

# Preventing Fraud On Your Website

By Aaron Turpen

Preventing Fraud On Your Website

Aaron Turpen  
aaron@aaronzwebworkz.com

Aaronz WebWorkz <http://www.AaronzWebWorkz.com>

The explosion of online commerce presents new opportunities and challenges for both the web merchant and the web thief. The special properties of the Internet, including the anonymity, reach and speed it affords, make it an especially tempting place to do business as a thief. All merchants, online or off, must take steps to prevent fraud from happening to them, but merchants online must be more vigilant. This guide will show you how your online presence can and why it should include risk management and fraud prevention tactics.

Current statistics show the instances of fraud in traditional “face-to-face” transactions to be around .06% of the whole. Online, however, they are much higher: 1.14% as of late 2001. [Gartner Group IT Advisory, November 2001] The most common form of fraud is what’s known as the “fraudulent chargeback.”

## How It’s Done

In order to combat fraud, one must first know how it is committed. Usually, the thief requires only a valid credit card number. These are gained in several ways, but rarely are they stolen from cyberspace. The most common ways to procure credit card numbers include mundane and traditional methods: theft of the card itself or theft of card receipts/imprints. Another, newer method of stealing card data is to “skim” it using a small machine made for the task. These can be used by employees who, given the opportunity, can swipe the card through their machine, which then stores the data for later retrieval to a PC or printer.

Once the data is obtained, a receiving mailbox or address is required. This is usually an abandoned house, a mailbox store, or even a Post Office Box. Once a shipping address is gained, the card can be used to purchase items on the Internet and have them shipped to the address.

Another way to steal from online merchants is the “chargeback” (as mentioned above). The customer buys the item from the online merchant (usually requesting a fast form of shipping), waits for it to arrive, and then complains to his or her card-issuing bank that the charge for the item is bogus. The bank, usually operating on a no-questions-asked policy, immediately credits the customer’s account and cancels the payment to the merchant bank.

## What It Costs

Besides the usually higher cost of processing for Card-Not-Present transactions (including higher interchange rates), the merchant usually bears full liability for losses due to fraud. Because the card-issuing bank usually has a no-questions-asked policy towards Internet chargebacks, your merchant bank usually does the same. Once a chargeback to the customer has been made, it is

nearly impossible for the merchant to reverse it to regain their money. So not only has the merchant lost the goods sold, but also the shipping, card transaction fees, etc. They also may incur merchant chargeback fees and manpower costs associated with it (for research and processing). This can easily reach several hundred dollars per case.

### Technologies For Fraud Detection

As with most security issues, the techniques and sophistication of both the defenders and attackers continue to compound one another. Obviously, there is no sure way to completely prevent fraud on your website, but there are numerous ways to lower your risk and thwart most efforts. The methods listed below are the most commonly used and thoroughly tested of the tools for prevention. Most likely, your strategy will include several of these together.

#### AVS – Address Verification System

When mail order companies began to proliferate in force and the card-not-present transactions they produced began to raise the number of fraudulent transactions in credit card processing, several banks got together and established the Address Verification System (AVS). The idea behind it is simple: all credit cards are billed to the customer's address, which is usually on the form or can be asked for during the transaction. If the information given by the customer can be matched against the information included in the issuing bank's records, there is a higher chance the card and transaction are legitimate. Since the checks are made by a computer, most of the matches are made against the numbers in the address rather than the address as a whole. So the ZIP code, street numbers, etc. are what are actually compared.

While this is a good method and is employed by many merchants, it is not required and the decision to use the information is left up to the merchant. Since the merchant is ultimately responsible for the costs involved with chargebacks, this is a fair system. There are several drawbacks to the system as well: 1) the shipping address and billing address are not always the same; 2) this is only available for cards issued in the U.S.; and 3) many orders that fail this check are still valid orders (estimated 98% of AVS failures are legitimate transactions).

#### CVM – Card Verification Methods

Although relatively new, this method is gaining momentum for one reason: it almost guarantees the person using the card has the card in his or her hand at the time of use. In other words, it removes many of the doubts associated with CNP transactions. It works simply: on the credit card is printed a short number (usually three or four characters in length). This number is not embossed or stored on the strip of the card itself, but is usually printed on the back in ink – generally on the signature strip. When prompted for this number, the cardholder enters it by physically looking at the card, and the merchant verifies it with the bank for a match/no-match response.

This method makes it harder for a stolen card NUMBER to be used, but is not a 100% foolproof way to verify a credit card. If the card was physically stolen or if the buyer intends to commit a chargeback anyway, it offers no protection. It should be noted, however, that in studies, cards with a verified CVM code are much less likely to be than those without (reportedly 80% lower). Also be aware that as this is a relatively new technology, it has not been fully standardized. Different card issuers give it different names including CVC2, CCV2, and CID.

#### Lockout and Refusal Systems

One of the more common ways for the less-sophisticated thief to gain valid credit card numbers is through brute trial-and-error. Using an automatic card number generator (available all over the Web for free) and a simple script or program to fill out a form for them, a would-be thief can generate and test thousands of credit card numbers in minutes. The idea is fairly simple and works like the "lock picks" for electronic locks that you see in the movies: the generator produces a 14 or 16 digit sequence which will comply with a MOD10 check (a standards consistency check used by issuing

banks to initially verify that a card is theirs); the number is then fed into an automatically-filled form on a website (website scouted and the automatic form filler has been previously set up by the thief), and processed for the transaction. If the bank refuses the card, an error page appears and the program continues from the beginning. If the number stumbled upon is legitimate, the account is charged and the merchandise is set to be shipped while the program stores the number as valid in a list with other validated numbers. Later, the thief can go back to these valid numbers and begin using them around the Web until they are maxed out or locked down by the bank.

