

Agent Training Manual

SECTION 13:
RISK MANAGEMENT
GUIDELINES



UNDERSTANDING THE TRANSACTION PROCESS

Authorizations

The first step in the transaction process is obtaining an authorization for the credit card transaction. An authorization should be obtained by swiping the magnetic stripe of a credit card through the POS terminal for the lowest risk exposure and cost.

Mail order/telephone order and e-commerce merchants can obtain an authorization by manually keying the card number into the POS terminal, PC software or secure gateway/virtual terminal.

The terminal or software then communicates with the network system, which advances through the Visa ® and MasterCard ® Interchange system to the cardholder's bank for approval of the transaction.

Upon approval, an authorization number is issued and prints on the receipt. An authorization is not a guarantee of payment or an indication of the funds being transferred to your bank account.

Settlement

At the end of every day authorizations are processed, transactions must be batched or settled. This process can be achieved by pressing a button or sequence of buttons on the POS terminal or software. Once the settlement process has been initiated, the POS terminal or software will dial-out and settle all the authorizations and submit them to We for funding. Successful settlement of the terminal does not guarantee funding into a checking account in a specific time frame.

Note: Some terminals, software and secure gateways are configured to automatically settle or "batch" every 24 hours. Detailed instructions on the operation of the POS terminal or software can be found in the Quick Reference Guide included in the welcome package.

Funding

After we receive settled transactions they are sent through a computer system for analysis. If the transactions processed fall within the parameters indicated on the Merchant Agreement, an ACH (Automated Clearing House) file is generated and sent to our member bank for funding.

The funding of transactions is sent via ACH to the designated bank account of your choice. Typically, funding time from settlement to deposit into the merchant's bank account is between 48 to 72 hours. Higher risk merchants may be approved with delayed funding.

Note: Discover ®, American Express ®, Diners Club ® & JCB ® are entirely independent settlement banks. Deposits and month-end statements are received separately for the above card types.

Accepting Credit Cards for Payment

What Not To Do

In order to decrease the probability of charge-backs and promote cardholder security, best practices must be followed when processing credit card transactions. Merchants must comply with the following Visa ® & MasterCard regulations:

Do Not...

- require a minimum or maximum purchase amount for using a credit card.
- surcharge or penalize a customer for using a credit card.
- discriminate against any specific card brand.
- run a transaction to provide a cash advance to yourself or a cardholder. Cash advances are strictly prohibited and can result in account termination. Only approved financial institutions (banks) are permitted to process this type of transaction.
- use a credit card to secure a paper check.
- record a cardholder's personal information on a sales slip.
- process transactions for goods or services that were not indicated on the Merchant Agreement. (Example: an auto repair shop selling a used car is prohibited.)
- submit a declined or expired credit card for settlement.

When Not to Accept a Credit Card...

- The signatures on the back of the credit card do not match the signed sales draft. If unsure of the signature comparison, void the sale or call for a Code 10 voice authorization. If the back of a credit card is not signed, use a driver's license for signature comparison.
- The card appears to be tampered with.
- The sale amount was declined an authorization.
- The customer does not have the actual credit card present at the time of purchase.

Transaction Authorization

To begin the card acceptance process the customer's credit card must be authorized. For the best rate available and lowest risk, swipe the magnetic stripe through the POS (point-of-sale) terminal. The terminal will dial-out and communicate through the network to the cardholder's issuing bank for an approval or decline.

Typically, authorization time is less than a few seconds. More than 95% of all transactions are approved; however, in some circumstances the issuing bank may decline the transaction or request further action from the merchant.

Tips for Swiping the Card:

1. Hold the card firmly as you slide it through the magnetic reader.
2. Slide the card only once, unless directed otherwise.
3. If there is a card read error, press the clear button before sliding the card again.
4. If the magnetic reader becomes dirty, be sure to contact the Help Desk to request some cleaning cards.

5. If the card cannot be swiped, manually key the account number into the POS terminal or software. An imprint of the card must be obtained in compliance with Visa ® & MasterCard ® regulations pertaining to non-swiped retail transactions.

