Card Acceptance Best Practices

Playing it Safe at the Point of Sale

Fraudulent activity costs U.S. businesses billions. And that is just lost revenue. When you consider the associated damage to reputations, the cost of fraud is astronomical. And it keeps growing.

In spite of technological advances and other developments, criminals are still finding ways to carry out fraudulent activity – especially those targeting POS systems. Should they come your way, there are steps you can take to lock them out and limit your risk.

- **Recognize the warning signs.** They are different for card-present and card not-present transactions. Make sure you and your employees know what they are.
- **Follow best practices.** Ensure everyone with customer contact knows how to properly accept a card for payment and follows best practices outlined below. Best practices are different for chip and magnetic stripe card-present and card-not-present transactions.

Card-Present Transactions

Having a card available for payment does not always ensure a safe transaction. There are several warning signs, and best practices to prevent card-present fraud.

Warning Signs of Card-Present Fraud

Certain customer behaviors could point to card fraud, but don't necessarily indicate criminal activity. Become familiar with your customers and let your instincts steer you in the right direction.

Watch for customers who:

- Purchase a large amount of merchandise without regard to size, style, color or price
- Try to distract or rush you during the sale
- Make purchases and leave the store, then return to make another purchase
- Make large purchases just after opening or as the store is closing
- Refuse free delivery for large items

Card-Present Best Practices (Chip Cards)

Chip cards are extraordinarily difficult to duplicate. The use of stronger authentication methods and unique transaction elements make chip card data less attractive to steal, and render it nearly impossible to commit counterfeit fraud.

In most POS situations, the cardholder, not the business owner, inserts the card into the terminal. Use the following best practices when accepting a chip card.

1. Ask your customer to insert their card into a chip ready device and leave it in the device during the entire transaction.
2. The chip card and terminal will determine if a PIN or signature is required for verification.

3. If a PIN is required, the device prompts the customer to enter it. (When a PIN-based transaction is approved, the customer retrieves the chip card from the terminal. There is no opportunity for the business owner to examine the card.)
4. If the transaction is PIN-verified, there is no need for a signature.
5. If the customer does not know their PIN, ask for another form of payment.
6. Print a copy of the transaction receipt for the customer.
7. If the transaction is not PIN-based, the receipt will have a signature line for the customer to sign.
8. Ask the customer for their card to compare signatures from the receipt and the back of the chip card. Do not accept an unsigned card.

If the POS terminal cannot read the chip on the card, follow "fallback" acceptance procedures and swipe the card's magnetic stripe or key enter the data. Warning: swiping or key-entering a transaction increases the risk of accepting a counterfeit card because the chip information is not available. And, with the October 1, 2015 liability shift, liability for chip card-present fraud shifts to whoever is not using chip technology.

Card-Present Best Practices (Magnetic Stripe Cards)

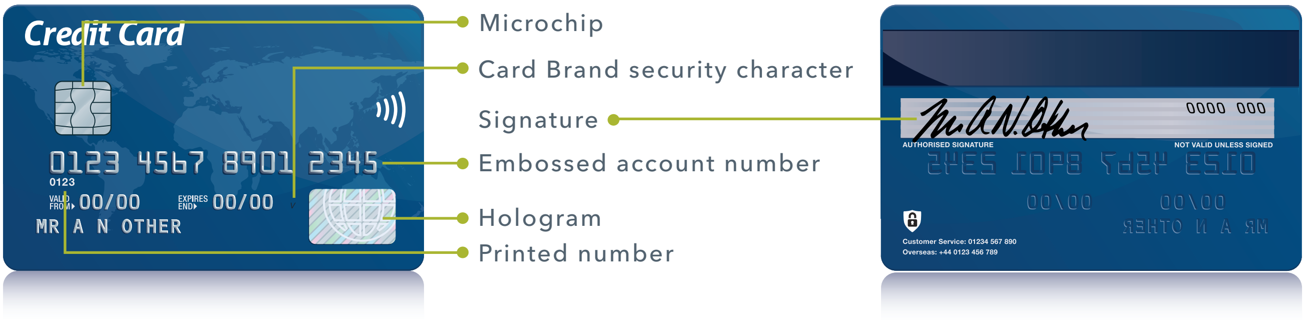
Use the following best practices when accepting magnetic stripe card-present purchases.

