

NOFRAUD PORTAL  
GUIDE

**NO**  **FRAUD**

This document serves as a guide to the NoFraud Portal account to ensure proper configuration and enable merchant functions and overview of all transactions running through the NoFraud system.

## Overview

The NoFraud Portal is the merchant's access to all things pertaining to their NoFraud configuration. Each client is required to set up an account prior to testing. The portal serves as a dashboard for merchants where they can exercise control through the multiple functions available to them. Through the portal, each merchant has access to a transaction section, whitelist, blacklist, resources, account settings and a few other functions. This paper serves as an explanation of each section in the portal.

Before you go live or begin testing you first need to set up your portal account to ensure proper configuration. You are required to save information under the account, integration and setting tabs. For that purpose, we will first walk you through the account information tabs.

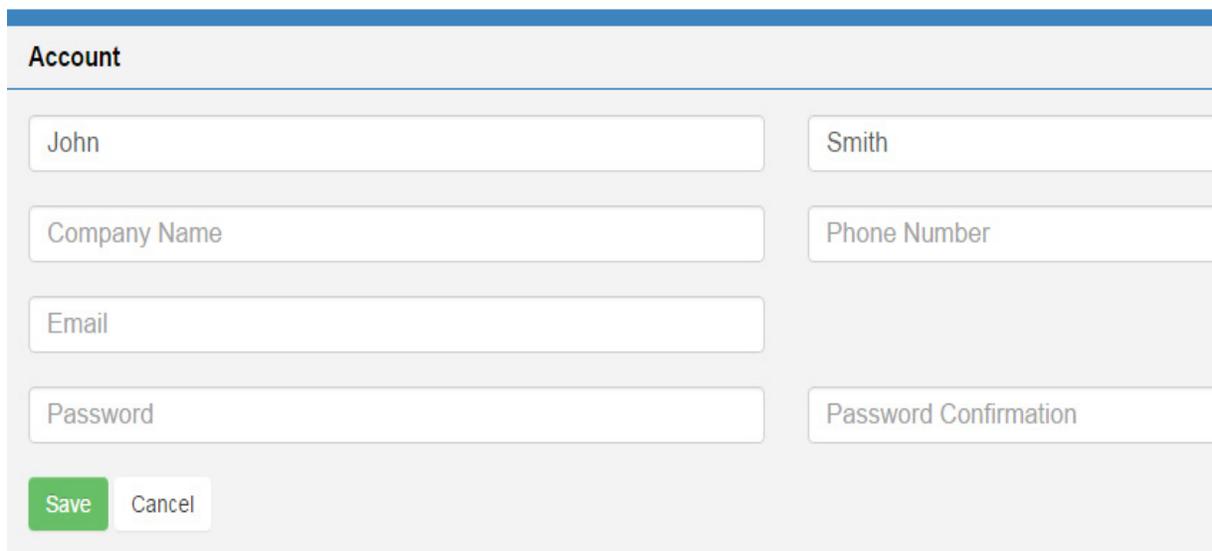
## Account Information

On the bottom left of your portal account, you have access to 4 different tabs that require merchant information input.

Please follow each tab instructions:

### Account

The first sub-section on the bottom left of your portal account. Fill out the basic information and save.