Response Codes

When submitting transactions for authorization, one of the following responses will appear in the LCD display:

- **Approved:** The cardholder's bank (issuer) has authorized the transaction. If a printer is attached or built into the POS terminal a receipt will print with an approval number. If a printer is not available, the approval number will appear in the LCD display and must be clearly written on an imprint slip.
- **Call Center:** The cardholder's bank (issuer) requests a voice authorization. Call the voice authorization number listed on the front of this Manual (also found on the sticker sent in the welcome package). The Voice Authorization Center will ask for additional information, and may issue an approval number or decline. If an authorization is approved by the Voice Authorization Center, run the transaction as a "Force" or "Off-Line" sale and imprint the credit card for chargeback protection. Note: A voice authorized transaction will not settle into your bank account unless forced or processed off-line. For more instructions on how to process this type of sale please reference the Quick Reference Guide or contact the 24-hour Help Desk.
- **Declined:** The cardholder's bank did not approve the transaction. Inform the customer that the credit card has been declined and ask for another form of payment.
- **Try Again LC:** Extremely infrequently a technical difficulty can occur when attempting to authorize or settle a transaction. The terminal will respond with a Try Again LC, which stands for Lost Connection. In the unlikely event of such a response, check the phone line connected to the terminal. Static on the line, call waiting, a shared fax trying to communicate or someone picking up the phone line in the middle of a transaction can all result in Try Again LC responses.

Confirming Account Numbers

After a transaction has been authorized, an approval number will display on the terminal screen and/or print on a sales slip. The account number printed on the receipt should be compared to the account number embossed on the credit card.

If the numbers match, the card is probably not counterfeit; if they do not match, call the Voice Authorization Center and request a "Code 10" verification or refuse the purchase.

Signed Sales Draft & Signature Verification

After the transaction has been authorized and a receipt is printed, the customer must sign the receipt. Obtaining the customer's signature is critical, because it is proof of his or her consent

to pay for the transaction. In the event of a dispute, the Risk Management will request copies of the signed sales draft.

If the POS terminal does not have a printer, adding one to your system is highly recommended.

Having a printer will assist your business with reporting, reconciliation, and customer disputes. A retail business that is unable to print receipts must take an imprint of each credit card and obtain the cardholder's signature on the imprinted sales draft. The signature on a sales draft or receipt must be compared to the back of the cardholder's credit card. If the cardholder has not signed the signature panel on the credit card, request to see his or her driver's license to validate his or her signature and identity.

Voice Authorizations / Code 10

If the POS terminal issues an authorization response of "Call Center" or you request "Code 10" verification, please complete the following steps:

1. Call the Voice Authorization phone number
2. Be prepared to provide the Merchant ID number, Bank ID number, cardholder's credit card number, expiration date and purchase amount.
3. If the transaction is authorized, record the approval code on the sales draft.
4. Complete the sales draft.
5. Imprint the customer's credit card on the sales draft.
6. The transaction must now be "Forced" or "Off-Line Processed". For detailed instructions on how to process this type of sale, please reference the Quick Reference Guide or contact the 24-hour Help Desk.

Manual Imprint

Every retail merchant should have a manual imprinter and plate. We provide imprinter plates to new merchant location. Visa ® & MasterCard ® regulations require merchants to obtain an imprint for all retail transactions that cannot be electronically authorized.

The imprint indicates that the cardholder was present at the time of the transaction. Imprints should be obtained in the following circumstances:

1. Imprint every sale or refund if the POS terminal does not have a printer.
2. The magnetic stripe is unreadable on your customer's credit card. Manually key the transaction and imprint the card.
3. The customer ordered the product over the phone and it is being delivered. Imprint the card at the time of delivery and obtain a signature.
4. The terminal issues a response for a voice authorization. Reference the above section on voice authorizations.
5. The cashier performs a Code 10 voice authorization.
6. Any time you feel that the likelihood of a customer disputing the transaction is high. An imprint will help the chargeback reversal process.

Manual / Key Entered Transactions

Merchants processing key-entered transactions are exposed to significantly higher amounts of charge-backs than transactions magnetically swiped at the point-of-sale. Merchants who process manually keyed transactions are categorized as one of the following:

- Mail Order (MO)
- Telephone Order (TO) (Collectively referred to as MO/TO)
- e-Commerce / Internet (INT)

Only merchants that specified on the Merchant Agreement and were subsequently approved for submitting MO/TO or e-commerce transactions for settlement will be permitted to do so.

Mail and Telephone Order Guidelines & Risk

We have detailed the best practice steps to processing a mail order/telephone order transaction below. Do not begin the process unless the product is available for shipment. It is against the Merchant Agreement to settle a credit card transaction before the product is stocked in inventory and ready to be delivered.

