



First National Merchant Solutions *Fraud Prevention Tips*

RETAIL

In order to prevent fraud from lost, stolen or counterfeit cards, the following procedures should always be adhered to at the point-of-sale:

- **Check the last four digits of the card account number.** If they do not match those on the receipt or on the terminal display, call the authorization center for a code 10. Key-enter the account number of a card only if the card cannot be read electronically. Always make an imprint of the card if a transaction is key entered.
- **Check the signature panel.** If the signature panel is not signed, ask the customer to sign the card. In addition, ask to see a piece of government identification such as a driver's license or passport. When the customer signs the card, compare the signature on the card to the signature on the receipt to make sure they match. If they do not match, call for a code 10.
- **Inspect the embossing.** The first four digits of the account number should be printed directly above or below the first four embossed digits of the account number.
- **Examine the hologram.** Make sure the hologram is clear and three-dimensional.
- **Hold the card throughout the transaction.** Doing this ensures that the point-of-sale staff is in control of the transaction.
- **Respond to "CALL" message.** If a "Call" message is displayed on your terminal after swiping the card, immediately call the voice authorization center and tell the operator, you are responding to a "Call" message and follow the operator's instructions.
- **Take your time.** Do not let a hurried customer cause you to disregard proper point-of-sale procedures.

Watch for Suspicious Behavior

While most of these behavior patterns can be observed during a normal transaction, point-of-sale staff should be alert for cardholders who:

- Purchase an unusual amount of large ticket items.
- Produce the card from a pocket rather than a wallet or purse.
- Cannot provide identification when asked.
- Attempt to hurry the transactions (especially close to store closing time).
- Purchase large ticket items and insist on taking them home immediately even if delivery is included with the sale.
- Make several small purchases in an attempt to stay under the floor limit of the transaction or ask what the floor limit is on the card.
- Charge high-ticket items on a card with a recent valid date.
- Appear nervous throughout the sale.



Returns and Exchanges

In the instance where a customer requests a refund for returned merchandise at your location with a Visa or MasterCard card, you must prepare a credit card voucher to properly credit a cardholder's account. Properly crediting cardholders is an important aspect of preventing fraud from occurring at your business location.

To prevent fraudulent retail credit transactions:

- ***Do not give cash refunds for merchandise purchased with a Visa or MasterCard.***
- ***Do not credit refunds to any Visa or MasterCard card other than the card used for the original transaction.***

Note: Visa and MasterCard do not require you to refund a transaction if your business' merchandise return and exchange policies are clearly disclosed to customers and written on sales receipts as "No Return," "In-Store Credit Only," or "Exchange Only."

Code 10 Actions

The majority of day-to-day electronic transactions are processed without question or suspicion of fraud. However, there are some instances where the transaction should be scrutinized due to unusual circumstances. If your point-of-sale staff receives an electronic authorization approval, but still suspects fraud, advise them to:

- **Keep the card in hand.**
- **Call your voice authorization center and say, "I have a Code 10 Authorization Request."**
- **Follow the operator's instructions.**
- **If you are instructed to keep the card, do so only if you can by peaceful means. Remember that your safety always comes first!**
- **Notify a customer service representative that you have recovered a card and ask for further instructions. You may be eligible to receive a cash reward.**

Before sending a card to First National Merchant Solutions, cut the card in half lengthwise without cutting the magnetic stripe, the account number, or the hologram.

DIRECT MARKETING

In a card not present environment, even though you cannot see the customers' card, adhering to some simple procedures while taking an order may be the difference between being victimized by fraud or preventing fraud. New technology such as **Address Verification Service (AVS)**, **Card Verification Value 2 (CVV2-Visa)** and **Card Validation Code 2 (CVC2-MasterCard)** exist today to help reduce fraud in the card not present environment. These tools should be utilized to reduce fraud at your business.

During the order taking process, ask the customer for:

- The card account number embossed on the face of the card.
- The card's expiration date.

Then ask the customer to:

- Turn the card over and read the last three digits, which trail the account number printed in the signature panel (this is the **CVV2** or **CVC2** code).

Note: Merchants who request the CVV2 or CVC2 code will receive a “match” or “no match” response when entering the transaction into a terminal for processing.

If you are suspicious:

- Ask for the four-digit number printed directly above or below the embossed account number. This number **must** match the first four digits of the embossed number. If the cardholder cannot find the four-digit printed number or if the number given does not match the account number, do not accept the card.
- Ask for the account number and expiration date of the card being used. All Visa card account numbers begin with the number “4” and MasterCard numbers begin with the number “5”-whether or not the account number is 13 or 16 digits in length. If the cardholder says it is a Visa card and the account number begins with a 5, it is not a Visa card, or vice versa.

Other suggestions for combating **Mail Order/Telephone Order** fraud at the point-of-sale:

- Ask the caller for the name of the card-issuing bank on their card and attempt to validate the first six digits of the card account number against the issuing bank's Bank Identification Number (BIN). This may deter a criminal who is not in possession of the card.
- Ask the caller for daytime and evening phone numbers in case information needs to be verified at a later date.
- Identify trends of past fraudulent occurrences. Use this information when accepting orders.
- Create a negative file containing addresses from which your company has suffered losses. Verify each address against this file.
- Modify your authorization system to alert the phone order representative when a “bad” account or address is entered.
- Question suspicious behavior such as apprehensiveness, indiscriminate ordering of fraud-prone merchandise (high-ticket items) or background noise which may indicate a public telephone is being used.
- Ask if you can call the caller back if you are suspicious. Or call directory assistance to verify the phone number.



ELECTRONIC COMMERCE

When processing electronic commerce transactions, be alert for:

- **A first purchase**, which is also typically the sole purchase made, allowing criminals to minimize the possibility of identification associated with recurring purchases.
- **Larger than “normal” orders** that maximize purchases on time-limited stolen or bogus payment card accounts.
- **Orders consisting of multiples of the same item or “big-ticket” items** that maximize resale value and profit potential.
- **Orders shipped “rush” or “overnight”** to deliver fraudulently obtained items as soon as possible for quick resale.
- **Orders from Internet addresses using free e-mail services** that do not require a billing relationship or verification that an account was opened by a legitimate cardholder.

Develop and maintain customer databases to track buying patterns and identify changes in buying behavior such as:

- **Transactions charged to similar account numbers** as fake account numbers generated by fraud schemes tend to be in sequential order.
- **Orders shipped to a single address but made on multiple cards** to maximize resale value and profit potential.
- **Multiple transactions charged to one card, over an extremely short period of time** to maximize usage on an account before it is closed.
- **Multiple transactions on one card or similar cards with a single billing address but multiple shipping addresses** that indicates fraudulent activity by an organized, large scale group.
- **Multiple cards used from a single IP (Internet Portal) address** to maximize purchases and profit potential.

By adhering to the above mentioned card acceptance procedures, your business can substantially reduce fraud associated with all types of transactions. As always, First National Merchant Solutions is dedicated to providing our processing clients with information, which will assist in the reduction of fraud at your business location.

Please contact your national account manager with questions regarding fraud prevention.