Signature
Card Services

PROTECT YOUR BUSINESS FROM LOSSES

WHILE ACCEPTING CREDIT CARDS

TABLE OF CONTENTS

Fraud is on the rise in the United States. Data breaches are coming in tidal waves these days, and it is more important than ever for business owners to learn how to protect their businesses from credit card fraud and losses associated with chargebacks.

With migration to the chip-card standard, a more secure way to process credit cards, it is expected that fraud will be increasing dramatically in the card-present sector prior to the migration deadline of October 1, 2015 and shortly after, as the fraudsters are trying to take advantage of the closing window of opportunity. Fraud is expected to move to the card-absent sector after the country completes its migration to the chip-card standard.

Depending on the credit card acceptance method you are using, there are guidelines against fraud exposure and losses. Below are the most common loss prevention tips for card-present (retail, restaurant, mobile) and card-absent (internet, mail/telephone order) environments.

Fraudsters are getting more and more sophisticated with their schemes, but there is still a lot that you can do to minimize your exposure to fraud. We have created this guide to help you understand where the potential problems are coming from and how to defend your business and your clients. This guide is a comprehensive overview of the available tools that merchants can use to reduce their exposure.

This list, while unspecific to your business and not exhaustive, provides fraud-protection tools that can be used when accepting and processing credit cards.

2 Preventing Fraud in a Card-Present Environment

1 Check the card security features. Reference the "Card Features and Security Elements" guide on Page 9 to validate the card.

2 Match the name on the card with the name on the receipt. If the name doesn't match, ask for another form of payment. If the receipt doesn't show a name, ask for ID to match the name. Also, contact your processor to change the settings on your terminal to show cardholder's name for future transactions.

3 Get a signature. Make sure that the signature on the back of the card matches with the signature on the receipt. If the card is not signed, check any picture ID for signature match.

4 Embossed and unembossed cards. Most of the credit cards have embossed account number, cardholder name and expiration date on them. If you are presented with an unembossed card, swipe it through your POS terminal or system, and if the magnetic stripe can't be read, ask for another form of payment. Do NOT key-enter any transactions with unembossed cards. Ask for another method of payment.

5 Check the expiration date. Do not accept a card with an expired expiration date.

6 Match the numbers. Check the embossed number on the card against the four digits of the account number displayed on the terminal.

7 Issuing a refund. When you issue a return, please make sure that the card you are crediting funds to is the same card the original sale was processed on.

8 Saving receipts. We recommend that you save all sales receipts for at least a year.

9 Chip vs. magnetic stripe. If you are presented with a credit card containing a chip and you already have a chip-enabled terminal, then process the transaction as a chip-card transaction by inserting the card in the machine; don't swipe it. Chip cards are protected against counterfeit, but we suggest that you still follow the foregoing protocol when processing a chip card.

10 Unable to read the card. In some instances, when you swipe a card, the terminal can't read the card. When this happens, usually it means one of the following:

- The terminal's card reader is not working.
- The card is not being swiped correctly.
- The card is altered or counterfeited.
- The card's magnetic stripe is damaged or demagnetized.

If the card won't read, you should

- Make sure you are swiping the card correctly.
- Check the terminal to make sure it is working properly.
- Call your processing company and they will run a quick diagnosis of your reader.
- If the terminal is working properly, check the card for authenticity (see Page 9).

  If the terminal is not working and you are positive that the card is legitimate, key-enter the transaction and call for voice authorization. Make an imprint of the front of the card and write down the authorization number. You might need both in case of a dispute. If the card you couldn't swipe is not embossed, do not key enter it. Ask for another method of payment.

How to Reduce Chargebacks in a Card-Present Environment

Reduce Chargebacks (Card-Present)

Chargebacks can be significantly reduced with a few helpful tips. Take time and make an effort to educate yourself and your employees on how to process credit cards with loss-prevention mindfulness to minimize the avoidable chargebacks..

1 Obtain an authorization for the full amount of the sale. Declined transactions should not be split into smaller amounts.

2 If an authorization request was declined, do not complete the transaction and do not attempt another authorization on the same card. Ask your customer for another form of payment. Do NOT call the number on the card.

