Avoiding Fraud

Learn to recognize the warning signs for fraud and follow these card acceptance guidelines to reduce your risk.
INTRODUCTION

Fraud comes in many forms and hurts merchants of all sizes. Whether you have a brick and mortar business, an ecommerce site, or a combination, you’re at risk for fraud. Vaniv monitors our merchant accounts for signs of fraud, but you and your employees are your business’ first line of defense. Read the following tips and guidelines to help protect your business.

DON’T BE BULLIED

If a customer attempts to intimidate a cashier by causing a fuss at the register, it may be to rush the purchase, which may lead to improper checkout. They may tell you that the card won’t read and not to bother running it through—that you’ll have to key it in manually. In such instances, customers have also been known to complain about the service or length of the line. They may even demand to see a manager—anything to keep the cashier’s attention off the authorization of the credit card.

Never call a telephone number given by the cardholder for authorization. Don’t be intimidated by these bullies; always take your time and make sure the correct procedure is followed when authorizing the card.
BORROWED CARDS

Beware of people presenting letters of authorization for use of a credit card. Under no circumstances are these letters an acceptable form of verification or authorization. Friends, coworkers, children and spouses are not permitted to borrow each other’s cards. The only person who should be presenting the card to you is the person whose name is on the front of the card and signature on the back of the card. Most often, the rightful owner gets the statement and a chargeback inevitably occurs.

THE MANUAL KEY-IN

Often fraud occurs when the thief damages the card on purpose so that you are forced to manually enter the number in the electronic point-of-sale terminal. Fraudulent cards are often damaged in order to bypass the antifraud features that are placed on them—the magnetic stripe cannot be swiped and transmitted to the verification center for authorization in the case of a manual key-in.

If you have an electronic point-of-sale terminal, swipe every card that is handed to you, no matter how damaged or worn. Be wary of customers who let you know right away that their card won’t read. If the card doesn’t work and you end up keying in the number, make sure you take an imprint of the card. If the card is severely damaged, simply ask for another form of payment.

FRAUDULENT RETURNS

It is estimated that, on average, nine percent of merchandise returns are fraudulent. Make sure your employees and customers are well informed of your return policies and monitor return activity by using the MercuryView® online portal reporting tools.
COUNTERFEIT CARDS

Stolen and counterfeit cards are a costly problem for merchants and credit card issuers alike. Because of the technology available to them, counterfeiters are able to reproduce false cards that are high quality, even without the benefit of the original. All they really need is personal information and technology to produce credit cards, debit cards, and smart cards.

THE PURPOSE OF CODE 10

Any time you have doubts about something—a fraudulent card, a signature or even a customer’s behavior—call in a Code 10. A Code 10 allows you to call for an authorization without the customer becoming suspicious.

After dialing the authorization center, inform the operator that you have a Code 10. The operator will put you through to the correct person, who will ask you a series of “yes” or “no” questions. Hold on to the card if possible while making the call. If the operator decides something is amiss, he or she will deny authorization. The operator may even request to speak to the cardholder to ask account information questions that only the true owner of the card would know.

A Code 10 can be used any time you feel a transaction may not be legitimate, even if you have already received approval on a transaction or if the customer has already left the premises.
WHEN TO CALL IN A CODE 10:

- If the embossing on the card is illegible.
- If the last few numbers are not embossed on the hologram, or if these numbers do not match the account number on the sales draft or at the terminal.
- If there is no Bank Identification Number (BIN) above or below the first four digits.
- If the name on the card does not match the signature or there is a misspelling.
- If the hologram is not clear or the picture in the hologram does not move.
- If the card does not have an expiration date.
- If the card does not start with the correct numeric digit (all Visa® cards should start with a 4, all MasterCard® cards with a 5).
- Be aware of cards that don’t swipe; check these cards for other security features.
- If a card does swipe, make sure the card number and the number that appears on the terminal match.
RISKY BUSINESS

Card processors like Vanity monitor merchant transactions for signs of fraud or abuse. This protects merchants and cardholders. Certain kinds of merchant behavior are not allowed and could result in the termination of your account.

Don’t ever use your own card to give yourself a cash advance. If you need to perform a transaction that is out of character for your business, give us a call first. For example, if you are a restaurant that typically does $30 swiped transactions, call us before you run a $5,000 sale for a catered wedding.

TIPS ON FRAUD PREVENTION

1. If a photograph of the cardholder is present on the card, merchants should compare the photograph on the card with the person presenting the card.

