled, this fee will not apply. You must enable or disable **Check Verification** at the system level, but you can turn it on and off at will.

The system will return one of three check verification responses:

- *Verified*: The account # is valid and the system indicates that the transaction will be successful.
- *Rejected*: The account # is not valid, or the system has reason to believe that the account is not in good standing.
- *Unknown*: The system has no information about the account. (This does not necessarily mean a bad account number—it may mean the bank holding the account is not included in the queried database.)

To configure your system to either process or fail the transaction based on the Check Verification response:

1. Select the **Enable** radio button for **Check Verification**
2. Click the **Configure** link for **Check Verification**
3. The configuration screen expands
4. In the **One Time Payment** column, for each possible verification response check the **Process Payment** box if you want to submit the payment upon that response. **Verified** is checked by default, and cannot be unchecked.
5. Do the same in the **Recurring Payment** column.
6. Click the **Save** button at the bottom of the page.

**PaySimple Support:** 800.466.0992