

# Fraud Prevention Settings

Last Modified on 12/19/2022 2:35 pm PST

Go to **Administration**, click on **Settings**, and then select **Fraud**.

The Fraud tab allows you to configure your Fraud Settings for our products. The Fraud options that can be configured are Duplicate Transaction Blocking, Transaction Limits, Client IP Address Velocity, and Do Not Disturb. These settings can help prevent a carding attack.

Within the Fraud tab, you can *View History* of changes, *Save Changes*, and *Reset* the default settings. Additional fraud settings for Address Verification and Card Verification Values can be configured in [Payment Profiles And Settings](#).

## Duplicate Transaction Blocking

We will reject a transaction within the duplicate window, regardless of which our product is used to process the transactions. Duplicate Transaction Blocking helps prevent your customers from clicking submit multiple times when there is a potential Internet delay in processing. To use Duplicate Transaction Blocking, enter the *Duplicate Window (in seconds)* for your transactions.

Once the Duplicate Window time frame is set, the following fields can be selected for duplicate blocking:

1. *Account Number* - defaulted on.
2. *Transaction Amount* - defaulted on.
3. *Merchant Reference Number* - defaulted off. To add, click on the checkbox and select **Save Changes**.
4. *Purchase ID* - defaulted off. To add, click on the checkbox and select **Save Changes**.

## Transaction Limits

We will reject transactions with amounts less than the minimum or greater than the maximum amount. These limits apply to any of our products used to process transactions.

The following fields can be configured for transaction limits:

1. Enter a transaction floor in the *Reject if transaction amount is less than* field, and select **Save Changes**.
2. Enter a transaction ceiling in the *Reject if transaction amount is greater than* field, and select **Save Changes**.

## Client IP Address Velocity

We will place a specific IP address in a block list for 24 hours should that IP address exceed the user-specified threshold (attempts) within the configured time frame. This block will persist for 24 hours even if the feature is disabled after the fact.

To configure Client IP Address Velocity:

1. Click the **Velocity Check** toggle, so it turns *green*.
2. Enter the desired timeframe (in seconds) in the *Timeframe* field.

3. Enter the desired threshold (attempts) that the system will allow before placing the IP address in a block list in the *Threshold* field.
4. Select **Save Changes**.

**Note:** *Client IP Address Velocity only applies to our Embedded Fields, Checkout, and Payment Gateway products at this time.*

## Do Not Disturb

Do Not Disturb will disable your payment processing capabilities for all our products during a specified time frame. The Do Not Disturb feature is helpful if you know you will not be processing payments during the set timeframe.

1. Click the **Do Not Disturb** toggle, so it turns *green*.
  2. Specify the start time for the **Do Not Disturb** feature in the first row labeled *From*.
  3. Specify the end time for the **Do Not Disturb** feature in the second row labeled *To*.
  4. Select **Save Changes**.
-