PCI-DSS: Payment Card Industry Training

Objectives
Completing the reading in this section will enable you to:

- **Practice the process of safe and effective Card-Present processing.**
- **Identify the key security features on credit cards.**
- **Locate additional security verification information.**

Credit card features and security elements

Each brand of credit card uses a set of unique design features and security elements to help merchants verify a card's legitimacy. By knowing what to look for on a card, you can avoid inadvertently accepting a counterfeit card or processing a fraudulent transaction.

After you have swiped the card, while waiting for authorization, take a few seconds to look at the card's basic features and security elements. Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way.

Note: Check the first digit in the account number. The first digit should always match the designated first digit for the card brand:

American Express – 3

Visa – 4

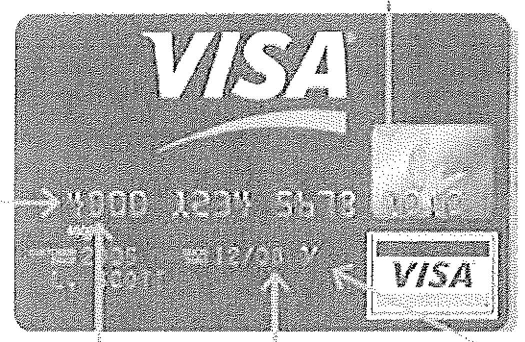
MasterCard – 5

Discover – 6

Hold onto the card

Note: Always keep payment cards in your possession during transaction processing. Holding onto the card gives you time to check card features and security elements and to compare the cardholder signature on the card with the signature on the transaction receipt.
What to look for on all cards (using Visa as an example)

On the Front of the Card



Look at the dove design hologram.

Compare the printed and embossed numbers.

Check the embossed account number for evenness and clarity.

Check the "Good Thru" or "Valid thru" date.

Look at the "flying V."

Compare the printed and embossed numbers.

A four-digit number is printed below the first four digits of the embossed account number on all valid Visa and MasterCards. These numbers should be identical. If the numbers are not identical or the *printed number* is missing, the card is not valid and should not be accepted.
Check the embossed account number for evenness and clarity

Look closely at the embossed account number for any signs that the card has been flattened and re-embossed. On valid cards, the numbers will be crisp and even; on altered cards, they may have fuzzy edges, or you may be able to see "ghost images" of the original numbers. The last grouping of numbers is embossed into the hologram. Pay special attention to that area, where ghost images are easiest to spot.
Check the "Good Thru" or "Valid Thru" date

Make sure the date of the transaction is no later than the date on the card. If the transaction date is after the "*Good Thru date*", the card has expired. In such instances, an authorization request can be called in to your authorization center, or you can ask the customer for a card that is currently valid.

Note:

- Always request an authorization on an expired card.
- If the Issuer approves the transaction, proceed with the sale.
- Never accept a transaction that has been declined.

Look for the embossed character

Each credit card company has their own unique character embossed on the front of their cards. Visa cards display a stylized embossed "V" located to the right of the "Good Thru" date on all valid Visa cards. If this character is missing or is not a "flying V", the card should not be accepted. Master Cards issued before June 1, 2006 have a scripted "MC" in this area, and

Discover Cards have a stylized "D" in between the "Member Since" and "Valid Thru" dates.

Note: MasterCards issued after June 1, 2006 will not have the "MC" Security Character. Cards issued before June 1, 2006 will continue to be valid until their expiration date or June 2010, which ever comes first.

Look at the design hologram

Visa, MasterCard, and Discover all employ a holographic security design on their cards. The key for all holograms is that they should reflect light, appear three-dimensional, and the image in the hologram should appear to move or shift when the card is tilted back and forth. If the image looks flat or doesn't move, the card may be counterfeit.

On Visa cards, a dove should appear in the hologram and it should seem to "fly" when the card is tilted back and forth. MasterCards have interlocking globes showing the continents with the word "MasterCard" in the background. The Discover card hologram shows a celestial sphere made of interlocking rings and an arrow pointer. The word "DISCOVER" appears in very small letters on the shaft of this arrow. The background of the image consists of a repetitive wave pattern with stars scattered throughout.

