

# iSpyFraud – Detailed Overview

iSpyFraud is a rule-set based fraud management utility that allows merchants to configure extensive filters to help them in detecting fraud and screening suspicious transactions. iSpyFraud's extensive reporting system gives merchants a quick and easy way to review transactions, block suspicious activity, and zero in on malicious users. iSpyFraud looks at transactions both before and after processing and can decline transactions before and after authorization. The successful implementation and reduction in chargebacks across numerous merchants has been a testament to the effectiveness of this product.

## iSpyFraud General Tab

### iSpyFraud Overview

The Welcome Screen gives you some basic information about what iSpyFraud does. Notice the Tabs at the top which browse to different sections inside the fraud console.



#### Welcome to the iSpyFraud™ Fraud Protection program.

Used as a first line of defense against the most common types of fraud, this program will help you define what transactions you will and will not accept.

To navigate the system, use the tabs at the top of the page. A brief overview of what each section does follows:

- **Thresholds:** This page allows you to set the parameters of your fraud protection, based on the amount of money charged per transaction, the number of transactions charged, etc.
- **User Ban:** This page allows you to ban specific users, by the IP address of their computer, by their credit card number, by country, or by their user information in your system.
- **Exceptions:** This page allows you to make exceptions to the fraud ban system for users you know are legitimate.
- **Waiting Review:** Transactions that have been flagged as possibly fraudulent will appear on this page, waiting for your review. If you find them harmless, do nothing. If you believe the transactions are fraudulent, you may cancel the charges put through by going to your gateway.
- **History Log:** This page allows you to see recent transactions performed, with a color-coding chart for easy reference as to whether the transaction was accepted, denied, etc.

More specific instructions will be found on each page.

# iSpyFraud – Detailed Overview

## iSpyFraud Thresholds Tab

### Dynamic Building of Fraud Scrubbing Rules

At a Glance, you can view some of the rule building controls. You can create both “Flag For Review” or “Deny” rules. Furthermore, you can differentiate between Attempted and Approved transactions. This gives you the flexibility of keeping someone from trying to spin credit cards and detecting it before they get *any* transactions approved.

This page allows you to set the parameters of your fraud protection. For example, you may choose to limit the amount charged in a single transaction, or in a day or week. Or, you may limit the number of transactions performed in a day or week. These transactions can be linked to either a credit card number or an IP address. You may also limit the number of times a user can input a different credit card number for transactions. These transactions can be set by either any attempted or only approved transactions.

Choose whether to review these suspicious transactions, or deny them outright. Click the “Update” button to put your Limit Rule in place. You will find your current rules in the “View/Delete Limit Rules” section. You may also edit the current rules by changing the parameters in the “Add/Edit A Limit Rule” section, and then clicking the “Update” button.

#### Add/Edit Credit Card Rules

- If single transaction amount exceeds \$  then Flag for Review
- If daily  transaction amount for CC exceeds \$  then Flag for Review
- If daily  transaction count for CC exceeds  then Flag for Review
- If weekly  transaction amount for CC exceeds \$  then Flag for Review
- If weekly  transaction count for CC exceeds  then Flag for Review
- If user changes credit card over  times for  transactions then Flag for Review
- If first  digits of CC match over   transactions then Flag for Review

#### Add/Edit IP Address Rules

- If daily  transaction amount for IP exceeds \$  then Flag for Review
- If daily  transaction count for IP exceeds  then Flag for Review
- If weekly  transaction amount for IP exceeds \$  then Flag for Review
- If weekly  transaction count for IP exceeds  then Flag for Review

#### View/Delete Limit Rules

# iSpyFraud – Detailed Overview

## User Ban Tab

### Static Rule Banning / Blacklisting

Along with Dynamic rules as specified above, you can also input Static rules such as banning specific countries, IP Address Ranges, Credit Card Numbers, E-Mail Addresses, etc...

#### IP Addresses

IP Address: ... (ban a single IP)

Complete Class C: ...\* (ban 255 IPs from the same block)

Complete Class B: ..\*.\* (ban 65,025 IPs from the same block)

IP Address Range: ... - ...  
(ban a range of IPs you specify)

Number of Days to Ban:  (Leave blank to keep forever)

Description:

Take Action:  Ban  Flag for Review

#### Credit Cards

In the Credit Card field, you may use '?' and '\*' characters to match more than one credit card at a time. '?' will match any single character, while '\*' will match any number of characters. For example, with '41234567890123??', any 16-digit credit card number beginning with '41234567890123' will match (the last two digits may be any number). Furthermore, with '4123456789\*', any number of at least 10 digits starting with '4123456789' will match. You may ban a given bank or BIN range by simply entering the first 6 digits of the card followed by '\*', e.g. '411111\*'.

Credit Card:

Number of Days to Ban:  (Leave blank to keep forever)

Description:

Take Action:  Ban  Flag for Review

#### Geographical Information

Country:

# iSpyFraud – Detailed Overview

## Waiting Review Tab

### Review Transactions Marked as Suspicious

The Waiting on Review Tab allows you to view any transactions that have been flagged as suspicious. From here, you can cancel or approve transactions. This dashboard will also tell you what rule(s) have been triggered that caused the transaction to be flagged as suspicious.

#### How to use this page:

Click the "History" links in yellow next to the user ID, the credit card number, and the IP address in order to view the recent history of each. You may, if you wish, click the red links to ban a single credit card, a whole bank sequence, a single IP address, or a whole Class C block.

After you have reviewed the transaction, put a checkmark in the 'Review Complete' box. At any time, click 'Clear Reviewed Transactions' to remove all checked transactions. Click the 'Clear All Transactions' button to mark all transactions across all pages as reviewed.