1. Always obtain the cardholder's name, billing address, billing zip code, account number, expiration date, and CVV2 Card Verification Value. The billing address, zip code and CVV2 number will be used during the authorization process.
2. Generate an invoice or sales draft with a description of the products or services being sold.
3. If possible, obtain a signature via fax on the invoice or sales draft.
4. Electronically authorize the transaction through the POS terminal or software.
5. The POS terminal or software will use the Address Verification System (AVS) protocol to ensure the billing address and zip code entered are accurate. If the address and zip code do not match, contact the customer immediately. If AVS does not match, a merchant may want to consider refunding or voiding out the transaction. To help avoid mistakes with AVS it is important to clarify with the customer the difference between his or her "Billing Address" and "Shipping Address". Successful verification of AVS information does not guarantee the transaction is not fraudulent.
6. Some POS terminals or software are equipped to process the Card Verification Value (CVV2). Obtaining and authorizing this number confirms that the credit card is present. It does not guarantee the transaction is not fraudulent, but provides another layer of defense.
7. Immediately after successfully authorizing payment from a customer, the product or the service must be delivered. Keep copies of the "proof-of-delivery" and shipment records with the authorization / sales draft receipts / invoice. Never charge a customer unless the product is in stock or the service to be performed can be promptly delivered.

E-Commerce Information, Guidelines & Risk

With the rapid growth of Internet shopping over the last few years, e-commerce has become a core part of our processing services. Offering products and services via the Internet presents unique opportunities for merchants to expand their businesses.

Visa ® & MasterCard ® regulations require all merchants approved for e-commerce processing to submit transactions via a secure online gateway.

Before a business can be approved to process e-commerce transactions, it must have a valid website with return and privacy policies posted. Should the products or services offered through an e-commerce merchant account change, we must be notified immediately.

A merchant that currently has a retail or MO/TO account with us, must submit an entirely separate application for e-commerce, if interested. We issue e-commerce merchants unique Merchant ID numbers upon underwriting approval, as does American Express and Discover.

The following e-commerce policies and procedures have been established to comply with Visa ®, MasterCard ® regulations:

1. E-commerce merchants must submit transactions for authorization & settlement through a secure online gateway.
2. Maintain a valid website with complete descriptions of the products and services sold.
3. The website must contain a return/refund and privacy policy.
4. The security protocols used to protect a customer's information like SSL, Thawte, Verisign must be disclosed.
5. Contact information for your business must be easily accessible to customers.
6. The shipping method, time frame, and delivery procedures must be clearly stated.
7. A transaction receipt via electronic mail must be provided to the customer and must include your business name, web address, contact information, and the terms & conditions of the sale.
8. AVS (the Address Verification System) must be used to validate the billing address of the cardholder.
9. Attempt the use of Card Verification Value (CVV2) to further validate the transaction.
10. After the payment has been accepted, the product must ship immediately. The customer can not be charged unless the product is in inventory and ready to ship.
11. Always keep the transaction receipt, shipping record (UPS, Airborne, FedEx or USPS) and proof of delivery on file. This information will need to be presented in the event of a chargeback.
12. It is highly advised to establish an internal fraud control system to review each order for validity. Any order that seems suspicious should be further investigated. Contact the cardholder for verification. Orders that failed AVS or CVV2 validation should be flagged for research. If an order is high risk or possibly fraudulent, void the transaction immediately. Shipping orders that do not pass the AVS or CVV2 system could result in charge-backs and loss of merchandise.
13. All e-commerce merchants should be extremely suspicious of international orders, especially in parts of Southeast Asia. Some geographic areas have a high frequency of fraud and black market stolen credit card information.

Debit & EBT Acceptance Procedures

The STAR Debit Network 2001 survey states that 75% of all credit card holders in the United States have an ATM or debit card, with more than 90% using them to make purchases at the point-of-sale.

The Nilson Report concludes that debit cards are becoming the most popular form of non-cash payments. The increasing popularity of this card base, makes it advantageous for any business to consider acceptance of ATM & debit cards.

Pin-Pads & Encryption

In order for a business to accept PIN-based debit card transactions, there must be a POS terminal with a printer and pin-pad. A pin-pad is an external device that plugs into a POS terminal or is built into the keypad of certain POS terminals. For a pin-pad to function correctly, it must be encrypted by We.

To verify that the proper encryption has been injected into a pin-pad or POS terminal, flip the unit upside-down and look for a sticker confirming the successful encryption.

