Fraud Protection Tips

To Protect Your Business

Keeping Customer and Card Information Safe

In today's increasingly electronic business world, keeping credit card and customer information confidential is progressively more important - and difficult. The Card Associations (Visa®, MasterCard®) mandate that all merchants maintain the highest information security standards, and it's just good business practice to be vigilant with your customers' information. Fraud comes in all shapes and sizes, and while non face-to-face transactions may carry a higher potential for fraud, it can happen in retail storefront businesses too.

To help you be mindful of the various forms fraud can take, the Merchant Services Loss Prevention Team has developed some tips and guidelines to help you protect your business.

"Code 10" - Your First Line of Defense

Whether you sell goods and services in a face-to-face environment, or via mail, phone or Internet, you can employ a "Code 10" authorization to verify additional information on a suspicious transaction. You may be prompted by your processing terminal to call for voice authorization of the charges (CALL AUTH, CALL CENTER), or you may simply not feel right about the transaction. In either case, you can use "Code 10" to gain additional information before you release your merchandise.

How to use "Code 10"

Call the voice authorization phone number 1-800-525-5093.

Choose the prompt for "Code 10". You will be transferred to a voice authorization representative and will be asked a series of questions about the transaction.

NOTE: Never call a phone number for the card issuing bank provided by a customer, or let the customer call the card issuing bank for you to obtain an authorization code. Do not accept an authorization code given to you by a customer. Any authorization code obtained from any source other than our Authorization Center cannot be verified.

If the order is a mail order, phone or Internet sale, be prepared to provide the cardholder name, billing address and shipping address. The representative will attempt to verify the information you provide with the bank that issued the card to the customer.

The representative will attempt to verify the cardholder information during your call. If this is not possible, the data will be forwarded to an investigator for further research. We will attempt to contact you within 24 - 72 hours with the current status or results of the investigation.

If an authorization request is declined, request another form of payment other than a credit card. Do not split a declined transaction into smaller increments to obtain an authorization.

Obtain an authorization code for the full amount of the sale. Always obtain the authorization code **before** shipping the merchandise.

An authorization code does not guarantee that a transaction will not be disputed later. An authorization code simply identifies that the amount of credit requested for that particular transaction is available on the card at the time of the sale. An authorization code does not protect you in the event of a chargeback regarding unauthorized transactions or disputes involving the quality or delivery of goods and services.

It is highly recommended to use Code 10 before charges have been placed on the credit card and **before the product has been shipped.** Doing so will allow you to avoid being billed for processing fees and loss of shipping costs on the transaction in question. Please note that you may still request a "Code 10" if the product has been shipped, but your chances to recover the product will be reduced.

CUSTOMER FRAUD:

Look Out For Suspicious Behavior and Requests

As fraudsters become more sophisticated, so do their schemes. Particular favorites target transactions that most often happen via phone or email. Here are some examples to watch out for at your business.

- **Relay Calls** - A relay call is an operator-assisted telephone call, usually used by someone who is hearing impaired. While this is a valid service, criminals have also used the service to place fraudulent orders. We recommend you request a "Code 10" authorization request for all orders obtained via relay call.
- **Bulk Orders** - Customers ordering large quantities of the identical or similar items. You should also be cautious of large bulk orders with a delivery address of an apartment or self-storage unit.
- **Multiple Cards** - Customers who provide multiple card numbers for the same purchase, especially when the card numbers are different by only the last few numbers.
- **Money is No Object** - Requests for overnight delivery, without regard to cost.
- **Immediate Shipment** - Customers who request immediate processing of the order and want the shipment's tracking number ASAP.
- **Immediate Pick Up** - Customers who place phone orders, request immediate processing of the order, and then advise they will have someone come to the store to pick up the product.
- **Alternate Deliver Address** - Requests for delivery to an address other than the billing address, or delivery to a freight forwarder. (Criminals will use United States based re-shippers to avoid detection of foreign shipments.)
- **Not Sold Here** – Telephone or online requests for merchandise you do not sell. Most common requests are for cell phones and laptop computers.
- **Free Email Orders** - Communication via a free email service (Yahoo, Hotmail, Gmail, etc).

