



# iSpyFraud Detailed Guide

- What is iSpyFraud?..... 2
- Basic Uses ..... 2
- Getting Started..... 2
- General Tab..... 3
- Thresholds Tab ..... 4
- User Ban Tab ..... 5
- Exceptions Tab ..... 7
- Waiting Review Tab..... 8
- History Log Tab..... 9
- Frequently Asked Questions ..... 11

## What is iSpyFraud?

Welcome to the detailed user guide for iSpyFraud, a rule-set based fraud management utility that allows merchants to configure extensive filters to aid in the detection of fraud by screening transactions throughout the processing lifecycle. As it operates in real time, iSpyFraud can decline transactions both before and after authorization, which can potentially mitigate high chargeback volume and offer merchants peace of mind when it comes to their own security, as well as that of their customers.

## Basic Uses

Though there are countless ways to use iSpyFraud based on varying scenarios merchants might encounter, there are certain uses of the software that could be considered universally relevant, including:

1. Monitoring and controlling transactions during a given timeframe by setting rules based on a combination of many parameters, including the following:
  - a. Transaction count
  - b. Transaction amount
  - c. IP address
  - d. User location
  - e. Credit card number
  - f. Credit card brand
2. Limiting internal credit card fraud or abuse attempts
3. Blocking transactions from specific countries
4. Reviewing suspect transactions in order to take action prior to settlement

The following instructions will aid merchants in choosing the settings that will prove most useful for them depending on the specific needs of their business. In addition to this guide, assistance can be accessed through our support team, which can be reached at (800) 617-4850 ext. 1 from 8 am-6pm central time, or at [support@nmi.com](mailto:support@nmi.com).

## Getting Started

When a merchant logs into the gateway, iSpyFraud can be found as a link under “Other Services” on the left side of the page. The link will take the merchant to the program’s General tab. Other than geography bans on transactions from certain countries, there are **no default settings** in place. There are default geography bans on the following countries (as sent in the Country field):

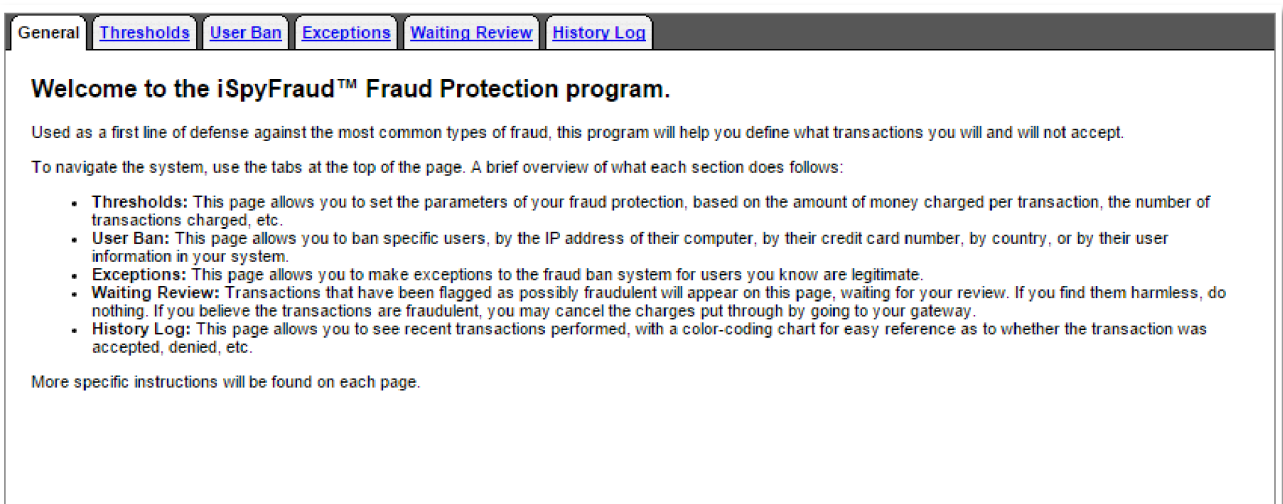
Afghanistan  
Albania  
Armenia

Azerbaijan  
 Bulgaria  
 Czech Republic  
 India  
 Indonesia  
 Iran (Islamic Republic of)  
 Kazakhstan  
 Kuwait  
 Lithuania  
 Macedonia, the Former Yugoslav Republic of  
 Malaysia  
 Pakistan  
 Romania  
 Russian Federation  
 Turkey  
 Ukraine  
 Viet Nam  
 Yugoslavia

The countries on this list are frequently the origin of fraudulent international transactions. The merchant can remove any of them from the ban list at will (see User Ban tab section for instructions).

