Five Tools You Can Use to Prevent Fraud

Reproduced from www.MerchantFraudSquad.com.

By Julie Fergerson
Co-Founder, ClearCommerce Corp.

As the co-founder of a company that creates e-commerce order processing software, I'm routinely asked about the types of tools that can help online merchants protect their businesses from fraud. Here I've outlined five that can help you:

1. Real-Time Credit Card Authorization
2. Address Verification Systems
3. Card Verification Codes
4. Rule-Based Detection
5. Predictive Statistical Model Software

While the first three tools are services available from a bank or credit card company, the last two are software packages you must purchase from software vendors. At the end of this article, I've provided some merchant rankings of these tools by their cost-effectiveness and success at fraud prevention.

1. Real-Time Credit Card Authorization

Obtaining a real-time authorization for a transaction from a credit card company is a good starting point for detecting and preventing fraudulent transactions. This will ensure that the credit card has not been reported as lost or stolen and that it is a valid card number.

However, an authorization does not tell you if the person using the card is authorized to use the card. There are many other tools that a merchant can use to anticipate a fraud, such as those discussed below.

2. Address Verification Systems (U.S. Only)

An address verification system (also called AVS) is a system that runs during the credit card authorization process. AVS will match the billing address provided by the customer with the billing address on file for that credit card.

This method is not foolproof, however. According to recent analysis by ClearCommerce, AVS returns a match in only about 40 percent of all transactions, when in reality a very small percentage of transactions are actually fraudulent. This means that many transactions that fail according to AVS are actually valid. Another important consideration is that 35 percent of the fraud cases examined by ClearCommerce matched addresses when run through AVS.

3. Card Verification Codes

Card verification codes (known as CVV2 for Visa, CVVC for MasterCard, and CID for American Express) are a fairly new way of verifying that a credit card is valid. For American Express, the code is a four digit number that appears on the front of the card above the account number. For Visa and MasterCard, the code is a three digit number that appears at the end of the account number on the back of the card. The code does not get printed on any receipts.

As a merchant, you can ask for this code on your online order form. In fact, MasterCard will require merchants to collect this information as of April 1, 2001.

4. Rule-Based Detection

With rule-based detection software, merchants define a set of criteria that each transaction must meet. Often called a "negative file," this set of rules can be based on past experiences, price limits, names, addresses, and the knowledge of human experts, such as risk analysts. These criteria should always maintain not only stolen credit card numbers, but also bad shipping addresses and shipping telephone numbers. The software will automatically screen incoming orders by these specific criteria and automate the decision to reject, review, or accept the order.

For example, a merchant might screen for unusually high dollar transactions, billing and shipping addresses that do not match (these are not useful for

businesses that cater more to gift-giving), an order for an unusually high number of one item, or names and credit cards that have been linked to fraud in the past.

5. Predictive Statistical Models

Predictive statistical model software analyzes data from millions of online sales to extract the profile of fraudulent transactions. Culling data from large, historical databases, the software develops a mathematical formula and applies it in real time to incoming transactions. Each transaction then receives a risk score based on its attributes.

Putting Them Together

All of the tools mentioned above are complementary to one another, as they each inspect different components of a transaction. The best way to combat fraud is to use layers of fraud protection. When using fraud tools, one plus one equals three-using more than one tool will usually yield better results than a using any tool alone.

Using a combination is also crucial for helping merchants reduce "insult rates"-rejection of a truly legitimate order. Each time this happens, you risk losing that customer and possibly some of their friends.

Costs and Effectiveness

Although a combination of tools is always a superior solution to any single tool, we've done a little research here at ClearCommerce about the overall effectiveness of each of these tools, as well as which tool is most cost-effective.

We asked 30 online merchants (this included both ClearCommerce customers and non-customers) to rank the tools they were using to prevent fraud in the order of most effective to least effective. We also asked them to rank the tools they were using based on which one was the "best bang for the buck." The results of this poll are summarized below.

Five Tools You Can Use to Prevent Fraud

Most Effective	Best Bang for the Buck
1. Rule-Based Detection	**1.** Rule-Based Detection
2. Real-Time Credit Card Authorization	**2.** Real-Time Credit Card Authorization
3. Card Verification Codes	**3.** Card Verification Codes
4. Statistical Models	**4.** Address Verification Systems
5. Address Verification Systems	**5.** Statistical Models

It's important to note that the costs for each of the tools listed above varies according to your type of business. You should also remember not to exceed the costs of fraud to your business when you are considering these tools. For example, if you lose $75,000 to fraud per year, and you can only recover $30,000 through fraud management tools, don't spend more than $30,000 on those tools.

Don't Forget Human Intervention

Finally, when you're trying to develop fraud prevention procedures, it is important to recognize that you can't always rely on technology-there may be a need to manually review a small percentage of orders. As we mentioned, merchants constantly balance the risk of accepting an order with the risk of losing the customer-in many cases, human intervention is still the best method.

You should also remember-because the majority of transactions you receive will be valid orders-that this extra effort can be an excellent opportunity to help you build a customer relationship that lasts a lifetime.

Julie Fergerson is co-founder of ClearCommerce Corporation. Based in Austin, Texas, the company develops e-commerce transaction software. If you'd like to ask Julie a question, send her an e-mail at julief@clearcommerce.com.