3 If you receive a "Call" message in response to an authorization request, call your authorization center. Be prepared to answer questions. The operator might want to speak to the cardholder. If the authorization is obtained, write down the authorization code on the sales receipt and process the sale as a key-entry. If declined, ask your customer for another form of payment.

4 Obtain the cardholder's signature; it is required for card-present transactions. Failure to obtain the cardholder's signature could result in a chargeback.

How to Reduce Chargebacks in a Card-Present Environment

5 Ensure that your return, refund and cancellation policies are clearly visible on the front side of the credit card receipt and on the invoice.

6 On cardholder statements, use a clear DBA (Doing Business As) name that customers will recognize. An unrecognized DBA name on billing statements is one of the most common causes of chargebacks. Contact your credit card processor to review and correct your descriptor (the name that appears on cardholder statements) if necessary.

7 Put your phone number on your customers' statements. If they do not recognize your descriptor, they can call you to find out who you are and why you charged them.

8 Always respond to a chargeback as quickly as possible. A limited amount of time (10 business days) is available to resolve a chargeback. If you miss the window of opportunity to respond, you forfeit your ability to fight the chargeback.

9 Some disputes are not the result of unauthorized credit card use. Rather, they start because the customer disputes the quality of the goods or services purchased. The best way to avoid this type of chargeback is to work closely with the customer to establish a mutually satisfactory solution.

6 Preventing Fraud in a Card-Absent Environment

Card-Absent Transactions

Card-absent merchants should establish policies and procedures specific to their business when processing credit cards. We are listing some of the main guidelines here, but you might want to consider adjusting them to reflect your business type and the specifics of your operations. Card-absent merchants must verify to the greatest extent possible the cardholder's identity and the validity of the transaction.

1. At a very minimum, collect the following:
   - The card account number
   - The name as it appears on the card
   - The card expiration date as it appears on the card
   - The billing address

2. Obtain a proof of delivery.

3. If you are taking an order over the phone,
   - Record the date & time of the conversation.
   - Make a note of any details of the conversation (if there is a transaction dispute, your notes can help).

4. If you are taking an order through mail or fax,
   - Obtain a signature on the order form.
   - Retain a copy of the signed order.

5. Use fraud prevention tools such as 3D Secure, AVS (Address Verification Service), and security code verification.

6. Perform internal screening or use third-party tools to handle questionable transactions.

How to Reduce Chargebacks in a Card-Absent Environment

1 Obtain authorizations for all card-absent transactions. Do not ship any goods or provide services prior to obtaining the authorization.

2 Obtain card expiration date. Never accept an expired credit card.

3 Communicate any changes to your original estimate in writing. Specify all updates and request a signature of confirmation for future reference.

4 Charge customers only after the goods have been shipped or the services have been provided. Ensuring the customer has received what they've paid for can decrease the likelihood of a chargeback. Send confirmation emails for online and telephone orders detailing goods/services purchased, itemized cost, terms of billing, returns, cancellations, etc.

5 Verify security code.

6 Conduct AVS.

7 Have a complete description of goods and services clearly displayed for customers to see. Describe the charge in full on the invoice. These details may help a customer remember the purchase.

8 Have your detailed and current contact information on all customer-facing material. On cardholder statements, use a clear DBA (Doing Business As) name that customers will recognize.

Reduce Chargebacks (Card-Absent)

8 How to Reduce Chargebacks in a Card-Absent Environment

An unrecognized DBA name on billing statements is one of the most common causes of chargebacks. Contact your credit card processor to review and correct your descriptor if necessary. Ensure your current "doing business as" name, contact number and web address appear on receipts, invoices, statement billing descriptors, etc.

9 Post your refund, return, and cancellation policy clearly.

10 Use various fraud-control tools to prevent fraudulent transactions.

11 Conduct additional scrutiny with suspicious transactions:

- Large or suspicious orders - Contact a cardholder to ensure the order is legitimate. If you are unable to reach the customer, you might have intentionally been given incorrect contact information - you should void this transaction.
- Rush orders or overnight shipping – Be wary of orders for which the customer is willing to pay more for faster delivery.
- Random orders (when a customer doesn't care about the specifics of the product)
- Suspicious shipping addresses:
  - PO Box or an office address is often associated with fraud.
  - Check the shipping address against a list of zip codes with high fraud rates.
  - Foreign orders - Also, be wary of orders with domestic billing addresses and foreign shipping addresses. They are usually fraudulent. As a general warning, be very cautious of any foreign orders. Generally, orders from Asia, the Middle East, and most parts of Africa are considered high-risk. Check with your processor for a list of countries you need to block.