Note: On MasterCards, the hologram may appear on the back of the card.
Look at the signature panel

The signature panel is similar for all card types. It should be white with the brand name of the card written repeatedly at an angle across the length of the panel. For example, Visa card signature panels display the word "VISA" reprinted in a diagonal pattern in blue, or blue and gold. On MasterCards, the word "MasterCard" is repeated at an angle in red, yellow, and blue, while "Discover Network" appears diagonally on the signature panel of Discover Cards.

In addition, the words "Authorized Signature" and "Not Valid Unless Signed" appears either above, below, or beside the signature panel of most credit cards.
Check for any signs of tampering

If someone has tried to erase the signature panel, you may see the word "VOID" where the brand name should be displayed. Other signs of tampering include white tape or correction fluid, or "ghost images," indicating that a criminal has written over or altered the original signature. An altered signature panel means the card is invalid.
Check the account number and security code

On the back of the card, the account number, followed by a three- or four-digit code, may be printed on the signature panel in inverse italics (leaning left). The 3- or 4-digit code is a security and validation code, also referred to as the *Card Verification Value2* (CVV2). The CVV2 is used primarily in *Card-Not-Present* transactions to verify that the customer is in possession of a valid credit or debit card at the time of the sale.
When something doesn't look right

If any card security features are missing or look altered, notify your supervisor.
Overview

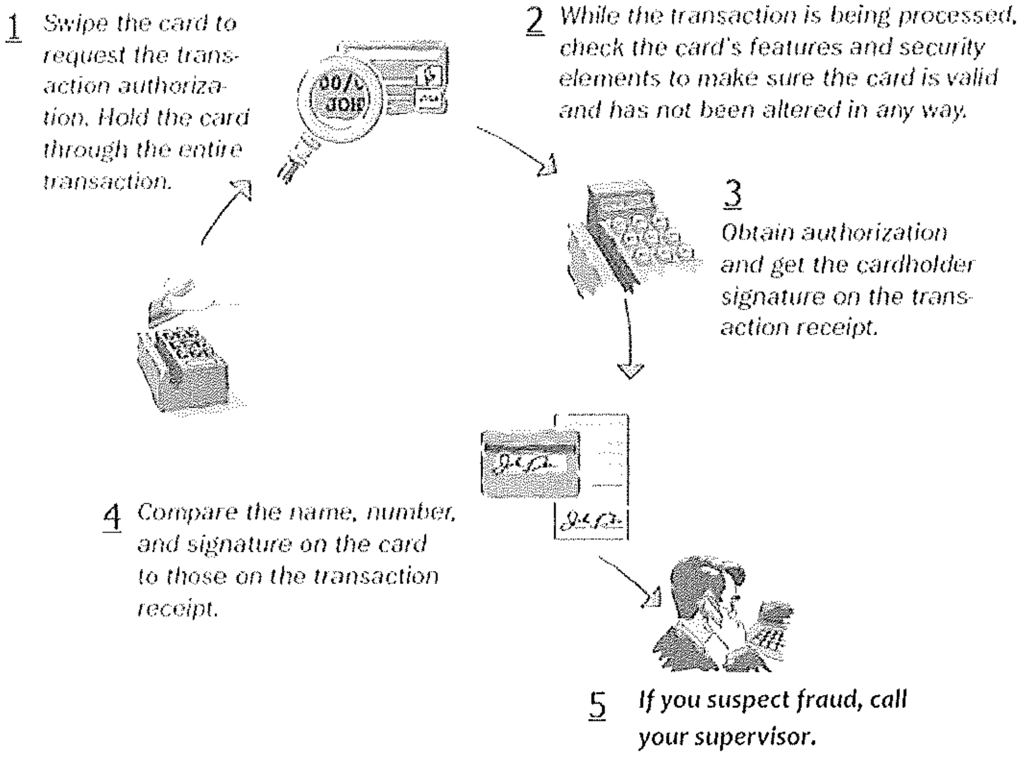
Card Present transactions are those in which both the card and cardholder are present at the point of sale.