## General Tab

The General tab gives basic information about what iSpyFraud does and has a brief overview of its contents. Note the tabs at the top of the screen, which browse to different sections within the iSpyFraud console.



The screenshot shows the 'General' tab selected in the iSpyFraud console. The navigation bar includes tabs for 'General', 'Thresholds', 'User Ban', 'Exceptions', 'Waiting Review', and 'History Log'. The main content area displays a welcome message and a list of instructions for each tab.

**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.

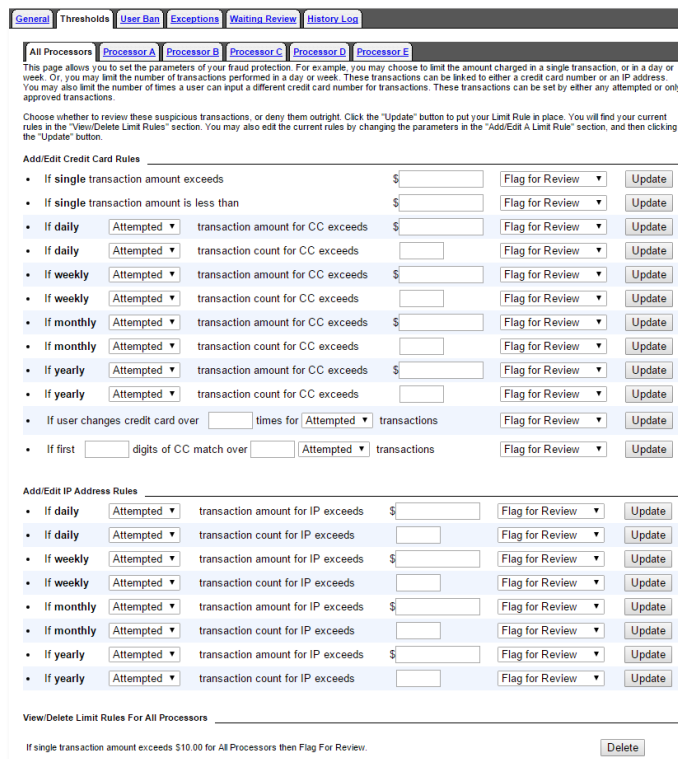
## Thresholds Tab

The Thresholds tab allows a merchant to set a variety of parameters on attempted or approved transactions, and these rules give the merchant the option to either Flag for Review or Deny Transaction. There are two main sections, titled **Add/Edit Credit Card Rules** and **Add/Edit IP Address Rules**, and the options in each section direct the merchant to set a threshold on a certain aspect of a transaction. These thresholds can be set in a combination of ways to track and/or block certain types of activity that may point to fraud.

For example, there are two rules pertaining to single transaction amount. If the merchant doesn't sell anything under \$20, they can set transactions for anything less than \$20 to be flagged for review or denied. This can help prevent card testing, in which a fraudster might charge small amounts to a large number of credit cards.

In another case, a merchant with a subscription-based business might use the option to limit attempted number of transactions; the merchant can flag for review transactions beyond the initial subscription fee that come from the same IP address within the same day to ensure that they're not fraudulent.

To set thresholds, the merchant simply chooses (if applicable) whether they wish to screen attempted or approved transactions (drop-down), enters the desired values, and then chooses whether the end result of a suspicious transaction should be to flag it for review or deny its approval (dropdown). Once these choices have been made, the merchant clicks "Update." Each rule must be updated individually. *For a more in-depth look at some possible uses of the Thresholds tab, see Use Cases.*



## User Ban Tab

The bans/flags in this tab are considered static, in the sense that they don't depend on the behavior of the user (the consumer). In each section, the merchant chooses what users or types of users to ban/flag, and any transactions originating with those users will either be banned outright or flagged for review, depending on the merchant's selections. Each section gives the option to View current bans and Add new bans. When the merchant clicks to the "View" screen, they also have the option to Delete any currently banned users.