1. Check the card security features to make sure that the card has not been altered.
2. Swipe the stripe through the terminal in one direction only.
3. Check the authorization response and take appropriate action

Authorization Response	Appropriate Action
Approved	Ask the customer to sign the sales receipt.
Declined	Return the card and ask for another method of payment.
Call or Call Center	Call your voice authorization center and follow the prompts.
Pick Up	Keep the card if it can be done peacefully.
No Match	Swipe the card and re-key the last four didgits. If "no match" appears again, keep the card if it can be done peacefully. Request a Code 10 authorization.

4. Get the cardholder's signature on the transaction receipt.
5. Compare the name, account number, and signature on the card to those on the transaction receipt. They should match.

If a card cannot be swiped, card account data must be entered into a POS terminal. A word of warning: key-entering a transaction increases the risk of accepting a counterfeit card because the magnetic stripe information is not available.



Use the following steps when key-entering a transaction:

1. **Check the POS terminal to ensure it is operating properly.** If the terminal is OK and the problem appears to be with the card's magnetic stripe, continue to step 2.
2. **Match the account number.** Verify the embossed account number on the front of the cards matches the number indent-printed on the back.
3. **Check the expiration date**. Look at the "good thru" or "valid thru" date to be sure the card hasn't expired. If the card has a "valid from" date, be sure the card isn't being used before it is valid.
4. **Follow any prompts, including requests for entering the CVV.** If the card does not have a legible CVV, consider asking for another method of payment.
5. **Check the signature on the card to ensure it matches the signature on the sales draft.** Do not accept an unsigned card.

If you suspect fraud, immediately make a Code 10 call to your voice authorization center.

Card-Not-Present Transactions

Businesses accepting card-not-present purchases must take extra precautions to limit exposure to fraud, including investment in additional technology and establishment of individual risk and fraud parameters.

Card-Not-Present Warning Signs

When more than one of the following occurs during a card-not-present transaction, fraud might be involved. Follow up, just in case.

- **First-time shopper**. Criminals are always looking for new victims.
- **Larger-than-normal orders.** Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchases.
- **Orders that include several of the same item**. Receiving multiples of the same item increases a criminal's profits.
- **Orders made up of big-ticket items.** These items have maximum resale value and maximum profit potential.
- **"Rush" or "overnight" shipping**. Crooks want their fraudulently obtained items as soon as possible, and since they aren't paying, they aren't concerned about extra delivery charges.
- **Shipping to an international address.** A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the U.S.
- **Transactions with similar account numbers.** This is often a signal the account numbers have been generated using software available on the Internet.
- **Shipping to a single address, but transactions placed on multiple cards.** This could indicate an account number generated by special software, or a batch of stolen cards.
- **Multiple transactions on one card over a very short period of time.** Often this is an attempt to "run a card" until an account is closed.
- **Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses**. A signal of organized activity rather than a single fraudster at work.
- **In online transactions, multiple cards used from a single IP (Internet Protocol) address.** The use of more than one or two cards could indicate a fraud scheme.
- **Orders from Internet addresses that offer free email services**. These email services involve no billing relationships, and often offer neither an audit trail nor verification that a legitimate cardholder has opened the account.

Card-Not-Present Best Practices

Take the following steps to stay ahead of crooks and reduce your fraud exposure when accepting card-not-present transactions.

1. Get an authorization.
2. Ask for the card expiration date and include it in your authorization request. An invalid or missing expiration date can indicate the person on the other end does not have the actual card in hand.
3. Use fraud detection tools like Address Verification Service (AVS) and Card Verification Value (CVV) as part of your authorization process.
4. Be on the lookout for questionable transaction data or other signs indicating an "out of pattern" order.
5. If you receive an authorization but still suspect fraud:
   a. Ask for additional information (e.g., request the financial institution name on the card).
   b. Contact the cardholder with any questions.
   c. Confirm the order separately by sending a note via the customer's billing address rather than the ship-to address.