CARD FEATURES AND SECURITY ELEMENTS

Every valid payment card features a number of security elements that are designed to enable merchants to verify the card's authenticity. Everyone who accepts card payments in the face-to-face environment should educate themselves on where these features are located and how they should look. They should develop procedures for card verification and implement them in every transaction. The process should only take a few seconds and could be done while you are waiting for an authorization response.

CARD TYPE	FRIST DIGIT OF ACCT #
AMEX	3
VISA	4
MasterCard	5
Discover	6

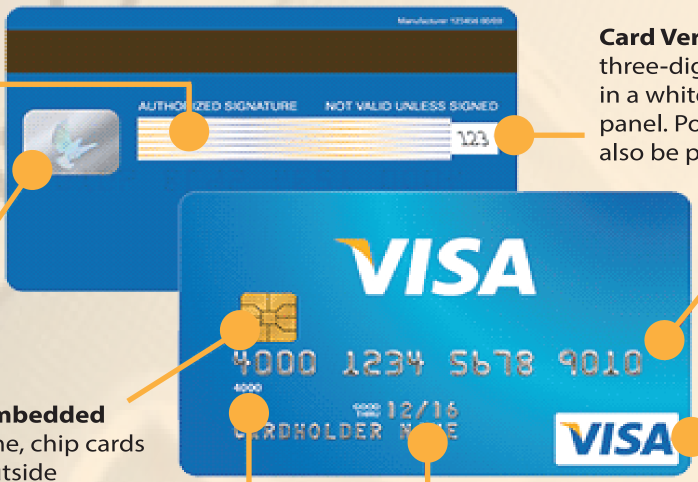
The account numbers of all Visa, MasterCard and Discover cards are comprised of 16 digits, and for American Express card, have 15 digits. All digits must appear even, straight, and the same size. The first digit of each card number identifies its type. Listed at left are the first digits that the major U.S. card brands use in their account numbers.

VISA Brand Card Features and Security Elements

The **Signature Panel** must appear on the back of the card. The words "Authorized Signature" and "Not Valid Unless Signed" must appear near the signature panel. If tampered with, the word "VOID" will be displayed.

The **Mini-Dove Design Hologram** may appear on the back on either side of the signature panel or on the front of the card above the Visa brand mark.

Visa chip cards are embedded with a chip. At this time, chip cards are primarily issued outside the U.S.



Card Verification Value 2 (CVV2) is a three-digit code that appears either on or in a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel.

Account Number on valid VISA cards begins with "4." All digits must be even, straight, and the same size.

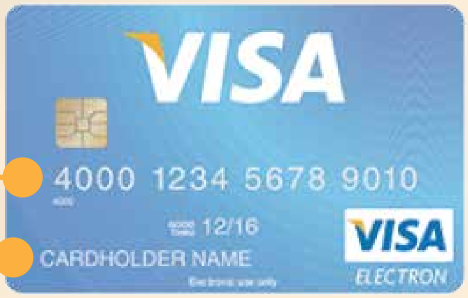
Visa Brand Mark must appear in blue and gold on a white background in either the bottom right, top left, or top right corner.

Expiration or "Good Thru" date should appear below the account number and must be current.

Four-Digit Bank Identification Number (BIN) must be printed directly below the account number and must match exactly with the first four digits of the account number.

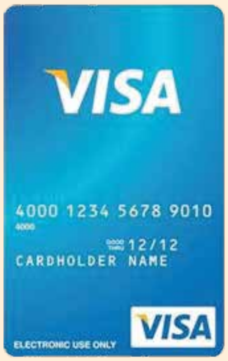
Unembossed 16-digit Account Number, Cardholder Name, and Expiration Date are laser-engraved, thermal or indent-printed securely on the front of the card.

Cardholder Name or a Generic Title may appear on an unembossed card.