This is by far the easiest form of attack to prevent. Since they follow an obvious and difficult-to-modify series of events, software can be put into place to detect these types of attacks. The easiest form is to reject more than X number of transactions from a certain IP address (whether they fail or not) in X amount of time (day, week, month). These attacks will also fail to pass an AVS and CVM check as well.

#### “Bad Customer” Lists

Most brick-and-mortar businesses have a list of customers they will not accept checks, credit cards, etc. from because of past experience with that customer. A similar list can be created for a web-based merchant as well. As each bad transaction takes place, it is recorded for future reference. When a new order is placed, the name/address/card number/etc. are checked against this “bad” list and rejected if a match is found. If done before any other processing takes place, this can flatly refuse any customer who has a history of fraud.

While this is a must-have for any business that accepts credit cards online, it does not prevent fraud from happening, but rather stops it from coming from the same source multiple times. For several obvious reasons, including the likelihood the customer has multiple cards and/or addresses, it is not foolproof, but is generally effective in dealing with repeat offenses.

#### Risk Scoring and Refusal Rules

These are the best methods to include in your strategy, as they are usually a strategy within themselves. Utilizing combinations of the above methods plus specifics about the order itself, these “scores” are assessed based on the type of risk believed to be involved. For example, a transaction may be for more than \$500 dollars (+3 to risk), include more than three of any item (+1 for each item higher than three), the card failed the AVS check (+3 to risk), and the shipping address is in the same state as, but different than the billing address for the card (+1 to risk). The total risk for this transaction is 8. On a risk scale of 1-15, it is considered to be medium-high risk and therefore is flagged for checking by a human employee, but is processed without pause. A risk factor of, say, 17 would mean the order would be flagged for definite review by an employee (who can call the phone number associated, double-check information given, etc.) and will not be processed until the employee gives it the OK. Whether the customer is alerted or not is usually up to the merchant.

This type of system uses several fraud prevention techniques, thereby significantly lowering the risk of fraud. It also allows the merchant to set standards for the characteristics of what he or she considers a good or bad transaction. The better the rules, the less the chance of theft. Over time, a risk-based system can become very good at its job and virtually eliminate most fraudulent transactions.

#### Recommended Fraud Prevention Strategy

Although I cannot recommend something specifically for your needs, on a broad scale, I can recommend a strategy that anyone doing business online should include in their overall scheme to prevent theft. Almost all fraudulent orders have certain characteristics that should raise a red flag should they appear. Using these and the tools listed above, you can put together a system to significantly lower your chances of being victimized.

The first thing your system should do is compare the order against your existing “Bad Customer” List. If it passes that check, then the following flags should be included in your rule-based risk scoring system:

- Larger-Than-Normal-Orders: any order that seems larger than would normally be placed, especially for multiples of the same item, should have a high-risk score.
- Fast-Shipping/Overnight-Shipping: any order that is shipped overnight should have a moderate risk score attached to it (at the very least, it should be shipped using a carrier which can verify a signature).
- Orders-To-An-Out-Of-State-Address: any order that is shipped to an address in a different state than the billing address of the credit card should be given a high-risk score.
- Failed-AVS-Verification: an order that fails this check should be given a moderate risk score.
- Failed-CVM: an order that fails this check should be given a moderate-high risk score.
- “Free”-Email-Address: an order which includes an anonymous email address such as Hotmail.com or Yahoo.com should be given a moderate risk score as many thieves use these addresses so that they can dump them easily.
- Multiple-Orders-From-The-Same-Card/IP/Shipping-Address: more than one or two orders from the same credit card or the same IP address, especially if the second order is significantly higher than the first, should be flagged with a high-risk score. More than two orders from either source should be rejected out of hand (it’s recommended you store IP/credit card numbers SECURELY for at least an hour for this check).

### Reporting Fraud

While there is little incentive, monetarily, for a merchant to report fraud, it should be done. It is a sad fact that most thieves who use Internet fraud are rarely caught and most stolen items are rarely returned to the merchant (not to mention costs reimbursed). However, a policy of reporting these instances can prove salvation should a thief be caught with records on file. After all, if you don’t report it, no one will know about it except you and the thief – a scenario unlikely to get you anywhere in court.

The basics needed are simple: a solid policy that is hard to screw up internally, detailed information kept on file to support investigations or prosecution (including what was taken and how much was lost in money and time), consistent reporting, helpful and timely response, and a policy for direct negotiation with the thief. These will help any investigation, whether internal or external. You will need to know who you should report fraud to (usually local law enforcement will direct you to the correct bureau and you should also include your merchant bank as a contact), what information they require, and who is the primary contact person at your business for these investigations.

Preventing fraud online is the responsibility of everyone who does business on the Internet. Obviously, the merchant has more reason to do so than not to since the merchant is the one who loses money when fraud takes place. Utilizing the tools available and building a strategy to fit your needs, you can reduce the number of fraudulent transactions for your business and save significant amounts of money.

[Get-Articles.com](http://Get-Articles.com) : 1000's of reprintable business and internet marketing-related articles.

[Submit your article for reprint.](#)