There are seven sections in the User Ban tab:

- 1. IP Addresses**
  - a. Merchants can ban/flag a single IP, multiple IPs from the same block, or a range of IPs
  - b. Merchants can specify a timeframe (number of days) in which to ban/flag IPs, or make the ban/flag indefinite
- 2. Credit Cards**
  - a. Merchants can ban/flag a single credit card number, multiple credit card numbers, or all credit card numbers with matching BINs
  - b. Merchant can specify a timeframe (number of days) in which to ban/flag credit card numbers, or make the ban/flag indefinite
- 3. Geographical Information**
  - a. Merchants can ban/flag transactions from any country
  - b. Merchants can specify a timeframe (number of days) in which to ban/flag a country, or make the ban/flag indefinite
  - c. A ban/flag on a specific country will automatically check for any billing/shipping addresses from that country and ban/flag users based on that information, and the merchant can also choose whether or not to verify IP addresses from that country
- 4. US/Non-US IP Ban**
  - a. Merchants can choose three actions (Nothing, Ban, or Flag for Review) for transactions that have a billing country of US but a source IP address outside the US
    - i. Unlike with the other sections in this tab, there is no timeframe specified for this ban
    - ii. Merchants who do not send the Country field with their transactions can set a US Country Default, which will assume (for the purposes of this particular ban) that the Billing Country is the US.
- 5. User Information**
  - a. Merchants can ban/flag specific customers based on customer user IDs, which merchants can assign via the use of Customer Vault. User IDs outside of Customer Vault can also be submitted by the merchant via API or by providing the billing email in the transaction
  - b. Merchants can specify a timeframe (number of days) in which to ban/flag certain users, or make the ban/flag indefinite

## 6. Email Address

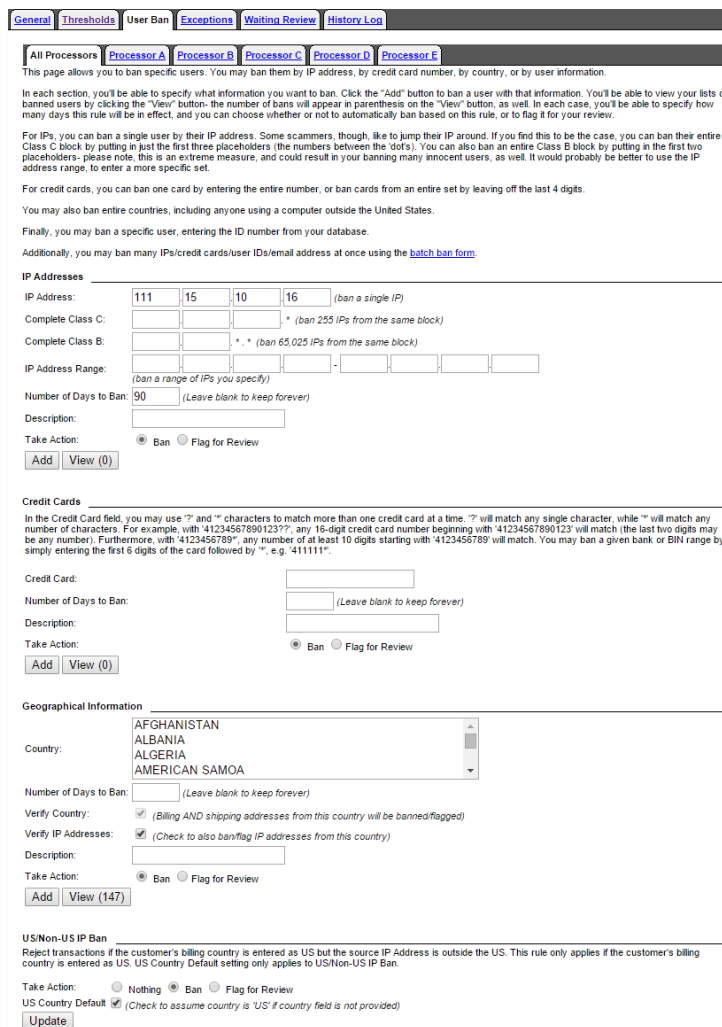
- a. Merchants can ban/flag customers by email address, or ban/flag any customer using an email address with a particular domain
- b. Merchants can specify a timeframe (number of days) in which to ban/flag certain emails or domains, or make the ban/flag indefinite