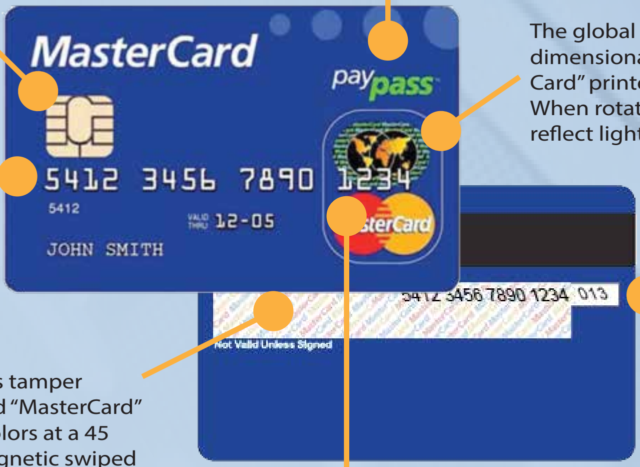
If the Dove Hologram is on the front of the card, the account number will be printed outside the hologram. The numbers may be smaller and placed closer together.

Alternate Card Front



Card design and VISA Brand Mark may be oriented horizontally.

MasterCard Brand Card Features and Security Elements



Paypass® contactless payment technology may be present on card. A signature is not required for PayPass® "tapped" transactions below a specified limit.

A chip may be present on the card. The cardholder may be prompted to enter in unique personal identification number or PIN when the card is inserted into a chip capable payment terminal.

The global hologram is three dimensional with a repeat "MasterCard" printed in the background. When rotated, the hologram will reflect light and appear to move.

The first 4 digits of the account number must match the 4 digit preprinted BIN. Remember, all MasterCard account numbers start with the number 5.

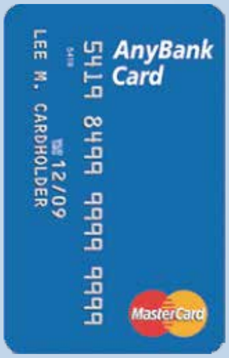
The 4 digits printed on the signature panel must match the last 4 digits of the account number, followed by the 3 digit indent printed CVC2 number.

The signature panel is tamper evident with the word "MasterCard" printed in multiple colors at a 45 degree angle. For magnetic swiped transactions, remember to compare the signature on the back of the card with the cardholder's signature on the receipt.

The last 4 digits of the account number must match the 4 digits that appear on the cardholder receipt.

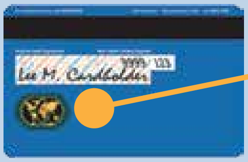
MasterCard allows its card-issuing banks some flexibility with the placement of the MasterCard hologram (on the cards' front or back), permit the use of holographic magnetic tape and supports vertical card designs. Below you will see how these features should appear.

Alternate Card Front

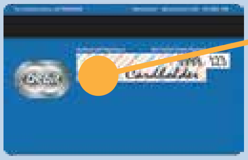


Card design and MasterCard Brand Mark may be oriented vertically.

Alternate Card Back

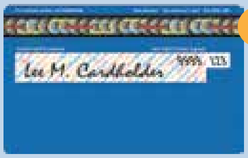


Global hologram on the back of a chip card design. The signature panel has been shortened to accomodate the chip.



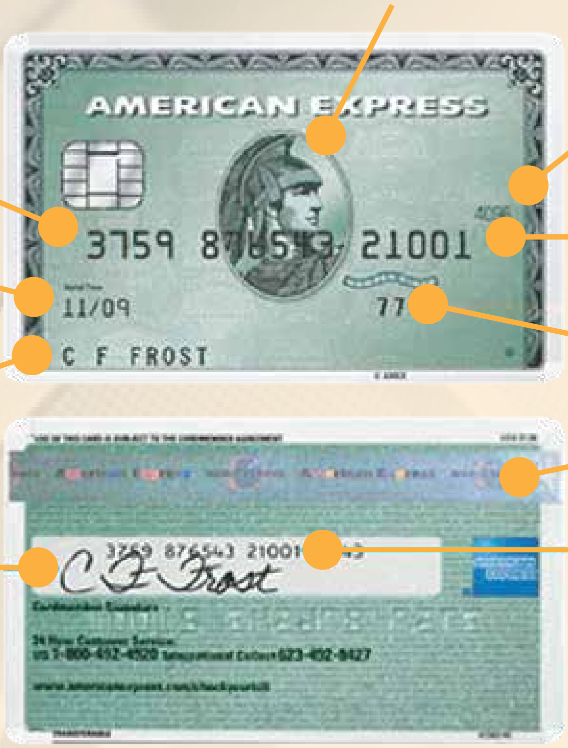
Debit hologram on the back of a magnetic stripe card design.