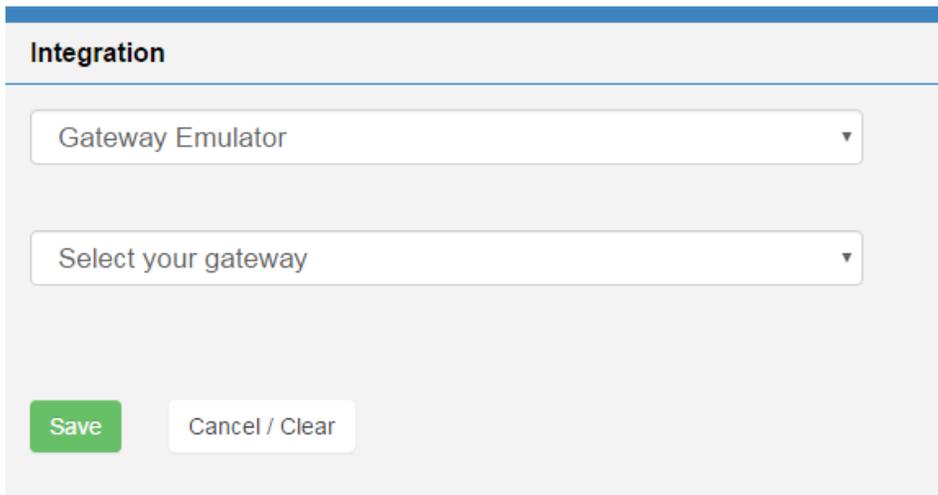


The screenshot shows a web form titled "Account" with a blue header bar. The form is divided into two columns of input fields. The left column contains fields for "First Name" (with the value "John"), "Company Name", "Email", and "Password". The right column contains fields for "Last Name" (with the value "Smith"), "Phone Number", and "Password Confirmation". At the bottom left of the form, there are two buttons: a green "Save" button and a white "Cancel" button.

1. First Name
2. Last name
3. Company Name - This should reflect the company name as customers recognize it because it is used for verification purposes.
4. Phone Number
5. Email - must be unique.
6. Password - you can reset your password here anytime.
7. Password confirmation.

## Integration

Through this tab, you will select which method of integration you are using.



The image shows a form titled "Integration" with a blue header. It contains two dropdown menus. The first dropdown menu is currently set to "Gateway Emulator". The second dropdown menu is currently set to "Select your gateway". At the bottom of the form, there are two buttons: a green "Save" button and a white "Cancel / Clear" button.

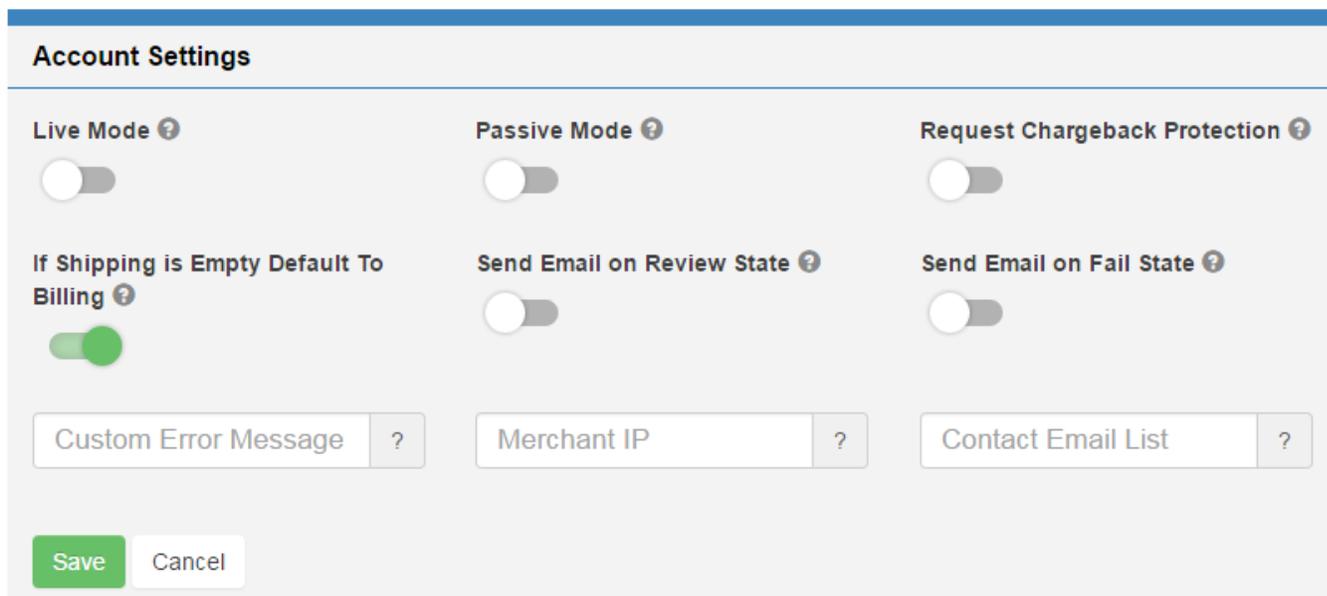
Methods of integration:

- Gateway Emulator -- You are required to select your gateway and fill out your gateway credentials.
- Plugin -- An API Key is generated automatically for your integration.
- Direct API -- An API Key is generated automatically for your integration.

Depending on your method selection, specific instructions ('Integration Tips') will appear at the bottom of the page to assist you with the integration.