Other Schemes to Watch For

- **Excess Funds Request** - A customer may request that you to process a VISA®/MasterCard® transaction for an amount greater than the purchase price of the goods or services and then request the excess funds be sent by wire transfer, money order or Western Union®, to a freight forwarding company or other person. There is a high probability of fraud in such a transaction and there is little chance for your business to recoup funds. This type of transaction is also a violation of VISA®/MasterCard® regulations, so you would not have the ability to favorably resolve a chargeback, should it occur.
- **Counterfeit Check Scheme** – The fraudster overpays for goods or services with a counterfeit check and requests you to wire transfer the difference back to them or an accomplice. This scheme has been reported on personal checks, business checks, cashier's checks and money orders. It results in a loss of both the merchandise and the cash overage.
- **Fraudulent Customer ID** - With today's technology it is possible to alter a photocopy of a credit card or personal identification such as a driver's license or passport. Sometimes a fraud order will include a faxed or e-mailed photocopy of the card to gain your trust. These photocopies do not guarantee that you are dealing with the correct cardholder. Always verify the order information with the authorization center before proceeding with the order.

Hot spots For Fraud

Fraud is no longer localized. Businesses across the globe can be subject to schemes that originate far from their locales. Current hot spots where mail order, telephone order, and Internet fraud are likely to originate include:

- **West Africa: Nigeria, Ghana, Gambia**
- **Asia: Indonesia, Singapore**
- **Eastern Europe: Bulgaria, Romania, Russia**

EMPLOYEE FRAUD

The Threat Within

Unfortunately, sometimes the fraudsters you must guard against are right inside your own organization. Employee theft of customer information is a growing challenge for businesses.

A number of advances in technology have made it easy for unscrupulous employees to steal customer credit information. Lax security procedures can also allow employees to pilfer or misuse the data. Here are some typical ways employees can perpetrate credit card fraud:

• **Process a Credit Transaction to Their Own Account** - Employees may issue credits to their own credit card or to an accomplice's card using the Merchant's POS device utilizing funds meant for the merchant's direct deposit account. Often these credits do not have an offsetting sale.

• **Record Card Numbers** - Employees may pocket receipts left behind by cardholders or may copy card numbers onto another piece of paper. Point of sale (POS) terminals that truncate the card number on the customer's receipt can help your business avoid this type of fraud.

• **Use of Card Skimmers** - A dishonest employee can steal valuable information right off a customer's card through use of a small, battery-operated "card skimmer." This hand-held device reads a card's magnetic stripe and records the cardholder data for later download to a computer. From there, the numbers can be used to make unauthorized purchases or create counterfeit cards. Some card companies offer a reward for information leading to the arrest and conviction of anyone involved in the manufacture or use of counterfeit cards.

Other Suspicious Employee Activity

Employee fraud can take other forms as well. Sometimes, it doesn't directly involve processing a card transaction. Here are some examples of suspicious activity that may be clues to employee theft:

• Deposits made outside of procedural time frames (i.e. daily deposits not occurring daily)
• Deposits not received by your bank (cash, check)
• Credit card receipts not retained as per company policy
• Customer complaints of payments not being applied to their accounts or only partial payments being applied
• Frequent errors applying customer payments
• Discrepancies between deposit receipts obtained from bank and deposit receipts kept internally
• Decrease in volume of cash received while other payment type volumes remain unchanged
• IOU's in cash reserves or "petty cash"
• Employees' personal checks in reserves used to balance reserve amounts

Employee Fraud Prevention Tips

Most terminals or transaction software tools allow a merchant to require a password in order to process a credit transaction, and there are a number of other tactics you can use to prevent employee fraud, including:

• Reconcile your work daily rather than monthly
• Password protect your POS Device and other payment processing equipment, if this feature is available
• Password protect the credit function on your POS device
• Secure your POS Device during non business hours
• Have a separate authorizer of credits in addition to the person who physically processes a credit
• Make sure all credits have accompanying documentation of customer information and reason for return or dispute
• Match credits to returned or disputed goods or services, verify with customers that they did actually return / dispute goods or services
• Have more than one person review monthly statements
• Review credits daily, or have a trusted employee do the review
• Fully investigate credits without matching sales
• Review any batches with negative dollar amounts (more credits than sales)
• Conduct quarterly internal audits as well as at random times and intervals
• Track credits by card number, terminal number, employee, frequency, and dollar amount (exception based reporting)
• Review any volume spikes in credit / return / dispute activity
• Review your monthly statements with your physical inventory
• Protect your passwords and verify internal access controls for online account reporting, and checking account change requests

POS device safety features

Today's credit card terminals have built in security features to help protect against fraudulent transactions. Some features are installed, but optional, so to take full advantage of built-in prompts for fraud prevention, be sure to have the options turned on. Call **Accept Credit Cards 1-800-476-5020** to verify that your solution can support these security features, and to verify that they are installed. You may need a download to your existing device to activate these security features.

- **Address Verification System (AVS)** - Your terminal can be set up for the AVS program, which allows you to include an address verification request with a transaction authorization request, and enables your non face-to-face transactions to qualify at better rates. You receive a separate result code indicating whether the address given matches the address the credit card issuer has on file for that account.
- **VISA Card Verification Value (CVV2) and MasterCard Card Validation Code (CVC2)** – These verification requests can be added to most terminals. This system will verify the three-digit code printed on the back of a credit card in the signature panel. You will receive either a "match" or "no match" response from the card-issuing bank if the validation code is provided at the time of the authorization.
- **The response codes for both AVS and CVV2/CVC2 are independent of the approval code.** You may receive a positive approval code but the AVS and CVV2/CVC2 response did not match. It is important to review all responses to make the best decision.

AVS Response Codes

CODE	DEFINITION
A	Address (street) matches - ZIP Code does not
B	Street address match, postal code in wrong format (international issuer)
C	Street address and postal code in wrong formats
D	Street address and postal code match (international issuer)
E	Error response for Merchant Category Code (SIC)
G	Card issued by a non-U.S. issuer that does not participate in the AVS system
I	Address information not verified by international issuer
M	Street address and postal code match (international issuer)
N	No match on address (street) or ZIP Code
O	No response sent
P	Postal codes match, Street address not verified due to incompatible formats
R	Retry, system is unavailable or timed out
S	Service not supported by issuer
U	Address information is unavailable (domestic issuer)
W	Nine-digit ZIP Code matches - Address (street) does not match
X	Exact AVS Match
Y	Address (Street) and five digits Zip match
Z	Five-digit zip matches - address (street) does not match

CVV2/CVC2 Response Codes

CODE	DEFINITION
Space	CVV2 processing not requested
M	CVV2/CVC2 Match
N	CVV2/CVC2 not matched
P	Not processed
S	CVV2 should be printed on the card, but it was indicated that the value was not present
U	Issuer does not support CVV2
X	Service provider did not respond

The use of CVV2, CVC2, and AVS can lessen a non face-to-face transaction's risk of fraud by providing additional information on which you can make a better business decision. However, CVV2, CVC2, and AVS do not eliminate chargebacks, nor absolve your business of liability for chargebacks associated with processing credit card transactions.

For more information about AVS and CVV2, CVC2, call Accept Credit Cards 1-800-476-5020. If you are an Internet merchant, contact your web provider for additional fraud settings that may be available to you through their service.

Telemarketers and door to door salespeople are engaging in fraudulent or high-pressure sales tactics have become a problem in our industry, and it is a problem that Accept Credit Cards would like you to have all the facts about. How serious is it?