## 7. Batch Ban

- a. Merchants can upload up to 5000 entries for a specific ban type at once
- b. Types can be chosen using the radio buttons above the Batch Data Box—merchants can select from IP/Range, Credit Card/Bank, User ID, and Email
  - i. Only one type of data may be uploaded at a time
- c. Merchants can specify a timeframe (number of days) in which to ban/flag certain values, or make the ban/flag indefinite

**Note: For any of the IP Address selections to work, the Merchant must collect the public-facing IP address from the consumer and provide it with the transaction.**

*For a more in-depth look at some possible uses of the User Ban tab, see Use Cases.*



The screenshot shows the 'User Ban' tab in a web application. It features several sections for defining ban criteria:

- IP Addresses:** Includes fields for IP Address (111.15.10.16), Complete Class C, Complete Class B, IP Address Range, Number of Days to Ban (90), Description, and Take Action (Ban/Flag for Review).
- Credit Cards:** Includes fields for Credit Card, Number of Days to Ban, Description, and Take Action (Ban/Flag for Review).
- Geographical Information:** Includes a Country dropdown menu (AFGHANISTAN, ALBANIA, ALGERIA, AMERICAN SAMOA), Number of Days to Ban, Verify Country, Verify IP Addresses, Description, and Take Action (Ban/Flag for Review).
- US/Non-US IP Ban:** Includes a description of the rule, Take Action (Nothing/Ban/Flag for Review), US Country Default (checked), and an Update button.



**User Information**

User ID:

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

Description:

Take Action:  Ban  Flag for Review

---

**Email Address**

Enter in an email address that you wish to ban from the system. The system will ban that email address specifically. You can choose a "global option" for ban by placing a "\*" in front of your email address. For example, if you want to ban a specific email account, you would type in 'someuser@emailaddress.com'. If you want to ban the entire domain email account, you would type in '\*@emailaddress.com'.

Email Account:

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

Description:

Take Action:  Ban  Flag for Review

---

**Batch Ban**

Here you may enter many ban values at once. First choose the type of ban you would like to use, and then enter the values in the text area below, one on each line. Choose the number of days to ban (or blank for forever), a description, and action type before clicking the Add button.

Type:  IP/Range  Credit Card/Bank  User ID  Email

Batch Data:

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

Description:

Take Action:  Ban  Flag for Review

## Exceptions Tab

The Exceptions tab goes hand in hand with the User Ban tab and is considered the “whitelist” to the User Ban’s “blacklist.” In other words, merchants can use the Exceptions tab to make concessions for certain known users that would otherwise be banned or flagged under the restrictions in the User Ban tab.

Any exception overrules all other rules. For example, if credit card 4111111111111111 is added to exceptions, the domain @gmail.com is banned, and the country Canada is banned, a transaction using “4111111111111111, test@gmail.com, and Canada” will be approved.

Merchants can create exceptions for

- **IP Address**
- **Credit Card**
- **User ID**
- **Email Address**

Exception values can also be uploaded using the same process as batch bans.

[General](#) | [Thresholds](#) | [User Ban](#) | [Exceptions](#) | **[Waiting Review](#)** | [History Log](#)

[All Processors](#) | [Processor A](#) | [Processor B](#) | [Processor C](#) | [Processor D](#) | [Processor E](#)

The 'White List' is a way to make exceptions to your ban parameters. Known good users (whom you know violate the restrictions, but accept them as a valid user anyway) can be entered here to bypass your restrictions without review. Users can be entered by User ID, email address, credit card, or IP.

In each section, you may enter the data of your known user, and click the "Add" button to make an exception for this user's specific information. You'll be able to view your lists of banned users by clicking the "View" button- the number of bans will appear in parenthesis on the "View" button, as well.

Additionally, you may whitelist many IPs/credit cards/user IDs/email addresses at once using the [batch white list form](#).

---

**IP Address White List**

IP Address:

Description:

---

**Credit Card White List**

Credit Card:

Description:

---

**User White List**

User Identifier:

Description:

---

**Email White List**

Email Address:

Description:

---

**Batch White List**

Here you may enter many whitelist values at once. First choose the type of exception you would like to use, and then enter the values in the text area below, one on each line. Enter in a description in the appropriate box before clicking the Add button.

Type:  IP/Range  Credit Card/Bank  User ID  Email

Batch Data:

Description:

## Waiting Review Tab

Merchants can view and take action on flagged transactions here; merchants can either void transactions that are in waiting review or allow them to settle by indicating that the review is complete. If no action is taken, transactions awaiting review will settle at the time set in the Merchant's Settlement Schedule.