2. Merchants should check cards for the hologram. A hologram is a three dimensional symbol in either gold or silver foil that is designed to help deter counterfeiting. The image should reflect light and appear to move when you tilt the card. NOTE: The Visa hologram is an image of a dove; the MasterCard hologram is an image of a world map; the Discover® hologram has four distinct images.

3. Merchants should check cards (including the signature panel) to see if they have been altered.

4. Merchants should check the valid date (some cards are not valid until the date shown) and the expiration date on the face of the card. If the card is not yet valid or expired, the card acceptor should not accept the card and should instead ask for another form of payment. NOTE: Cards are valid through the last date of the month, unless an exact date is displayed.
For each card type, merchants should be aware of the first four digits and the total number of characters. NOTE: A Visa-branded card number begins with a “4” and has 13 or 16 digits; a MasterCard-branded card number begins with a “5” and has 16 digits; a Discover card number begins with a “6” and has 16 digits.

Merchants should check the first four digits of a card. For Visa and MasterCard, the first four digits of the embossed card number must match the four digits printed above or below that number on the front of the card.

The account number on the front of the card should match the number printed on the back of the card in the signature panel. For Visa, American Express® and Discover, merchants should compare the entire account number imprinted in the signature panel with the embossed account number on the face of the card.

For MasterCard, merchants should compare the four-digit truncated account number imprinted in the signature panel with the last four digits of the embossed account number on the face of the card.
For MasterCard, merchants must contact their acquirer for instructions if:

- Merchants believe there is a discrepancy in the signature.
- The last four digits of the embossed account number do not match the four digit truncated account number on the signature panel or displayed on the terminal.
- The photographic identification is uncertain.

If any MasterCard does not have a MasterCard hologram on the lower right corner of the card face, merchants must confiscate the card and contact their acquirer’s Code 10 operator for instructions on card pick-up and mailing.

Merchants should attempt to swipe every card through a POS terminal. If the terminal cannot read the card, merchants should take a manual imprint of the card. When using a manual imprinter, merchants should check the draft for a clear impression of the card to ensure that they have captured the embossed card account number.

Merchants should also complete the draft with the date, description of merchandise/service, sales tax, total dollar amount and authorization number, and get a signature.
Merchants should never allow customers to tell them how to “get the transaction to go through” (for example, by doing a ticket only transaction without getting an authorization). This will result in a chargeback, and these customers will have “stolen” or obtained items for free.

Merchants must obtain customers’ signatures. The signature on the draft must match the signature on the back of the card.

If a customer’s card is unsigned, merchants should request another form of identification with a photo and signature. Merchants should request that the customers sign their cards and then compare the two signatures.

If customers refuse to sign, merchants should inform them that they are unable to accept an unsigned card for payment and then request another form of payment. The card association rules dictate that card acceptors must not complete the transactions if cardholders refuse to sign the card.

Visa, MasterCard, and Discover’s websites provide materials designed for merchant use and offer tips on what merchants can do to prevent fraud.
TIPS ON FRAUD PREVENTION CONTINUED

11. Use caution when taking an overseas order. Fraudulent transactions that originate overseas are on the rise. Remember that international transactions are high-risk transactions. Know your customer. Properly identify the person with whom you are dealing. Take a second look at what is being ordered and where it is being shipped. Did your customer offer you multiple cards as payment? Is the customer asking for immediate shipment? If so, you may have just detected a fraudulent transaction and saved yourself from taking a loss. There is a tremendous amount of fraud with international transactions, and it is virtually impossible to win the chargeback case. Banks outside the U.S. may not support additional security features like AVS, CVV2, and Verified by Visa®. If in doubt, do not hesitate to contact Vanity and we will be happy to assist you.
Utilize security functions such as entering the “last four digits” of the card on swiped-card transactions and Address Verification and CVV2 code to discourage use of counterfeit cards. Verified by Visa and MasterCard SecureCode are payment initiatives designed to reduce the risk of unauthorized use of cardholder account by authenticating the cardholder attempting to make a purchase online. Authentication makes internet shopping better and safer for both buyers and sellers by reducing the merchant’s exposure to fraud and frivolous disputes, and protecting the cardholder from fraudulent use of his/her card. Implementing Verified by Visa shifts liability away from the merchant and onto the card issuer.

If you are going to run an unusually large transaction, or if you need to manually key numerous transactions when you usually swipe your credit cards, call ahead to let Vanitv know what you are doing. Otherwise, your account may be flagged for unusual and suspicious activity, which may cause your funds to be held.