Once a POS terminal and a properly encrypted pin-pad are installed, ATM & debit cards can be processed for payment.

PIN # Security

- Never ask your customer for their Personal Identification Number (PIN).
- Keep the pin-pad in close proximity to the register and allow the cardholder enough space to privately enter the PIN.
- The receipt for a PIN-based debit transaction must be printed from the POS terminal or a separate receipt printer. Imprint slips are not acceptable. The receipt must be maintained for record purposes for two years.
- PIN-based transactions do not require a signature from the cardholder.

Cash-Back & Surcharges

Merchants setup to process PIN-based ATM & debit transactions may offer a “cash-back” option to customers. In addition, customers may be charged a fee (similar to how an ATM operates) for enjoying the convenience of “cash-back”. The process works by running a normal debit/ATM transaction, entering the purchase amount and then the cash-back amount. The pin-pad will activate, displaying the total dollar amount and applicable surcharge amount. The customer accepts the transaction by entering the PIN number.

The POS terminal will then dial-out for authorization of the total transaction amount. Upon authorization the cash-back amount may be provided to the customer. The debit network will credit your checking account for the sale amount, cash-back amount, and any applicable surcharge in the normal deposit time. The surcharge amount you wish to charge customers must be programmed into the POS terminal.

Important! Cash-back is only permitted on PIN-based ATM and debit cards. Never run a cash-back or cash advance on a credit card, which would violate Visa ® & MasterCard ® regulations and can result in account termination.

Electronic Benefits Transfer (EBT) Information & Procedures

Electronic Benefits Transfer presents a unique payment option to merchants and customers. An EBT card is used by the federal and state governments to deliver food stamps and cash benefits to qualified EBT recipients.

An EBT card replaces paper food stamps, unemployment checks, cash benefits, and other government funded programs. It was mandated by the federal government that all states have an EBT program to replace the paper system by October of 2002. As a result, merchants in the retail, grocery and convenience store marketplace have a growing demand to accept EBT as a form of payment.

To participate in the Electronic Benefits Transfer program, merchants must obtain an FCS or FCN number from their state's agriculture department. Please contact our Technical Help Desk to have EBT added to your merchant account, if an FCS or FCN number has been issued.

There must be an encrypted pin-pad available to facilitate the process.

Refunds and Exchanges

Refunds or credit back to a customer's credit card can be processed for the return of products or services. It is imperative that a refund policy is clearly posted and accepted by the customer. It is strongly recommended that the terms-of-sale and refund policy is printed on the sales receipt. This can be programmed into the POS terminal.

No cash or check refunds are permitted on a credit card purchase. This presents the potential for charge-backs.

The following steps ensure the proper refund or exchange of a credit card purchase:

1. Ask the customer for the credit card used for the original purchase.
2. Compare the account number on the credit card to the sales receipt for confirmation. The account numbers must be the same.
3. If the cardholder does not have the original card present, manually key the refund. Do not refund another card, the same account number must be credited.
4. If a printer is used with the POS terminal, follow the procedures in the Quick Reference Guide for processing a refund.
5. If the POS terminal does not have a printer, the manual imprinter must be used. Record all information on the sales slip, indicating a refund. Imprint the card for your records.
6. If the customer is only returning a portion of the purchase, the entire amount must be refunded first. Then process the amount of the sale that remains as a new transaction.
7. If the sale was originally processed as a PIN-based ATM/debit transaction, there are two options: refund the same card or give cash. Note: ONLY PIN-based ATM/debit refunds are allowed to be issued in the form of cash instead of refunding the card.

Cardholder Privacy

Visa® and MasterCard® regulations prohibit merchants from recording personal information on the sales receipt/draft. This information in conjunction with the account numbers listed on the sales draft could be used to commit fraud.

Keep cardholder account and personal information separate and under tight security. Release of this information is only permitted to authorized law enforcement officials.

It is extremely critical that CVV2 Card Validation numbers are not written, recorded or stored electronically nor manually under any circumstances.

Honoring Cards & Display of Signage

Upon approval of the Merchant Agreement, the merchant agrees to honor both Visa® & MasterCard® without discrimination. Visa and MasterCard require your business to clearly display signage at the point of sale. Included in the welcome kit is a supply of counter and window decals.