Merchants will be able to see which rule triggered the review.



[General](#) | [Thresholds](#) | [User Ban](#) | [Exceptions](#) | [Waiting Review](#) | [History Log](#)

[All Processors](#) | [Processor A](#) | [Processor B](#) | [Processor C](#) | [Processor D](#) | [Processor E](#)

**There are 373 transactions awaiting review.**

**Overview:**  
 This page allows you to review suspicious transactions. 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.

**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.

Sort By: [\[User ID\]](#) [\[Date\]](#) [\[Credit Card\]](#) [\[Amount\]](#) [\[IP\]](#) [\[Country\]](#) [\[Exceeded Threshold\]](#)  
 Pages: [\[View All\]](#) [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#) [\[6\]](#) [\[7\]](#) [\[8\]](#)  
 Viewing: 1 - 50 of 373

		Review Complete <input type="checkbox"/>
Transaction ID:	<a href="#">2914110006</a>	
Result:	Approved	
Processor:	ProcessorA	
Time:	12/08/2015 08:25:12 AM 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:	\$10.00	
IP Address:		
User Country:		
Threshold Exceeded:	Single Transaction Amount Exceeds Limit	
	<a href="#">Show Details for this CC/IP:</a>	
<hr/>		
Transaction ID:	<a href="#">2914109966</a>	Review Complete <input type="checkbox"/>
Result:	Approved	
Processor:	ProcessorA	
User Identifier:	john@example.com <a href="#">[History]</a> <a href="#">[Whitelist User ID]</a>	
User Email:	john@example.com <a href="#">[History]</a> <a href="#">[Whitelist User Email]</a>	
Time:	12/08/2015 08:25:11 AM 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:	\$10.00	
IP Address:		
User Country:	US	
Threshold Exceeded:	Single Transaction Amount Exceeds Limit	
	<a href="#">Show Details for this CC/IP:</a>	

## History Log Tab

The History Log offers the merchant a searchable record of all transactions scrubbed by iSpyFraud. This log is useful for a merchant who is trying to assess the risk of potential fraud, or to evaluate known fraud patterns. A drop-down menu allows merchants to limit a search by time/date of transaction, and merchants can search by transaction ID, credit card number, email address, or IP address.

The log is color coded by transaction status: Accepted (green), Review (yellow), Exception (blue), or Denied (red). For statuses of Review and Denied, a magnifying glass next to the response status allows merchants to see which rule was triggered.

[General](#) | [Thresholds](#) | [User Ban](#) | [Exceptions](#) | [Waiting Review](#) | [History Log](#)

[All Processors](#) | [Processor A](#) | [Processor B](#) | [Processor C](#) | [Processor D](#) | [Processor E](#)