Note:
In some countries it is mandatory for Debit MasterCard cards to bear the Debit hologram.



Holographic magnetic tape may be used in lieu of the hologram or in conjunction with the hologram. A longer signature panel is used on traditional magnetic stripe cards.

AMEX Brand Card Features and Security Elements



All American Express account numbers are embossed and start with "37" or "34".

The expiry date is embossed and it shows the time period during which the card is valid.

Compare the name embossed on the card with the name on your customer's ID. Cards are not transferable.

Compare the signature with the one on the sales receipt. If the presented card is unsigned, request a photo ID with signature and request your customer sign the card and sales receipt while you hold the ID.

The clarity of the Centurion is similar to U.S. currency. The Centurian portrait is phosphorescent and the term "AMEX" is visible under UV light.

The 4-digit Card Identification Number (CID) is printed above the embossed account number on the right or left of the card and cannot be scratched off.

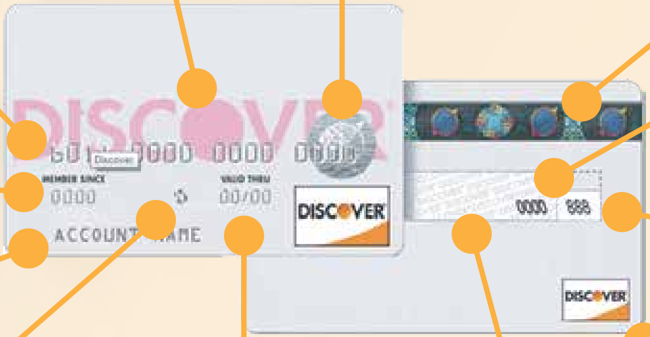
Account numbers are embossed (15 digits), with no alterations and spaced in 4, 6, and 5 digits.

The "member since" date is embossed – compare the age of your customer.

Some cards have a hologram of the American Express image embedded into the magnetic stripe.

The printed account number must match the embossed number on the front of the card.

Discover Brand Card Features and Security Elements



Account number. All Discover account numbers begin with "6" and are 16-digit long. Embossed numbers should be uniform in size and spacing, and extend into the hologram. Unembossed cards may display the account number and expiration date printed flat on the front.

Discover Network. The words "Discover" or "DISCOVER NETWORK" will appear under an ultraviolet light.

Hologram. Some Discover cards may display a hologram on the front of the card with a globe pierced by an arrow. However, if the back of the card displays a holographic magnetic stripe, there is no hologram on the front.

Magnetic stripe. Discover's magnetic stripe should look smooth, with no signs of tampering. Some Discover cards display a holographic magnetic stripe with blue circles.

Member since date. Located to the left of the expiration date, it indicates the month and year in which the account was open.

Cardholder name. In some cards, a "Business Name" may be embossed below the account name.

Last four digits. The last four digits of Discover's card number are also displayed within the signature panel, in reverse indent printing.

Card Identification Number (CID). The three-digit CID is printed in a separate box, immediately to the right of the signature panel on the back of the card.

Stylized "D". An embossed security character appears as a stylized "D". However, no such symbol is present on unembossed cards.

Expiration date. As with the other brands, the "Valid Thru" date, which indicates the last month in which the card is valid, is placed underneath the account number and to the right of the "Member Since" date.

The words "DISCOVER" or "DISCOVER NETWORK" appear repeatedly within the signature panel on the back of the card.

Discover brand mark. Discover's Network Acceptance Mark will appear on the front and / or back of the card.

800-631-3072
support@signaturecard.com
www.signaturecard.com

Signature
Card Services