The **Federal Trade Commission**, the U.S. Postal Service, and local Better Business Bureaus nationwide have judged the problem serious enough to issue warnings about so-called "high pressure" practices, and in some cases, investigations have led to lawsuits against deceptive companies.

Accept Credit Cards' main concern is for our customers who have placed their trust in our services. The most serious concern for Accept Credit Cards customers is the likelihood that equipment, supplies and services sold by these companies may not be legitimate and might damage the equipment or significantly increase your fees. However, equally important for our customers is the bottom line: Even though deceptive telemarketers and door to door salespeople say that the prices they offer are exceptionally low, in fact the opposite is usually true; **the prices are often grossly inflated.**

Since they never retain customers, these practitioners must make all the money they can on the first sale. Their business depends on using high pressure and deception to make a lot of sales fast.

Here's what to watch out for:

1. The caller is not the salesperson you normally deal with.
2. The caller tries to avoid giving their phone number.
3. The sales pitch is high-pressure, with a time element—if you don't "act now", the price being offered will change.
4. These operations often get information about your equipment by pretending to be a legitimate Customer Service representative making a customer satisfaction survey. Once they know the machines you are using, a salesman will call back with the pitch tailored to your equipment.

Here's what to do:

1. Always call **(800) 476-5020** to verify that you are dealing with an Accept Credit Cards agent or service technician
2. Get their phone number, if it not **(800)476-5020** they may be attempting to defraud you. Call us immediately. Most deceptive telemarketers will not give out their phone number.
3. If the caller or door to door salesperson is unfamiliar but claims to be from Accept Credit Cards, call us.
4. If you come in contact with one of these scams, report it to the Federal Trade Commission, the Postal Service or your local Better Business Bureau.

More about Fraud Prevention

Here are helpful websites and toll free numbers to provide more information and assistance on avoiding credit card fraud in your business.

www.visa.com - Includes tips, regulations, news and fraud features from VISA. (Choose option for Merchants/Businesses.)

www.mastercard.com - Includes tips, regulations, news and fraud features from MasterCard. (Choose option for Merchants.)

http://zip4.usps.com/zip4/welcome.jsp - United States Postal Service website to validate an address physically exists. This does not confirm that a person lives at the address, but does confirm the address is real.

www.ic3.gov - Internet Fraud Complaint Center (IFCC) The IFCC is a partnership between the FBI and the National White Collar Crime Center. This site allows victims of Internet fraud to report fraud online to the appropriate law enforcement and regulatory authorities.

www.forwarders.com - This is a list of freight forwarders. Many times international criminals will ship to these addresses and have the order sent on to its final destination(s) by the freight forwarding company.

VISA Merchant Verification Service: 800-847-2750 (AUTOMATED)
Option 1, Address Verification: enter in the numeric portion of the street address, zip code, and VISA card number and it will advise you if there is a match. Option 2, Issuing Bank Phone numbers: enter the VISA card number and it will provide you with the 800 number for the issuing bank if available.

MasterCard Assist: 800-622-7747
Select your language preference, then Option 2. Enter the MasterCard card number and it will provide you with the 800 number for the issuing bank if available.

Discover Address Verification: 800-347-7988 (AUTOMATED)
You will need your Discover Merchant number. Enter the Discover card number and address information, and it will advise you if there is a match.

American Express Address Verifications: 800-528-2121
Option 3 allows you to verify the name and address of a particular AMEX card number.

These Fraud Prevention Tips are not an amendment to your Merchant Processing Agreement, the Terms of Service, or the Merchant Operating Guide, governing your processing relationship with NOVA Information Systems, Inc. These Fraud Prevention Tips are provided to you to enhance your awareness of circumstances in which potential fraudulent activity may occur and offer suggested measures to you to combat, reduce, or minimize the impact of the acceptance of fraudulent transactions. NOV-FPT550 Rev0707