UHFS Merchants are required to take all reasonable steps to assure that the card, cardholder, and transaction are legitimate. Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability.

Doing it right at the point of sale

Whether you are experienced or new to the job, following these few basic card acceptance procedures will help you to do it right, the first time and every time. The illustration below provides an overview of the card acceptance steps that are to be followed at the point of sale. Each step is explained in greater detail in this section.

Illustration of Card Acceptance



1 *Swipe the card to request the transaction authorization. Hold the card through the entire transaction.*

2 *While the transaction is being processed, check the card's features and security elements to make sure the card is valid and has not been altered in any way.*

3 *Obtain authorization and get the cardholder signature on the transaction receipt.*

4 *Compare the name, number, and signature on the card to those on the transaction receipt.*

5 ***If you suspect fraud, call your supervisor.***

It pays to swipe the stripe

On the back of every credit and debit card, is a magnetic stripe. The stripe 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, this information is electronically read and relayed to the card issuer, who then uses it as crucial input for the authorization decision.

Note:

- Swipe the card to request transaction authorization.
- Hold the card throughout the entire transaction.

Verifying the account number

Most *Point of Sale terminals (POS)* also allow merchants to verify that the account number embossed on the front of the card is the same as the account number encoded on the card's magnetic stripe. How you check the numbers depends on your POS terminal. In some cases, the magnetic stripe number is displayed on the terminal or printed on the sales receipt. In others, the terminal may be programmed to check the numbers electronically. In such instances, you may be prompted to enter the last four digits of the embossed account number, which will then be matched against the last four digits of the account number on the magnetic stripe.

Only the last four digits of the account or credit card number should be printed on a transaction receipt. If the numbers don't match, you will receive a "No Match" message. In such instances, discreetly notify your supervisor.

If a card doesn't read when swiped

In some instances, when a card is swiped, the terminal will not be able to read the magnetic stripe or perform an authorization. When this occurs, it usually results from one of three causes:

- The terminal's magnetic-stripe reader is dirty or out-of-order.
- The card is not being swiped through the reader correctly.
- The magnetic stripe on the card has been damaged or demagnetized.

Note: Damage to the card may happen accidentally, but it may also be a sign that the card is counterfeit or has been altered.

What to do

- Check the terminal to make sure that it is working properly and ensure that you are swiping the card correctly.
- If the terminal is okay, 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 (**See:** Card Features and Security Elements).
- If the problem appears to be with the magnetic stripe, contact manager or lead staff to manually enter card information.

Risks involved

Key-entered transactions are fully acceptable, but they are associated with higher fraud chargeback rates. In addition, when transactions are key-entered, the benefits associated with special security features—such as the expiration date and *Card Verification Value 2 (CVV2)*—are not available.

Overview

The authorization process allows the card issuer to approve or decline a transaction. In most cases, authorizations are processed electronically in a matter of moments. However, to protect against fraud, the card issuer may request additional information about the transaction. If done properly, authorizing a transaction is quick and easy, and protects merchants against fraud and *chargebacks*.

Authorization responses

Authorization should be seen as an indication that account funds are available and the card has not been reported as lost or stolen. It is not proof that the true cardholder or a valid credit card is involved in a transaction.

During the authorization process, you should receive one of the responses listed in the following table, or one that is similarly worded.