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

End Time

Date (UTC)	Trans. ID	Email	Credit Card	Amount	IP Address	Country	Response	Last Action
12/08/15 23:23	<a href="#">2914963150</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	5.25	<a href="#">209.37.68.130 (ban)</a>		Approved	Approved
12/08/15 23:23	<a href="#">2914962996</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	1.25	<a href="#">209.37.68.130 (ban)</a>		Approved	Attempted
12/08/15 23:23	<a href="#">2914962862</a>		<a href="#">4...1111 (ban)</a>	0.25	<a href="#">209.37.68.130 (ban)</a>		Approved	Attempted
12/08/15 23:22	<a href="#">2914962535</a>		<a href="#">4...1111 (ban)</a>	0.25	<a href="#">209.37.68.130 (ban)</a>		Approved	Attempted
12/08/15 21:15	<a href="#">2914832890</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	55.00	<a href="#">50.76.64.234 (ban)</a>	US	Review	Approved
12/08/15 21:10	<a href="#">2914827295</a>		<a href="#">4...1111 (ban)</a>	26.35	<a href="#">50.76.64.234 (ban)</a>	US	Approved	Approved
12/08/15 21:05	<a href="#">2914822546</a>		<a href="#">4...1111 (ban)</a>	15.00	<a href="#">50.76.64.234 (ban)</a>	US	Denied	Attempted
12/08/15 21:04	<a href="#">2914821765</a>		<a href="#">4...1111 (ban)</a>	10.00	<a href="#">50.76.64.234 (ban)</a>	US	Denied	Attempted
12/08/15 17:00	<a href="#">2914552709</a>		<a href="#">4...1111 (ban)</a>	1.00	<a href="#">50.76.64.234 (ban)</a>	US	Denied	Attempted
12/08/15 16:47	<a href="#">2914535018</a>		<a href="#">5...1111 (ban)</a>	1.00	<a href="#">50.76.64.234 (ban)</a>	US	Denied	Attempted
12/08/15 16:21	<a href="#">2914499974</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	20.00	<a href="#">209.37.68.130 (ban)</a>		Approved	Approved
12/08/15 15:59	<a href="#">2914467639</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	10.00	<a href="#">209.37.68.130 (ban)</a>		Approved	Approved
12/08/15 15:46	<a href="#">2914451034</a>		<a href="#">4...1111 (ban)</a>	10.00	<a href="#">50.76.64.234 (ban)</a>		Denied	Attempted
12/08/15 08:25	<a href="#">2914110152</a>		<a href="#">4...1111 (ban)</a>	1.00		US	Approved	Approved
12/08/15 08:25	<a href="#">2914110136</a>		<a href="#">4...0002 (ban)</a>	15.00			Denied	Attempted
12/08/15 08:25	<a href="#">2914110087</a>		<a href="#">4...0002 (ban)</a>	10.00			Review	Approved
12/08/15 08:25	<a href="#">2914110044</a>		<a href="#">4...1111 (ban)</a>	10.00			Review	Approved
12/08/15 08:25	<a href="#">2914110006</a>		<a href="#">4...1111 (ban)</a>	10.00			Review	Approved
12/08/15 08:25	<a href="#">2914109966</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	10.00		US	Review	Approved
12/08/15 08:25	<a href="#">2914109929</a>		<a href="#">5...1111 (ban)</a>	5.00		US	Approved	Approved
12/08/15 08:25	<a href="#">2914109831</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	1.00		US	Approved	Approved
12/08/15 08:25	<a href="#">2914109726</a>	<a href="#">john@example.com (ban)</a>	<a href="#">4...1111 (ban)</a>	0.01		US	Review	Attempted
12/08/15 08:25	<a href="#">2914109702</a>		<a href="#">4...1111 (ban)</a>	19.99			Denied	Attempted
12/08/15 08:25	<a href="#">2914109683</a>		<a href="#">4...1111 (ban)</a>	19.99			Denied	Attempted
12/08/15 08:24	<a href="#">2914109639</a>		<a href="#">3...1009 (ban)</a>	5.00		US	Approved	Approved

201 - 225 of 397 Records - Page 9 of 16  
[1](#) [3](#) [4](#) [6](#) [7](#) [9](#) [11](#) [12](#) [14](#)

[\[Previous\]](#)

Jump to page #

[\[Next\]](#)

## Frequently Asked Questions

### **Q: What types of merchants need iSpyFraud?**

**A:** Though all merchants can benefit from the reassurance a fraud scrubbing utility offers, it's true that some merchants are more likely to be targeted by fraudsters than others. For example, merchants who process international transactions are considered higher risk, as are those in certain verticals, such as online gambling, online dating, membership-only websites with adult content, or even unexpected ones like consumer electronics. Non-profits that accept donations are also at risk and can benefit from iSpyFraud, as they are often used by fraudsters for card testing/spinning schemes.

It's also anticipated that as EMV cards become standard in card present transactions, there will be a rise in card not present fraud, meaning more e-commerce merchants will be at risk. iSpyFraud is an ideal solution to combat the predicted spike in online credit card fraud.

### **Q: Does iSpyFraud work in card present transactions?**

**A:** Although iSpyFraud was originally designed for e-commerce, it works equally well for card present transactions. The software's thresholds and rules do not discriminate between retail and keyed transactions, nor is the utility's scrubbing ability restricted by transaction origin (API, Virtual Terminal, Batch Upload, etc.).

### **Q: Can iSpyFraud block someone from coming to my website?**

**A:** No, iSpyFraud can only take action on transactions sent to the Gateway. It cannot block activity happening on a website prior to data being sent to the gateway. Merchants can speak to their hosting provider or web developer if they need to block an individual from accessing their website entirely.

### **Q: I'd like to use iSpyFraud on my website, but I don't want to use the Gateway to process. Is this possible?**

**A:** No, iSpyFraud is an additional service that can be added onto a gateway account to scrub transactions processing through it. It cannot be used as a standalone service. Merchants must be processing through the gateway to take advantage of the iSpyFraud scrubbing service.