## Settings

Merchants can disable and enable certain functions. We recommend that these changes only be made by an authorized account holder or the admin of the account. For the purpose of this illustration we enabled all functions, they are disabled by default unless you are a Shopify user.



The image shows a form titled "Account Settings" with a blue header. It contains several settings:

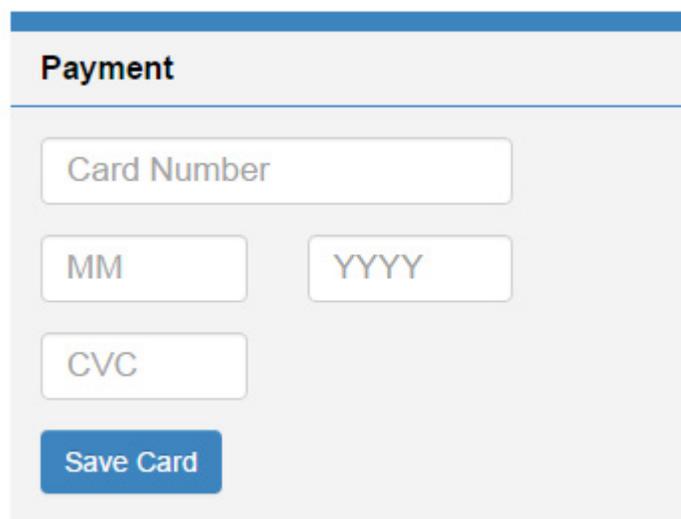
- Live Mode**: Disabled (toggle switch).
- Passive Mode**: Disabled (toggle switch).
- Request Chargeback Protection**: Disabled (toggle switch).
- If Shipping is Empty Default To Billing**: Enabled (toggle switch).
- Send Email on Review State**: Disabled (toggle switch).
- Send Email on Fail State**: Disabled (toggle switch).
- Custom Error Message**: Text input field with a question mark icon.
- Merchant IP**: Text input field with a question mark icon.
- Contact Email List**: Text input field with a question mark icon.

At the bottom of the form, there are two buttons: a green "Save" button and a white "Cancel" button.

1. Live Mode - Turn on to take your account out of test mode and go live.
2. Passive Mode - Turn on to have NoFraud render decisions on your orders without affecting the process. (All orders are sent directly to the gateway, even if NoFraud failed it.) This is used to observe NoFraud's process without it affecting your orders. You can make internal decisions based on the NoFraud status.
3. Remove Chargeback Protection - By disabling this function, you are turning off the chargeback protection guarantee.
4. If Shipping is Empty Default to Billing - If an order's shipping address is empty, use the order's billing address as the shipping address. This function is only relevant to physical goods and not services.
5. Send Email on Review State - Receive a notification for each order that NoFraud reviews.
6. Send Email on Fail State - Receive a notification for each order that NoFraud fails.
7. Custom Error Message - Customize the error message customers see in your cart when they get denied by NoFraud.
8. Merchant IP Address - The IP address of the store or physical location that you will be taking phone orders from (Multiple IP addresses can be entered separated by comma.) This information allows us to differentiate between orders placed over the phone and those that are placed from the customer browser.
9. Contact Email List - A list of emails to receive the NoFraud notifications. Separate each email address with a comma.

## Payments

To automate the billing process each month, please enter the following payment information.



The image shows a payment form with a blue header bar containing the word "Payment" in bold. Below the header, there are several input fields: a large field for "Card Number", two smaller fields for "MM" (month) and "YYYY" (year), and a field for "CVC". At the bottom of the form is a blue button labeled "Save Card".

1. Card Number - The credit card number that will be charged the balance of each month.
2. Card Expiration Month - Credit card's expiration month (two digits).
3. Card Expiration Year - Credit card's expiration year (four digits).
4. CVC - Credit card's security code (Usually found on the back of the card consisting of three or four numbers.)
5. Remember to click 'Save Card'.

