



## Card Present Safeguards

- 1. Swipe the card through the point of sale system/Insert the card into a chip-reading device.**
  - A card that has been “swiped” generally has lower interchange fees than those that are manually keyed. In addition, the customer’s information is automatically captured with that transaction.
  - Avoid key entry whenever possible. If you must enter numbers manually, be sure to get an imprint of the card.
- 2. Authorize the transaction.**
  - Review the authorization response and take the appropriate action:
  - Approved – Ask the customer to sign the sales receipt.
  - Declined – Return the card to customer and ask for another form of payment.
  - Call or Call Center – Call us at **800-228-1122** for a voice authorization.
  - Pick Up – Keep the card if you can do so peacefully.
- 3. Validate the physical card. Ensure the card has not been altered.**
  - Request a signature and be sure that the signature on the transaction receipt matches the signature on the card.
  - A signature is not always required on certain small ticket transactions. Check with Hancock Whitney Merchant Services Customer Support Team at [MerchantServices-Support@hancockwhitney.com](mailto:MerchantServices-Support@hancockwhitney.com) or 866-597-5721 for more details.
- 4. Settle the transactions daily.**
  - Authorizations that are not settled within a day will receive a higher interchange rate.

## Additional Guidance by Card Brand

For **Visa**, you can find further guidance on how to handle suspicious transactions and best practices related to chargeback management:

[Card Acceptance Guidelines](#)

[Chargeback Management Guidelines:](#)

[Fraud Prevention Guidelines](#)

**MasterCard** has published [Guidelines](#) on what to do if you suspect fraud

**American Express** has also published best practices around deterring fraud: [Fraud Prevention from American Express®](#)

**Discover** has outlined [Best Practices](#) for preventing fraud.



## Card-Not-Present Safeguards

(Phone order, e-commerce, etc.)

- 1. Authorize the transaction. Do not complete a transaction if the authorization request was declined.**
  - All transactions must be authorized.
  - Avoid key entry whenever possible. If you must enter numbers manually, be sure to get an imprint of the card.
- 2. Utilize fraud prevention tools such as:**
  - **Address Verification Service (AVS)** to check the cardholder's address given at the time of the sale against the address on file with the cardholder's bank.
  - **Card Verification Value (CVV2/CVC2)** to verify the security code located on the signature panel of the card. (On American Express cards the number is printed on the front of the card.)
- 3. If you receive an authorization but are suspicious of fraud, ask more questions.**
- 4. Ensure timely processing between the time the order is placed and the time you deliver the goods.**
- 5. Your transaction date should be the same as your shipment date and not be greater than 7 days from the authorization date.**
- 6. Do not charge your customer before you have shipped your goods. Obtain a cardholder's signature upon delivery of the shipped goods.**
- 7. Settle all transactions daily.**

## Additional Guidance by Card Brand

For **Visa**, you can find further guidance on how to handle suspicious transactions and safeguards related to chargeback management:

[Card Acceptance Guidelines](#)

[Chargeback Management Guidelines](#)

[Fraud Prevention Guidelines](#)

**MasterCard** has published [Guidelines](#) on what to do if you suspect fraud

**American Express** has also published safeguards around deterring fraud: [Fraud Prevention from American Express®](#)

**Discover** has outlined [Helpful Tips](#) for preventing fraud.