Remember, an authorization is not a guarantee of payment. An authorization means funds are available and the card has not yet been reported as lost or stolen.

In all cases, if you suspect fraud, immediately make a Code 10 call to your voice authorization center.

Code 10

If you suspect fraud at any time during the transaction process, you can make a Code 10 authorization request. This alerts the card issuer to the suspicious activity, without alerting the customer.

Code 10 steps:

- Keep the card in hand to quickly respond to questions.
- Call your voice authorization center and follow the prompts for a Code 10 authorization
  - o If you care transferred to the card issuer, you may be asked a series of yes/no questions.

You're Not Alone

Business owners using TSYS Merchant Solutions for their processing are not fighting fraud alone. TSYS Merchant Solutions takes fraud very seriously, and has numerous safeguards in place to reduce risk.

- TSYS Merchant Solutions' state-of-the-art processing platform includes fraud-detecting technology that monitors transactions for suspicious activity. If a questionable transaction is uncovered, a customer service representative will call the affected business owner to verify information.
- TSYS Merchant Solutions screens business owners' accounts and infrastructure to ensure technology is set up correctly.
- TSYS Merchant Solutions has representatives who sit on industry and card brand committees focused on reducing fraud.
- TSYS Merchant Solutions maintains close associations with government agencies and fraud-fighting groups to stay abreast of fraudulent activity and the latest crime fighting efforts.

Adding layers of security not only protect your customers' data, they safeguard your reputation and business. TSYS Merchant Solutions has a portfolio of security solutions available to help safeguard your business.

- **Next-Generation Credit Card Machines**
  A complete line of credit card terminals that make accepting cards and other payments a seamless part of your business. Terminals are EMV® and NFC enabled to accept today's payment types such as Apple Pay™ and Samsung Pay™, and are easily updated to accept future payment options.

- **TSYS Merchant Solutions Guardian℠**
  Security solutions to help protect your business from cyber criminals and the overwhelming cost of a data breach. TSYS Guardian Security Suite includes:

  o **Encryption/Tokenization**
  Industry-leading protection for credit card data that converts account information into random, unreadable formats during the transaction process.

  o **Card-Compromise Assistance Plan (C-CAP)**
  A unique assistance plan that provides up to $100,000 per merchant identification number to pay expenses associated with a real or suspected data breach.

  o **PCI Validation**
  Assistance with meeting mandatory data security requirements to protect cardholder account information.

Look for more fraud prevention, security and reference guides at www.usa.visa.com, www.mastercard.com, www.americanexpress.com and www.discovernetwork.com.

WHO WE ARE

TSYS Merchant Solutions is a leading payment processor with more than 30 years of experience providing first-rate service and comprehensive end-to-end payment solutions to businesses accepting payments across North America. Our dedicated, experienced team of industry professionals provides innovative card-acceptance solutions and unparalleled customer service every day to meet the long-term needs of our customers.

TSYS Merchant Solutions is a wholly owned subsidiary of TSYS® (NYSE: TSS). TSYS delivers advanced technology and enhanced value to many of the world's leading companies, making it possible for hundreds of millions of consumers to use their credit, debit, commercial, private-label, prepaid and chip cards safely and securely.

TO LEARN MORE

contact 800.354.3988
or email merchantsales@tsys.com

f www.facebook.com/tsysmerchant

www.twitter.com/tsysmerchant

You Tube www.youtube.com/tsysmerchant

g+ www.plusgoogle.com/+tsysmerchantsolutions

in www.linkedin.com/company/tsysmerchantsolutions

GET TO KNOW TSYS

AFRICA	ASIA-PACIFIC	COMMONWEALTH OF INDEPENDENT STATES	EUROPE	INDIA & SOUTHEAST ASIA	MIDDLE EAST	NORTH & CENTRAL AMERICA, MEXICO & THE CARIBBEAN	SOUTH AMERICA
+27 21 5566392	+603 2173 6800	+7 495 287 3800	+44 (0) 1904 562000	+911204191000	+971 (4) 391 2823	+1.706.644.3819	+1.706.644.3819