

## Best Practices for Internet Merchants

The following best practices, taken from various experts, are offered to help you avoid being victimized by Internet fraud. Experience suggests that there are certain characteristics that can be tip-offs to possible fraud. *Each of these characteristics by itself is very seldom cause for alarm*; rather, it's when several of these factors characterize an Internet purchase that you may be the target of a fraud scheme.

Be alert for transactions with several of these characteristics:

- **First-time shopper.** Criminals usually hit a merchant once, and don't go back a second or third time.
- **Larger-than-normal orders.** (This requires knowledge of what a "normal-sized" order is.) Because they may be using stolen cards or bogus account numbers that have a limited life span, those who may be conducting fraudulent activity need to maximize the size of their purchase.
- **Orders consisting of several of the same item.** As these items are intended for resale, having more of them increases the criminal's profits.
- **Orders made up of "big-ticket" items.** These items have maximum resale value and therefore maximum profit potential.
- **Orders shipped "rush" or "overnight".** Crooks want these fraudulently obtained items in their hands as soon as possible for the quickest possible resale, and aren't concerned about extra delivery charges.
- **Orders from Internet addresses making use of free e-mail services.** For these services, there's no billing relationship and often no audit trail or verification that a legitimate cardholder has opened the account.
- **Orders shipped to an international address.** A significant number of fraudulent transactions are shipped to bogus cardholders outside of the U.S. And the Visa Address Verification Service can't validate non-U.S. addresses.

These next several characteristics are ones that might require you to have knowledge of a number of the company's transactions. Ideally, there will be a database or account history files against which to compare individual sales for possible fraud.

- **Transactions on similar account numbers.** This is particularly useful if the criminals are using account numbers generated by a CreditMaster-type scheme.
- **Orders shipped to a single address but made on multiple cards.** These could also be characteristic of a scheme based on CreditMaster-generated account numbers or a batch of stolen cards.
- **Multiple transactions on one card over a very short period of time.** This could be an attempt to "run" a card until the account is closed.
- **Multiple transactions on one card or similar cards with a single billing address but multiple shipping addresses.** This could represent some organized activity, rather than one individual at work.
- **Multiple cards used from a single IP (Internet Protocol) address.** More than one or two cards could well indicate a fraud scheme.

What card-not-present merchants should do if suspicious:

- **Ask for a Code 10 authorization.** A separate phone call to your authorization center asking for a Code 10 authorization lets the center know you have concerns about a transaction.
- **Ask the customer for additional information.** For example, ask for day and evening phone numbers, and call the customer back later. Some merchants ask for the bank name on the front of the card.
- **Separately confirm the order with the customer.** Send a note via his/her billing address, rather than the "ship to" address.

### **The best advice of all**

Trust your instincts. If the sale seems too good to be true, it probably is. We hear all too often that what a merchant thought was a great sale turned out to be fraud. So check a little more into that huge order from a customer you've never done business with that was shipped to somewhere halfway around the world. That little bit of extra checking might well prevent you from being the victim of a fraud scheme.

### **Basic Card Acceptance and Fraud Control Procedures**

The growth of the mail order/telephone order (MO/TO) and Internet markets means increasing numbers of merchants are now processing transactions in situations where the card and cardholder are not present—and fraud may be especially difficult to detect. Authorization is required on all card-not-present sales, and MO/TO and Internet merchants should also be encouraged to develop in-house fraud control policies and provide appropriate training to their employees.

### **Ask for the card expiration date**

The *Visa U.S.A. Operating Regulations* states that where possible, card-not-present merchants should ask customers for the card expiration, or Good Thru, date. Including the date in your authorization request helps to verify that the card and transaction are legitimate. A MO/TO or Internet order containing an invalid or missing expiration date may indicate counterfeit or other unauthorized use.

### **Ask for CVV2 to confirm the cardholder has a genuine Visa card**

The Card Verification Value Service ([CVV2](#)) is a three-digit security number indent-printed on the back of Visa cards to help validate that:

- The customer has a genuine Visa card in his/her possession, and
- The card account is legitimate

To use CVV2, merchants simply ask card-not-present customers for the last three numbers in the signature panel on the back of Visa cards. This information is then submitted with other transaction data (card expiration date and account number) for electronic authorization. A CVV2 Result Code (generally, "Match" or "No Match") is returned with the authorization. The Code indicates whether or not the CVV2 code submitted matches the CVV2 code calculated by the Visa authorization system. If you receive a No-Match Result Code, you may want to re-submit the CVV2 with a zero-dollar authorization request to rule out the possibility of a key-entry error. Otherwise, a No-Match result should be viewed as a sign of potential fraud and taken into account with the remainder of the authorization response data (approval and AVS response).

CVV2 should never be stored as a part of order information or customer data.

### **Use AVS to check the cardholder's billing address**

The Address Verification Service (AVS) is an automated fraud prevention system that allows card-not-present merchants to check a cardholder's billing address as part of the electronic authorization process. Studies have shown that perpetrators of fraud in card-not-present transactions often do not know the correct billing address for the account they are using, so verifying the address can provide merchants with another key indicator of whether or not a transaction is valid.