Fraud Identification and Prevention

Prohibited Transactions

Certain types of transactions present a high degree of risk. As a result, Visa and MasterCard regulations and/or the Merchant Agreement prohibit your business from processing the following transactions:

- Attempting to process a sale on a previously charged back purchase.
- Processing transactions for the purpose of collecting debt, bounced checks, etc.
- Attempting to settle or force transactions that were declined.
- Attempting to reauthorize a declined transaction.
- Processing a transaction on an expired card.
- Attempting to split a transaction amount to avoid a decline.
- Processing a transaction for the purpose of a cash advance.
- Attempting to process a sale for a cancelled service or returned product.
- Processing sales with more than one payment processor or bank offering credit card services similar to We.
- Processing transactions for other businesses, merchants, or products/services not explicitly listed in the Merchant Agreement. Such practice is called factoring.
- Attempting to process a transaction more than once.
- Processing your own credit card for the purpose of funding your checking account.
- Refunding sales when the funds are not in your checking account to cover the debit.
- Processing any annual memberships or future delivery products without the written approval of We.

It is imperative to understand and educate your staff on prohibited transactions. Attempting to process any of the above transactions could result the suspension or termination of your merchant account.

Counterfeit Credit Cards / Security Features

Stolen and counterfeit cards are a major problem for merchants and issuing banks alike. Readily available technology makes it easy for counterfeiters to reproduce nearly perfect copies of legitimate credit cards.

All credit cards have the same basic security features with each brand containing some distinct qualities. Proper training of your staff on detection of counterfeit credit cards can reduce credit card fraud and loss of merchandise. Most card issuers will pay a small reward to the cashier who catches a stolen or counterfeit card.

The basic components of a credit card include the color, embossing, signature panel, CVV2 number, and hologram.

Color:

The color of the card should be even without any noticeable alterations.

Embossing:

Another criteria to exam is the account number embossing. All characters should be raised without any variation. It is common for a counterfeiter to iron down the account numbers and re-emboss with new information. In such cases, the small font 4 digit number printed directly on the credit card will not match the first 4 digits of the embossed number. All Visa cards will start with a 4, MasterCard cards with a 5, and Discover cards with a 6.

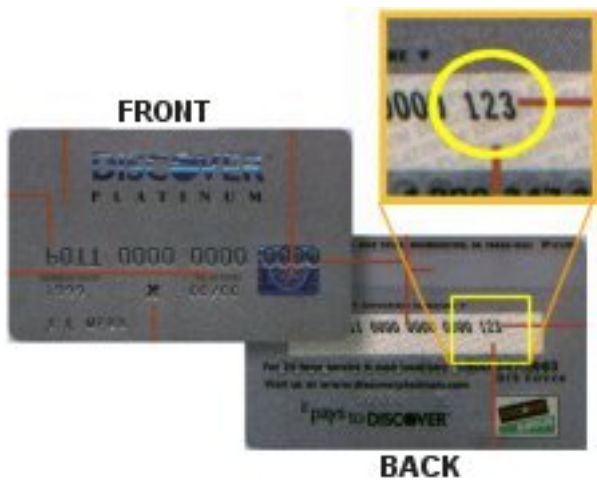
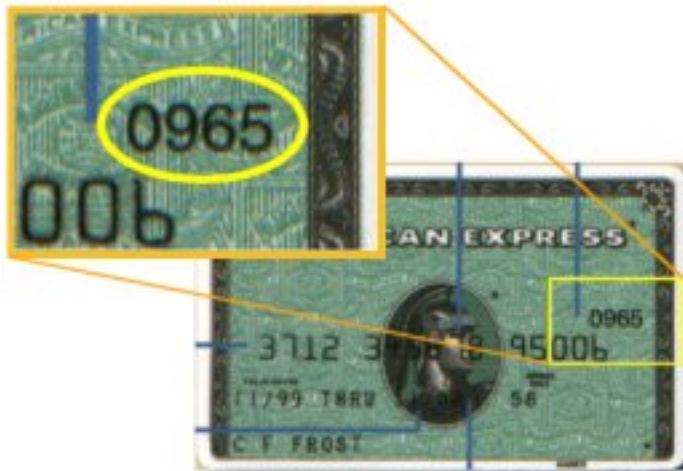
Signature Panel:

After examining the embossing and account numbers, check the signature panel on the back of the card. It should have the MasterCard or Visa logo background wash. The panel should contain the signature of the authorized cardholder. The Card Verification Value (CVV2) will be located on the signature panel.