## Transactions

The purpose of the transaction section is to provide a general overview of all transactions running through NoFraud. See the image below:

Transactions													
Q Transaction Search		Status ▾ clear filters										Filter by Date	
	Time	NF	Gateway	Transaction ID	Customer	Card	Amount	Billing	Shipping	AVS	CVV		
open	NOV 25 04:44pm	<b>Fail</b>		101217357 ebbp08wp	LEAR21630 SOLARES	Mastercard 2692	\$69.95	8020 NW 60TH ST. 33195	8020 NW 60TH ST. 33195	N	M		
open	NOV 25 04:44pm	<b>Fraudulent</b>	Pass	746004718 7sjyqg2	Teresa Brown	Visa 6159	\$112.00	1531 Elderberry 44077	1531 Elderberry 44077	D	M		
open	NOV 25 04:43pm	<b>Fraudulent</b>	Pass	a9pi1y 5ex4tr3n	Audee Nelson	Visa 4135	\$278.63	6801 Spencer Cir 33610	6801 Spencer Cir 33610	N	M		
open	NOV 25 04:43pm	<b>Fraudulent</b>	Pass	SP-370188 lfa0ck0i	Debra Hubert	Visa 5160	\$131.94	247 third avenue 95062	247 third avenue 95062	Y	M		
open	NOV 25 04:43pm	<b>Fraudulent</b>	Pass	746004717 b1qndg3h	Cheryl Krueger	Amex 1007	\$83.35	507 Enchanted Oa 78121	507 Enchanted Oa 78121	M			

Through this general overview, you will see the following transaction information:

1. Date/Time that the order was received.
2. NoFraud's decision. (see terminology page for decision details)
3. Gateway's response.
4. Transaction ID .
5. Customer Name.
6. Card Information.
7. Amount – the cost of goods purchased.
8. Billing Information.
9. Shipping Information.
10. AVS Result.
11. CVV Result.

Each order can be opened and viewed in greater detail. See image below of an open order.

Based on the field result, the color will vary for each section:

- The NoFraud result section will be green if it passed, yellow if it's in review, and red if it failed.
- The Gateway result section follows the same pattern as the NoFraud result section.
- The Transaction section is based on the CVV result. If it's a match, the box will be green; if it's not a match, it'll be red.
- The Billing section is based on AVS. If the address is a full match, the box will be green; if it's a partial match, it'll be yellow; if it fully doesn't match, it will be red.
- The Shipping section will be green if it is shipping to the AVS-verified address either partially or fully (for example, if it ships to a house with the same ZIP, it'll be green); if it ships to a completely different address, the box will be red.
- IP Geolocation is always blue.

The map will mark the shipping and billing location so you can easily visualize the distance between the cardholder (assuming the AVS is verified) and the person it is shipping to.

Note: If there is no IP on an order or if the shipping is the same as the billing, geolocation does not appear on the map.

# NO FRAUD

- Transactions
- Whitelist
- Blacklist
- Phone Order
- Resources

Mendel Schneerson

- Account ■
- Integration ■
- Settings ■
- Payment ■
- Sign Out

## Transaction - pe4y3rjd Report Fraud

NoFraud	
Date Created	NOV 28 1:17pm
Action	✔ pass
Merchant	testing
Gift Card	No
Passive Transaction	No
Chargeback Protection	Yes

Gateway	
Gateway	Direct API
Action	Pass
Gateway Time	914 ms
Result Code	
Message Code	
Message Text	
Auth Code	
Transaction ID	

Transaction	
Amount Total	\$94.05
Shipping Cost	\$0.00
Invoice Number	87t5gt
IP Address	74.72.241.154
Card Type	Visa
BIN Match	NA
Last 4 of Card Number	1111
AVS	N
CVV	M

Billing 	
Name	Kallyn Sharott
Company	
Address	47-50 Van Dam Street Long Island City
State / Region	NY
Zip	11101
Country	US
Phone	
Email	sharottkallyn@yahoo.com

Shipping 	
Name	Kallyn Sharott
Company	
Address	47-50 Van Dam Street Long Island City
State / Region	NY
Zip	11101
Country	US