To use AVS, simply ask card-not-present customers for their billing address as it appears on their monthly statement. This information is then submitted with other transaction data for electronic authorization. Address verification and authorization occur simultaneously—in a matter of seconds—and an AVS response code is returned with the authorization. The code indicates whether or not the address submitted matches the billing address on file with the account issuer. A "Partial Match" or "No Match" response should be viewed as a sign of potential fraud, and the customer's order should be held until the merchant can verify that the transaction is, in fact,

legitimate.

### **Train employees to recognize suspicious orders and customer behavior**

Card-not-present merchants should also develop in-house policies and procedures for handling irregular or suspicious transactions—for example, unusually large orders—and provide appropriate training for their sales staff. Being able to recognize suspicious orders may be particularly important for merchants involved in telephone sales, and employees should be given clear instructions on the steps to take to verify these transactions.

### **Suspicious cardholder behavior**

Telephone-order sales employees should be on the lookout for any of the following signs of suspicious customer behavior:

- **Rush orders:** Urgent requests for quick or overnight delivery—the customer who "needs it yesterday"—should be another red flag for possible fraud. While often perfectly valid, rush orders are one of the common characteristics of "hit and run" fraud schemes aimed at obtaining merchandise for quick resale.
- **Random orders:** Watch out also for customers who don't seem to care if a particular item is out of stock—"You don't have it in red? What colors do you have?"—or who order haphazardly—"I'll take one of everything!" Again, orders of this kind may be intended for resale rather than personal use.
- **Suspicious shipping address:** Scrutinize and flag any order with a ship-to address that is different from the billing address on the cardholder's account. Requests to ship merchandise to post office boxes or an office address are often associated with fraud. In addition, merchants should keep lists of zip codes where high fraud rates are common and verify any order that has a ship-to address in these areas. If your business does not typically service foreign customers, use caution when shipping to addresses outside the U.S.—particularly if you are dealing with a new customer or a very large order.

In examining what appears to be an unusual order, keep in mind that if the sale sounds too good to be true, it probably is.

### **Order Verification Procedures**

If you become suspicious about a card-not-present order, try to verify the transaction by asking the customer for additional information. These requests should be made in a conversational tone so as not to arouse the customer's suspicions. If the customer balks or asks why the information is needed, simply say that you are trying to protect cardholders from the high cost of fraud.

The following steps may help to verify card-not-present transactions:

- **Ensure the customer is in possession of the card.** Ask the customer for the name of the issuing bank shown on the card or for the printed four-digit number on the face of the card. Any hesitation in providing this information may mean that the customer is not in possession of the card and is using a stolen or counterfeit account number.

Another way to find out if a card is present is to ask the caller if the account number appears on the signature panel on the back of the card. If so, ask for the Card Verification Value 2 ([CVV2](#)), the three-digit code at the end of the account number.

**Check the customer's personal information.** Request day and evening telephone numbers and verify them through directory assistance or by calling the customer directly. If possible, you should also compare the billing and ship-to address on the

order with the address you used for mailing the customer any catalogs or other marketing materials.

## **Data Security**

In today's environment where valid account numbers have become a highly marketable commodity, data security should be a central concern for merchants and a key component of all policies and practices related to the acceptance and processing of transactions. The Visa U.S.A. *Operating Regulations* states that merchants are responsible for ensuring that account information is stored in secure areas with access limited to authorized personnel. In addition, merchants are prohibited from storing magnetic stripe information following a transaction or from disclosing cardholder data to anyone—except if it is needed by an acquirer, issuer, or third-party processor to complete a sale. A merchant's data security policies should also be designed to prevent fraud scams involving collusive employees. Whenever possible, account numbers should be encrypted or scrambled during transaction processing, and electronic equipment—such as laptop computers—that can be used to steal or replicate account information should not be allowed in the workplace.

## **Additional Requirements for Internet Merchants**

### ***Web Site Requirements***

The merchant's web store must contain specific information that is dictated by the card associations. Some of these are:

- Complete description of the goods or services offered
- Returned merchandise and refund policy
- Customer service contact, including Electronic Mail Address and/or telephone number
- Transaction currency (e.g., U.S. dollars, Canadian dollars)
- Export or legal restrictions (if known)
- Delivery policy

### ***Authorization and Clearing Requirements***

An electronic commerce transaction must be identified in both the authorization request and clearing record with the appropriate Electronic Commerce Transaction indicator values.

### ***Retrieval Request Requirements***

- Merchant Name
- Transaction Amount
- Transaction Date
- Purchaser Name
- Authorization Code
- Transaction Type (Purchase or Credit)
- Description of Merchant
- Return/Refund Policy (if restricted)
- Unique Transaction Identifier
- Code that identifies transaction as a Customer Payment Services (CPS) transaction

## **Processing Costs**

In addition to the gateway costs outlined above the merchant will also see the traditional charges of discount rates and transaction fees. Today the card associations see Internet transactions as a MOTO (Mail Order/Telephone Order) type transaction, thus they reflect these higher fees.

**Some parameters to consider**

- E-commerce transactions qualify for CPS/Card Not Present
- Card Not Present/Signature Not Obtained
- Or Address Verification Required.
- Authorization must be within 7 days of transaction date
- Invoice number required
- Authorization amount must equal transaction amount