



**Reminder:
Don't Store Magnetic-Stripe Data**

The rising incidence of identity theft is a concern to everyone. Please remember that *Visa U.S.A. Inc. Operating Regulations* prohibit the storage of magnetic-stripe data after obtaining an authorization.

Visa Resources

To help educate your sales and customer service associates and bring them up to speed on all the latest procedures, see the following publications:

- ✓ *Visa Rules for Merchants: Card Acceptance and Chargeback Management Guide*
- ✓ *Visa USA Merchant Catalog*
- ✓ *Visa E-Commerce Merchants' Guide to Risk Management*

Visit our web site at:
www.visa.com/merchants
or call Visa Fulfillment at 1-800-847-2311.

**It Pays to Swipe
the Stripe**



It Pays to Swipe the Stripe

Built-In Fraud Protection on Visa Cards

On the back of every Visa® card, you'll find a magnetic stripe. It contains the cardholder name, card account number and expiration date, as well as special security information designed to help detect counterfeit cards. When the stripe is swiped through the terminal and electronically read, this information is relayed to the Issuer and used as crucial input to the authorization decision.

What Happens with Key-Entered Transactions?

Sometimes when you swipe the card, the terminal is not able to read the magnetic stripe and perform an electronic authorization. In this situation, you may need to key-enter the transaction data. When transactions are key-entered, special security information benefits are not available.

Examples of legitimate reasons for key-entry:

- The card is not present (mail, telephone, and Internet transactions)
- A terminal is not available (home delivery)
- The card's magnetic stripe cannot be read (the stripe has been damaged)

Examples of situations causing unnecessary key-entry:

- The terminal's magnetic-stripe reader is not working properly
- The card is not being swiped properly through the terminal

Disadvantages of a Key-Entered Transaction

✓ Increased risk of fraud and counterfeit

The magnetic stripe's special security features that work with your terminal and the authorization system are ineffective.

✓ Increased Cost

Key-entered transactions cost more to process, and are declined more often.

✓ Less Efficient

Key-entered transactions are more time-consuming and allow more potential for error.

✓ Lost Sales

Key-entered transactions are declined more often—making the potential for lost sales higher.

Best Practices to Minimize Key-Entered Transactions

To minimize unnecessary key-entry and improve your business profitability, you are encouraged to incorporate the following best practices into your operations and conduct regular training and review sessions with sales associates.

CALCULATION To obtain the percentage of key-entered transactions occurring at a particular terminal, divide the total number of key-entered transactions for the terminal by the total number of sales for the terminal. Exclude from both totals any mail/telephone orders that may have been made at the terminal.

Investigate High Key-Entry Rates

Perform the calculation for each terminal for each sales shift to determine the "key-entry rate per sales associate." Repeat the process for each store. If this percentage is greater than one percent per terminal or sales associate, try to find out why.

If a card won't read when swiped...

1. Take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way.
2. Follow store procedures, which may require you to use the terminal's manual override feature to key-enter the transaction data for authorization.
3. Make sure to imprint the card on the transaction receipt. The imprint will prove the card is present in the event of a dispute, and minimize potential for financial liability.
4. Suggest to your customer that he/she note whether the stripe is working the next time the card is used. If transactions are being key-entered at other merchant locations, the customer may want to contact the card-issuer for a replacement.

Find Causes and Look for Solutions

Use the chart below to assess high key-entry problems and determine possible solutions.

UNNECESSARY KEY-ENTRY CAUSE:	SOLUTION
Damaged Magnetic-Stripe Readers	Check magnetic-stripe readers regularly to make sure they are working.
Dirty Magnetic-Stripe Readers	Clean the magnetic-stripe reader head several times a year to ensure continued good use. Many cleaning products are available for this purpose. If you don't have a supply of cleaners, contact your merchant bank or Visa Fulfillment* to order Visa ReaderCleaner cards (Item #MIM 01.04.03).
Magnetic-Stripe Reader Obstructions	Remove obstructions near the magnetic-stripe reader. Electric cords or other equipment could prevent a card from being swiped straight through the reader in one easy movement.
Spilled Food or Drink	Remove anything (e.g., food or beverages) near magnetic-stripe readers that could soil or damage the machines.
Anti-Theft Devices that Damage Magnetic Stripes	Keep magnetic anti-theft tag deactivation devices away from any counter where a customer might place his or her card. These devices can erase a card's magnetic stripe.
Improper Card Swiping	<ul style="list-style-type: none"> • Swipe the card once in one direction, using a quick, smooth motion. • Never swipe a card back and forth. • Never swipe a card at an angle as this may cause a faulty reading.

* Visa Fulfillment at 1-800-847-2311 or www.visa.com/merchant