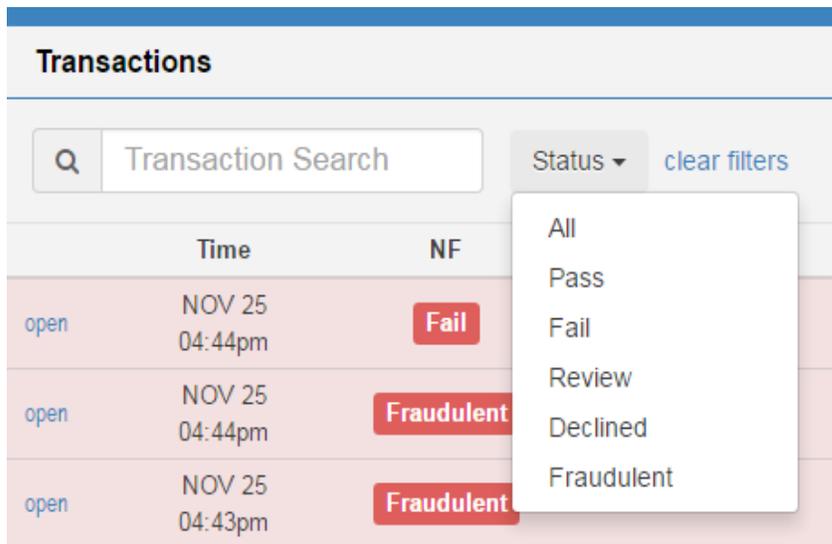
IP Geolocation 	
Distance From Billing	0
Match Billing Country?	Yes
IP Country	US
IP Region	NY
IP City	Long Island City
Proxy?	No
Corporate Proxy?	No
ISP	Time Warner Cable
IP User Type	residential

### Location Map

© 2017 NoFraud | NoFraud.com | Resources

## Transaction Filters

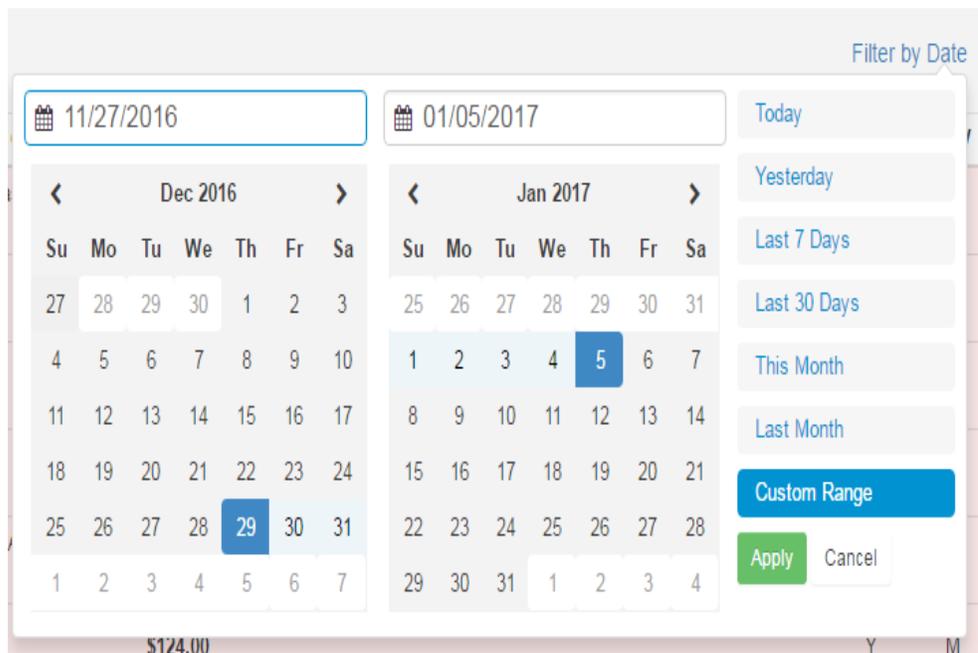
There are a few filters that can provide a more limited view of the transaction page. The dropdown icon allows you to view transactions based on status. The search bar allows you to filter all transactions based on any data entered. For example, if you want to search a specific IP, type it in and all orders matching your request will be pulled up.



The screenshot shows the 'Transactions' interface. At the top, there is a search bar labeled 'Transaction Search' and a 'Status' dropdown menu. The dropdown menu is open, showing options: All, Pass, Fail, Review, Declined, and Fraudulent. Below the search bar, there is a table with columns for 'Time' and 'NF'. The table contains three rows of transaction data:

	Time	NF
open	NOV 25 04:44pm	Fail
open	NOV 25 04:44pm	Fraudulent
open	NOV 25 04:43pm	Fraudulent

The calendar view allows you to pull up transactions within certain dates. You can set the criteria by clicking each box and selecting the date desired on the calendar. The system will automatically set the page to show the transactions within the time frame selected.