Response	**Meaning**
Approved	Card issuer approves the transaction. This is the most common response—about 95% of all authorization requests are approved.
Declined or Card Not Accepted	Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account.
Call, Call Center, or Referrals	Card issuer needs more information before approving the sale. Most of these transactions are approved, but you should call your authorization center and follow whatever instructions you are given. In most cases, an authorization agent will ask to speak directly with the cardholder or will instruct you to check the cardholder's identification. (**See:** Signature unsigned cards for acceptable forms of ID**).**
Pick-Up	This response indicates that the card issuer would like the card to be confiscated from the customer. However, UHFS Employees should not attempt to pick up credit cards, even when the card issuer requests this action, as this could potentially cause confrontation and safety issues.
No Match	The embossed account number on the front of the card does not match the account number encoded on the magnetic stripe. Swipe the card again and re-key the last four digits at the prompt. If a "No Match" response appears again, it means the card is counterfeit. Discreetly notify your supervisor.

Upon transaction approval

When a transaction is approved, the Point of Sale (POS) terminal automatically prints a sales receipt. When a negative or alert message is received, the response is displayed on the POS terminal, and no sales receipt is printed. Whatever the message, continue to treat the customer courteously so as not to arouse alarm or suspicion.

Signature and identification

The final step in the card acceptance process is to ensure that the customer signs the sales receipt and to compare that signature with the signature on the back of the card. When signing the receipt, the customer should be within your full view, and you should check the two signatures closely for any obvious inconsistencies in spelling or handwriting.

While checking the signature, you should also compare the name, account number, and signature on the card to those on the transaction receipt.

1. Match the name and last four digits of the account number on the card to those printed on the receipt.
2. Match the signature on the back of the card to the signature on the receipt. The first initial and spelling of the surname must match.

Note: The embossed name and receipt signature do not need to be the same.

Note: If the transaction is accepted with a non-matching signature and it turns out to be fraudulent, your business may be liable, even if all other procedures were followed.
Unsigned cards

While checking card security features, also make sure that the card is signed. An unsigned card is considered invalid and should not be accepted. If a customer gives you an unsigned card, the following steps must be taken:

1. Check the cardholder's ID. Ask the cardholder for some form of official government identification containing their photograph, such as a driver's license or passport. Social Security Cards are not acceptable forms of identification. The ID serial number and expiration date should be written on the sales receipt before you complete the transaction.
2. Ask the customer to sign the card. The card should be signed within your full view, and the signature checked against the customer's signature on the ID. A refusal to sign means the card is still invalid and cannot be accepted. Ask the customer for another signed credit card.
3. Compare the signature on the card to the signature on the ID. If the cardholder refuses to sign the card, and you accept it, you may end up with financial liability for the transaction should the cardholder later dispute the charge.

Note: The words "Not Valid Without Signature" appear above, below, or beside the signature panel on most credit cards.
"See ID" in lieu of signature

Some customers write "See ID" or "Ask for ID" in the signature panel, thinking that this is a deterrent against fraud or forgery; that is, if their signature is not on the card, a fraudster will not be able to forge it. In reality, criminals don't take the time to practice signatures: they use cards as quickly as possible after a theft and prior to the accounts being blocked. They are actually counting on you not to look at the back of the card and compare signatures—they may even have access to counterfeit identification with a signature in their own handwriting.

"See ID" or "Ask for ID" is not a valid substitute for a signature. The customer must sign the card in your presence, as stated above.

Note: A refusal to sign means the card is still invalid and cannot be accepted. Ask the customer for another signed credit card.
Suspicious behavior

In addition to following all standard card acceptance procedures, be on the lookout for any customer behavior that appears suspicious or out of the ordinary.

At the point of sale

- Purchasing large amounts of merchandise with seemingly no concern for size, style, color, or price
- Asking no questions or refusing free delivery on large items (for example, heavy appliances or televisions) or high-dollar purchases
- Trying to distract or rush sales associates during a transaction
- Making purchases, leaving the store, and then returning to make more purchases
- Making purchases either right after the store opens or just before it closes

Of course, peculiar behavior should not be taken as automatic proof of criminal activity. Use common sense and appropriate caution when evaluating any customer behavior or other irregular situation that may occur during a transaction. You know what kind of behavior is normal for your particular place of business.

If you feel really uncomfortable or suspicious about a cardholder or transaction, notify your supervisor.