Clear Reviewed Transactions

Clear All Transactions

Sort By: [\[User ID\]](#) [\[Date\]](#) [\[Credit Card\]](#) [\[Amount\]](#) [\[IP\]](#) [\[Country\]](#) [\[Exceeded Threshold\]](#)  
Pages: [\[View All\]](#), [\[1\]](#), [\[2\]](#), [\[3\]](#), [\[4\]](#), [\[5\]](#), [\[6\]](#), [\[7\]](#), [\[8\]](#), [\[9\]](#), [\[10\]](#), [\[11\]](#), [\[12\]](#), [\[13\]](#), [\[14\]](#), [\[15\]](#), [\[16\]](#)  
Viewing: 1 - 50 of 797

		Review Complete <input type="checkbox"/>
Transaction ID:	<a href="#">454812259</a>	
Result:	Attempted	
Customer Name:	Bienvenido David	
Order ID:	O-1000	
User Identifier:	<a href="#">bdavid@veteransadvantage.com</a> <a href="#">[History]</a> <a href="#">[Whitelist User ID]</a>	
User Email:	<a href="#">bdavid@veteransadvantage.com</a> <a href="#">[History]</a> <a href="#">[Whitelist User Email]</a>	
Time:	12/06/2007 09:51:37 PM UTC	
Credit Card Number:	4...1111 <a href="#">[History]</a> <a href="#">[Ban Credit Card / Credit Card Group]</a> <a href="#">[Whitelist Credit Card]</a>	
Amount:	\$100.00	
IP Address:	<a href="#">68.236.182.179</a> <a href="#">[History]</a> <a href="#">[Ban Single IP / Class C]</a> <a href="#">[Whitelist Single IP]</a>	
User Country:	US	
Threshold Exceeded:	Daily Attempted Transaction Amount for CC Exceeds Limit (\$100.00)	
	<a href="#">Show Details for this CC/IP:</a>	
		Review Complete <input type="checkbox"/>

# iSpyFraud – Detailed Overview

## History Log Tab

### Full audit history of all transactions – scrubbed or not

Lastly, you can use the History tab to review all transactions. This is helpful when trying to understand and determine fraud patterns. You will be able to see all approved, whitelisted, blacklisted, reviewed, and declined transactions. You can search by IP Address, Transaction ID, etc... to look for obvious patterns.

This page allows you to see recent transactions performed. Transactions will appear in green (accepted), yellow (under review), blue (an exception has been made) or red (transaction denied). Where a magnifying glass icon appears, you may click it for more details.

Accepted Review Denied Exception

You may also search by Transaction ID, User ID, credit card number, email address, IP address or by date and time.

Search \_\_\_\_\_

Transaction ID

Email

Credit Card

IP Address

Begin Time 01 ▾ 01 ▾ 2007 ▾ 12 AM ▾

End Time 12 ▾ 19 ▾ 2007 ▾ 11 PM ▾

Date (UTC)	Trans. ID	Email	Credit Card	Amount	IP Address	Country	Response	Last Action
12/06/07 21:51	<a href="#">454812259</a>	<a href="#">bdavid@veteransadvantage.com (ban)</a>	<a href="#">4...1111 (ban)</a>	100.00	<a href="#">68.236.182.179 (ban)</a>	US	Review	Attempted
12/06/07 21:14	<a href="#">454801499</a>	<a href="#">bdavid@veteransadvantage.com (ban)</a>	<a href="#">4...1111 (ban)</a>	100.00	<a href="#">68.236.182.179 (ban)</a>	US	Approved	Attempted
11/21/07 16:17	<a href="#">430270073</a>		<a href="#">4...1111 (ban)</a>	1000.00	<a href="#">68.236.182.179 (ban)</a>	US	Denied	Attempted
11/20/07 09:17	<a href="#">428155683</a>	<a href="#">colin@echelondata.com (ban)</a>	<a href="#">4...0771 (ban)</a>	80.77	<a href="#">72.32.184.52 (ban)</a>		Review	Attempted
11/20/07 02:11	<a href="#">427585790</a>	<a href="#">colin@echelondata.com (ban)</a>	<a href="#">4...0771 (ban)</a>	80.77	<a href="#">72.32.184.52 (ban)</a>		Approved	Attempted
11/19/07 22:45	<a href="#">427218195</a>	<a href="#">colin@echelondata.com (ban)</a>	<a href="#">4...1111 (ban)</a>	8.90	<a href="#">72.16.141.98 (ban)</a>		Approved	Attempted
11/19/07 12:13	<a href="#">426304286</a>	<a href="#">colin@echelondata.com (ban)</a>	<a href="#">4...0771 (ban)</a>	80.77	<a href="#">72.32.184.52 (ban)</a>		Review	Attempted
11/19/07 12:01	<a href="#">426300565</a>	<a href="#">colin@echelondata.com (ban)</a>	<a href="#">4...0771 (ban)</a>	80.77	<a href="#">72.32.184.52 (ban)</a>		Approved	Attempted
11/10/07 13:55	<a href="#">412980312</a>	<a href="#">colin@echelondata.com (ban)</a>	<a href="#">4...0771 (ban)</a>	80.77	<a href="#">72.32.184.52 (ban)</a>		Approved	Attempted
10/20/07 04:00	<a href="#">398427318</a>	<a href="#">kucag@mail.com (ban)</a>	<a href="#">5...7442 (ban)</a>	78.44	<a href="#">72.32.184.52 (ban)</a>		Approved	Attempted