

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

10 Ways to Reduce Chargebacks & Fraud

By **Jim Conley II**

10 Ways to Reduce Chargebacks & Fraud by Jim Conley II

Merchant concern about online credit card fraud and chargebacks is rising at a significant rate. According to the 2001 Online Fraud Report, conducted by Mindwave Research, it revealed that, "41% of merchants say the issue of online credit card fraud is 'very serious' to their business." As e-commerce continues to flourish the number of instances of credit card fraud and chargebacks will continue to mount higher. It should go without saying that the need to take certain measures to reduce and virtually eliminate chargebacks and fraud is certainly paramount.

Here are some ways you can greatly reduce the instances of chargebacks and fraud, even potentially eliminate the risk altogether:

#10 Interactive Voice Response (IVR) Terminals

IVR Terminals, developed by VoiceStamps <http://www.voicestamps.com>, are a relatively new solution that greatly reduces chargebacks and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order. The voice recorded order verification is then automatically e-mailed to the merchant for filing in the event the customer tries to dispute the charge on their account.

#9 Collect CVC2 and CVV2 Verification Numbers

10 Ways to Reduce Chargebacks Fraud

This tactic alone can not only reduce instances of chargebacks by 26%, according to Visa, but also reduce any pass-through fees that may be charged when a credit card order is conducted. On the back of MasterCard, most Visa and Discover credit cards is a 3-digit security code located right after your credit card number. Requiring customers to give the 3-digit code acts as an additional verification measure.

American Express cards also have a similar security code that is located on the front of the card right above the cardholder's account number and is usually 4-digits long. Most online payment processors support entering the security codes when processing credit card orders. Check with your payment

gateway provider (i.e. Verisign, Authorize.Net, ECHO Inc., etc) for details.

#8 Use Address Verification System (AVS)

AVS checks to ensure the address entered on the order form matches the address to where the cardholder's billing statements are mailed to. People ordering products and/or services using a stolen card number will never use the real cardholder's billing address, so this is your chance to stop the order before it's too late. AVS only works with orders conducted in the US. Failure to use AVS when processing credit card transactions will always result in paying higher credit card processing fees.

#7 Scrutinize orders from developing foreign countries

A large percentage of fraudulent Internet purchases are made from Indonesia, Russia, and other eastern block or developing countries. Accept orders from such countries at your own risk until a worldwide AVS system is developed.

#6 Let customers know what name will appear on statements

Many merchants who use 3rd Party Processing companies have run into problems because the company name that appears on cardholder's monthly statements is usually the name of the 3rd party processing company and not the company name of the site the cardholder made their purchase from. This isn't always the case, but in many cases it is. If you use a 3rd party processor, and even if you don't, make sure the

customer knows what name will appear on their credit card statement at the end of the month. This will help to reduce any confusion that might would otherwise occur.

#5 Handle suspicious orders accordingly

If an order seems suspicious the best way to handle the situation is to either call or e-mail the customer and attempt to verify that they placed the order. As a rule of thumb, if in doubt, check things out. It may be a good idea that if a customer makes an unusually large volume purchase from your site to follow-up with a verification call. This is where a system like IVR terminals, previously mentioned above, can come in very handy.

#4 Watch out for orders using free e-mail addresses

Be wary of accepting orders from people who used a free e-

mail address when ordering (i.e. Hotmail, Yahoo, etc.). Tracking people who used a free e-mail address is almost impossible, it's much easier for them to get away then if they used their Internet Service Provider (ISP) or their own company web site e-mail address. To check whether an e-mail address is a freebie or not just take the part of the address after the "@" symbol, add "www" to the front of it and see what website it brings up (i.e. joe@yahoo.com = www.yahoo.com

#3 Signatures on delivery

If your business delivers products use a carrier that requires a signature on delivery, and allows you to have a copy of the signature. Retain these for your records.

#2 Request fax copies of ID and credit card

You may want to request your customer to fax a copy of both sides of their credit card and driver's license. This tactic usually works best in a B-to-B (business to business) sales environment. While this is not a defense under Visa or MasterCard rules, it is yet another way to deter fraud.

#1 Posting a warning message

10 Ways to Reduce Chargebacks Fraud

Taking the time to post a warning message on your order page to those who may attempt to make a fraudulent order will greatly deter the number of instances of fraud. Be sure to mention that IP (Internet Protocol) addresses are being logged. IP addresses can come in handy when locating people about fraudulent orders.

Taking measures to deter and eliminate fraud and chargebacks from occurring are a necessity in order to operate a successful online business. Each day companies dedicated to risk management are developing solutions to provide merchants, like yourself, with extra protection because of the financial burdens chargebacks and fraud can bestow if ignored.

Jim Conley II, CEO/Founder of MerchantSeek (<http://www.merchantseek.com>). Search FREE for a Merchant Account Provider that meets your business needs and budget. Plus learn details about different payment processing solutions available to you.

Tips For Combating Click Fraud

By Gabriel Adams

Click fraud is one of the biggest issues in the pay per click industry right now. It's easy to understand why, too - click fraud costs advertisers money, but gives no return. It cuts deep into profit margins, and in some cases, may be the difference between making money and losing money.

Click fraud is, at its simplest, clicks on ads that are not generated by a real person interested in making a purchase. Click fraud can come from many different sources:

Click bots, which are robots designed to click on ads, are one source. Click bots are often run by an affiliate of the PPC search engine.

Competitors may click on your ads to try to drive your cost up.

Click schemes are programs people join to click on ads for each other. Usually these people are affiliates of the PPC search engines.

Combating click fraud can be tough. One of the easiest ways to combat click fraud is to not advertise on search engines who deliver lower quality traffic. This factor is easily determined with conversion rates. If one search engine's traffic converts at 2 percent, and traffic from the second search engine converts at 1 percent, you know the traffic from the second search engine is half the quality. Click fraud is likely one of the factors involved.

In addition to such basic tracking mechanisms, you can use more advanced tracking mechanisms to try to catch click fraud. For example, you could use a script that you would gather data on visitors from

10 Ways to Reduce Chargebacks Fraud

PPC search engines (data might include IP address, number of times they clicked on the ad, and time they spent on the site) and use that data to pick out suspicious visitors. You can then submit the data to the search engine and request a refund on the traffic.

Click fraud is probably the biggest problem in the PPC industry, and you can work to save yourself some money by combating click fraud.

Bespoke click fraud detection and protection software from Evolution Internet Ltd:

improve your life and find your happiness. Only 9.95Seven ways to improve your life and find your happiness.



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!