Hologram:

The hologram is the last security feature and the hardest to alter or counterfeit. The hologram consists of a three dimensional foil image. The foil material can consists of a gold or silver color and presents an image as you reflect light off the card. The Visa hologram appears to be a dove flying. MasterCard's hologram consists of rings, globes and spheres, with the word "MasterCard" surrounded by two alternating colors.





Suspicious Shopping Patterns

Customers that are looking to commit credit card fraud or commit a crime will try to catch employees off guard. They will typically enter at a busy point or just before closing. The shopper may select lots of items for purchase without paying much attention to the price, size, or quantity. If one observes this type of shopping pattern, call immediately for a Code 10 authorization.

Fraudulent Returns

Merchants need to be especially aware of the transactions cashiers are running. It is very common for a cashier to issue refunds to his or her own credit or debit card. Fraudulent cashiers could steal substantial amounts of money without being caught, if not monitored carefully. We strongly suggests a password protecting the refund feature on the POS terminal; this will limit access to owners and management.

International Cards

International cards are often attributed to credit card fraud in the retail, MO/TO and e-commerce environments. Most retail merchants are not familiar with the design and security features in an international card. This confusion can lead to lost merchandise and charge-backs.

If suspicious of an international credit card transaction, call the Voice Authorization Center for a Code 10.

For MO/TO and e-commerce merchants, We caution against accepting international transactions. The likelihood of fraud increases dramatically with orders from outside the United States.

The geographic area of immediate concern is Southeast Asia and the Middle East. These locations have a pattern of credit card fraud and black market account.

UNDERSTANDING YOUR MERCHANT TERMINOLOGY

Address Verification Service (AVS):

The process of validating a cardholder's given address against the issuer's records to determine accuracy and deter fraud. This service is provided as part of a credit card authorization for mail order/telephone order transactions. A code is returned with the authorization result that indicates the level of accuracy of the address match and helps secure the most favorable interchange rates.

Adjustment:

An adjustment is initiated by EMG to correct a processing error. The error could be a duplication of a transaction or the result of a cardholder dispute. The acquirer debits or credits the merchant DDA account for the dollar amount of the adjustment.

Audio Response Unit (ARU):

This is an electronic authorization and capture product where the merchant uses a touch-tone telephone to process transactions.

Authorization:

The process of verifying the credit card has sufficient funds (credit) available to cover the amount of the transaction. An authorization is obtained for every sale. An approval response in the form of a code is sent to a merchant's POS equipment (usually a terminal) from a card-issuing financial institution that verifies availability of credit or funds in the cardholder account to make the purchase. Also see Point-of-Sale.

Authorization Response:

An issuing financial institution's electronic message reply to an authorization request, which may include:

Approval -- transaction was approved

Decline -- transaction was not approved

Call Center -- response pending more information; merchant must call the toll-free authorization phone number.

Authorization Code:

A code that a card-issuing bank returns in an electronic message to the merchant's POS equipment that indicates approval of the transaction. The code serves as proof of authorization.

Auto Close:

A terminal feature that allows an end-of-day batch closing to occur automatically at a specified time, without having to be initiated by the merchant.

Automated Clearing House (ACH) File:

A file with instructions for the exchange and settlement of electronic payments passed between financial institutions. It represents debits and credits to be deducted from or added to an account automatically as they occur.

Average Ticket (Average Sale):

The average dollar amount of a merchant's typical sale. The average ticket amount is calculated by dividing the total sales volume by the total number of sales for the specified time period.

Bankcard:

A credit card issued by a Visa- or MasterCard-sponsored financial institution. (American Express, Discover, Diners Club, JCB, etc., are issued directly from their respective operations, rather than through banks.)

Batch:

The accumulation of captured credit card transactions in the merchant's terminal or POS awaiting settlement.

Capture:

The submission of an electronic credit card transaction for financial settlement. Authorized credit card sales must be captured and settled in order for a merchant to receive funds for those sales. Also see Settlement.

Cardholder:

Any person who holds a payment card account (bankcard or otherwise); a person that uses a credit card to purchase goods and services.

Card-Issuing Bank:

An EFT Network Member-Bank that runs a credit card or debit card "purchasing service" for their account holders. An example is Citibank and the Citibank Visa Card that they issue.

Card Not Present:

A transaction where the card is not present at the time of the transaction (such as mail order or telephone order). Credit card data is manually entered into the terminal, as opposed to swiping a card's magnetic stripe through the terminal.