The screenshot shows the 'Filter by Date' overlay. It features two calendar views: 'Dec 2016' and 'Jan 2017'. The date range is set from 11/27/2016 to 01/05/2017. The 'Dec 2016' calendar shows the 29th selected. The 'Jan 2017' calendar shows the 5th selected. On the right side, there are buttons for 'Today', 'Yesterday', 'Last 7 Days', 'Last 30 Days', 'This Month', and 'Last Month'. At the bottom, there are 'Apply' and 'Cancel' buttons.

## Transaction Terminology

Each transaction has its corresponding NoFraud status and Gateway response visible on the order in the portal. Here is a breakdown of what each term means:

The NoFraud Decision appears under 'NF' by each transaction and can be either of the following results: Pass, Fail, and Review.

Fail - Transactions that fail have been deemed fraudulent and are not sent to the gateway. A generic message is sent to the customer while they are in the cart. This gives legitimate customers the chance to rectify any error(s) and resubmit the order.

Review – This is the status for when the system is unable to make an automatic decision based on the data received. These transactions will be held in a review state in the portal. An internal investigation is conducted by NoFraud. Most investigations are cleared up within 2 hours although they may take up to 48 hours, depending on how difficult it is to reach the cardholder. NoFraud will only use contact information that is known to be linked to the cardholder. Merchants are notified and periodically updated throughout the investigation. Once a decision is made, NoFraud will change the status in the portal to either Pass or Fraudulent. Merchants have the ability to make these decisions and change the status on their own. \*Note: the Chargeback Protection Feature does not cover orders that were passed by the merchant.

Pass – The transaction has been deemed legitimate and is directed to the gateway. Merchants have the ability to change the status of these orders to fraudulent if they are notified that the transaction carries high risk. These changes should be reported to NoFraud so that we can flag the information to ensure all future attempts from that customer are futile.

The Gateways response appears under 'Gateway' by each transactions and can be either of the following results: Fail, Pass, and Error.

All orders passed by NoFraud are automatically directed to the gateway for processing. However, the Gateway can decline the transaction based on data errors, rendering an 'Error' or 'Fail' decision. Being that these are payment processing errors, NoFraud has no control over the decisions. We recommend that the cardholder reach out to their bank with questions on Gateway fails or errors.

Pass – the payment has been successfully authorized.

Please notify your account manager of all status changes made on the merchants end.

## Blacklist / Whitelist

Blacklist: All orders that match any entries on this list will automatically get declined by NoFraud and not sent to the gateway.

Whitelist: All orders that match any entries on this list will automatically pass NoFraud and get sent to the gateway.

We don't suggest using the blacklist frequently as it can obstruct unrelated attempts with similar credentials. IPs are typically interchangeable and many customers use the same forwarding companies as their shipping address. We recommend only authorized users and the account admin control this section.

### BlackList

Email

	Created At	Field	Value	
<input type="button" value="✕ Delete"/>	JAN 9 05:08pm	Email	jane@jane.com	<a href="#">edit</a>

### WhiteList

Email

	Created At	Field	Value	
<input type="button" value="✕ Delete"/>	JAN 9 05:08pm	Email	john@john.com	<a href="#">Edit</a>

1. Field Type - Type of information that NoFraud will check to see if an order is on the blacklist. (Types: Email, IP address, Phone, Name, Address)
2. Field Value - The data that the checked field will be compared to. I.E. if you want to allow a specific IP address, select field type IP address and enter the blacklisted IP address in the field value and press save. It will now show up in the Rule Table. Name is constructed as (billing first name billing last name) Address is constructed as (address city, state zip).
3. Rule Table - List of rules you have created to allow orders.
  - a. Created - When the rule was created.
  - b. Field Type
  - c. Field Value
  - d. Edit - Edit the rule
  - e. Delete - Delete the rule.

## Questions About the Portal?

NoFraud offers excellent support to help guide you through every step of the way. Our team of experts are ready to answer any questions you may have regarding your NoFraud Portal Account.

### Contact Information:

Blumi Gross: Fraud Analyst  
Email: [blumi@nofraud.com](mailto:blumi@nofraud.com)  
Phone: 888-773-3669 EXT 103

Mendel Schneerson: Developer  
Email: [mendel@nofraud.com](mailto:mendel@nofraud.com)  
Phone: 888-773-3669 EXT 111