



# Top 5 Fraud Defense Tips

## eBC Guide to Protecting Your Business From Fraud

Protect your online business from fraud. One of the great things about the Internet is anonymity. One of the worst things about the Internet is anonymity - especially for ecommerce merchant. If you utilize payment gateways for credit card transactions or are considering doing so, it is important to ask the gateway provider about their pre-screening procedures (this precedes actual credit card payment processing). Some offer none at all!

Many payment gateway providers use the Address Verification System (AVS). AVS provides some protection by comparing the billing address on the web order form to the address held by the cardholder's bank.

The transaction may be approved even if the address verification information does not match! The merchant faces the possibility of chargeback's if the payment gateway decides to continue with the transaction on a questionable match.

So here are the top 5 fraud defence tips.

### **#1) Protect yourself by requesting Information**

While consumers value their privacy and require quick web site ordering facilities, it is of the utmost importance that you gather sufficient customer identity details during the ordering process. The customer's name, credit card number and expiry date is not enough. Tell your customers why you need the information and what you will do with it - after all, it's in their best interests too. The fewer chargeback fees you have to pay, the cheaper you can offer goods and services.

### **#2) Check the Email Address**

Fraudsters rarely use their own email address. With the proliferation of free email services, it is quite easy to provide false contact details. A false Yahoo email address can be established within 5 minutes. Increasing numbers of Internet retailers are refusing to process web site orders that list free email address services as the primary point of contact, opting to request from customers their ISP or business email addresses. You can check an email address quickly by going to the originating domain and seeing if it provides a free email service.

### **#3) Check the Shipping Address**

If the shipping address is different to the billing address, be wary; although it is not uncommon for people sending gifts to others to request a different shipping address, or if the billing address is a post office box.

You'll rarely find a fraudster sending goods to the legitimate cardholders address. At the point of ordering, request a telephone contact number for your customer. State that you need this number in order to contact them if there are any problems. Many cardholders of compromised accounts have been alerted in this way. The fraudster definitely won't give you his own phone number as he/she can then be traced! If you are unsure, email the customer or call them to confirm the authenticity of the transaction. Fraudsters hate merchant contact of any kind.

#### **#4) Be Wary of Overseas Orders**

Overseas orders are very risky, but an integral part of your online business. It is very difficult to retrieve goods or apprehend fraudsters once the goods have left the country. Make further enquiries with the credit card company if an order seems suspect.

Unfortunately, Eastern Europe is still a very high risk region for the origin of credit card fraud, with many online business owners refusing to process orders from Eastern Europe. Other high risk regions are Indonesia, Turkey, Pakistan, Malaysia and almost anywhere in Africa.

#### **#5) Unusual Orders should be Unusual**

Unusually large orders requesting express delivery definitely warrant further investigation, especially if the customer has not purchased from you before. Customers are pretty cautious, and will tend to place small orders in the first instance to test the efficiency and integrity of your online business, or they'll make some sort of contact with you prior to ordering.