LEVIN, SILVEY, ZELKO & CO., P.A.

Certified Public Accountants

MITCHELL H. SILVEY, CPA
ROBERT A. ZELKO, CPA
BONNIE L. MACKEY, CPA, CSEP

2699 STIRLING ROAD, SUITE B-205
HOLLYWOOD, FLORIDA 33312-6543
(954) 985-8808 (BROWARD)
(954) 985-8839 (FAX)
WWW.LSZCPA.COM

How to Avoid Online Fraud

Fraud differs from identity theft. Stealing one's identity involves stepping into another's shoes, actually opening accounts and loans, then not paying. Fraud is stealing one's funds through forgery and/or use of unauthorized credit cards. Conducting business over the Internet exposes merchants to the greater risk of losses due to fraud. Therefore, risk management and fraud prevention must become a part of a merchant's e-commerce infrastructure.

The cost of fraudulent transactions can be very costly for the merchant, since they bear the brunt of charge backs. It's unlikely that the merchandise will be recovered in a fraudulent transaction; therefore, the cost of goods sold is more than sales. Other costs associated with the fraudulent sale are shipping costs, credit card and bank fees and administrative costs. These could add up to hundreds of dollars. Thus, the need for online fraud protection is prevalent.

Typically, merchants with "big ticket" items, such as electronics, jewelry and computers are in a higher risk situation for fraudulent orders. The risk is never the same for all products; therefore, being able to separate orders, customers and products is the key to minimizing risk efficiently. Fraud is a moving target with new schemes; therefore, the risk concentration and prevention must change accordingly. Of course, we need to weigh the cost of risk management versus maximizing sales. One method of minimizing fraud is not to accept international orders; however, that's a large market to loose. A better solution would be to have better fraud screening in place. Another verification mechanism that significantly reduces the chance of fraud is the deployment of card verification (the 3 or 4 digit number on a card).

The task of detecting fraud is a difficult one and we run the risk of rejecting some legitimate orders. An effective "front-end" screening process is one in which similar traits in orders are flagged and/or orders with email addresses associated with previous fraudulent orders. On a broader scale, orders shipped to an address other than the billing address with expedited shipping could be an indication of a fraudulent transaction. Even though online tools and programs are available for the initial screening, human intervention is still needed to determine whether or not an order is fraudulent. This interaction is time consuming, but a necessary step to ensure customer satisfaction and minimize lost sales.

Fraud will continue to evolve and merchants must always fine-tune their risk management software and policies to detect. Charge back orders of fraudulent transactions should be screened for patterns to look for in future orders. If a catalog is updated and promotional materials sent out, the volume of orders could contain fraudulent transactions; therefore, regular monitoring of the risk management screening methods is beneficial.

On the "flip side," we as consumers must beware of the fraudulent merchant. We must understand as much as possible about the merchant, feedback, delivery, valid email address, etc. Never give out your social security number or driver's license number. Be sure you are dealing with a secure site before entering your credit card number (yellow padlock and/or https). Don't invest in anything you're not sure about; do your homework to be sure the company is legitimate.

If you feel a fraud has been committed, a complaint can be filed at http://www1.ifccfbi.gov/cf1.asp.

November 2005