Chargeback:

A credit card transaction that is billed back to the merchant after the sale has been settled. Chargebacks are initiated by the card issuer on behalf of the cardholder. Typical cardholder disputes involve product delivery failure or product/service dissatisfaction. Cardholders are urged to try to obtain satisfaction from the merchant before disputing the bill with the credit card issuer.

Close Batch:

The process of sending the batch for settlement.

Code 10 Authorization:

If a merchant suspects a card is fraudulent at the time of the transaction, the merchant can call their voice authorization phone number and ask for a code 10. The voice operator will instruct the merchant how to proceed.

Commercial Cards/Corporate Cards:

Credit or charge cards issued to businesses to cover expenses such as travel and entertainment and procurement. Includes the multiple payment card brands of purchasing cards, business cards, corporate cards, and multi-utility fleet cards. Visa and Master Card now have special procedures for passing billing information back to the card-issuing bank so that it can be displayed on cardholder statements; this is a program for promoting the use of credit cards for business purchases by providing purchase tracking to business users. New regulations require that this billing information be passed back with the transactions; otherwise, a higher pass-through fee will be incurred.

Credit Reversal:

Nullification of an authorized transaction (sale) that has not been settled. If supported by the card issuer, a reversal will immediately "undo" an authorization and return it to the open-to-buy balance on a cardholder's account. Some card issuers do not support reversals.

DDA Account:

This is the merchant's Demand Deposit Account, otherwise known as the merchant's home town bank account.

Debit Card:

Payment card whose funds are withdrawn directly from the cardholder's checking account at the time of sale (online debit on a Debit Network) or after batch settlement (off-line debit on a Credit Card Network).

Discount Rate:

The percentage of sales amounts that the bankcard acquirer card-issuer charges the merchant for the settlement of the transactions.

Edit Rejects:

The rejection of a sales draft by Visa or MasterCard before a transaction processes through interchange, but after it has been paid by the acquirer.

Electronic Data Capture (EDC):

Process of electronically authorizing, capturing, and settling a credit card transaction.

Fleet cards:

Private label credit cards designed mainly for repairs, maintenance, and fueling of business vehicles.

Footer:

Text printed at the bottom of a sales draft. A merchant can customize the footer (i.e., Have a Nice Day, No Refunds, Thank You for Shopping with Us, etc.).

Interchange:

The standardized electronic exchange of financial and non-financial data associated with sale and credit data between merchant acquirers and card issuers on various types of MasterCard and Visa transactions.

Interchange Fee:

A fee paid by an acquirer to an issuer for transactions entered into interchange. The interchange fee is a percentage applied, according to Visa/MasterCard regulations, to the

dollar value of each transaction. There are multiple categories of interchange, and Visa and MasterCard each have their own criteria for their own categories. A transaction must meet the specified criteria for a category in order for that category's rate to be applied. Each transaction is evaluated individually, so various interchange rates may apply within one batch of merchant transactions.

Issuing Financial Institution:

The financial institution that extends credit to a cardholder through bankcard accounts. The financial institution issues a credit card and bills the cardholder for purchases against the bankcard account. Also referred to as the cardholder's financial institution.

Manual Close:

A batch close that must be initiated by the merchant on a daily basis, as opposed to an auto close at a pre-set time.

Merchant:

Customer of a processor/acquirer.

Merchant Identification Number (MID):

This number is generated by a processor/acquirer and is specific to each individual merchant location. This number is used to identify the merchant during processing of daily transactions, rejects, adjustments, chargebacks, end-of-month processing fees, etc.

Magnetic Stripe:

A strip of magnetic tape affixed to the back of credit cards containing identifying data, such as account number and cardholder name.

Mail Order/Telephone Order (MOTO):

Credit card transactions initiated via mail, email, or telephone. Also known as card-not-present transactions.

Network:

Company and system used to authorize and capture credit card transactions.

Non-Qualified Transaction Fees (Non-Qual):

Bankcard sales transactions that do not meet set Visa/MasterCard criteria for that particular merchant and are processed at a higher interchange rate. An example of this is a merchant that is retail (card present) that processes a card-not-present transaction (or manually enters card data rather than swiping the magnetic stripe through the terminal). The merchant will pay the difference between what they should have paid on retail and what they actually qualified for (card not present). This difference is called a non-qualified interchange fee.

PC Software:

A software program that is designed to perform a specific function on a computer system. Examples would be accounting systems, manufacturing systems, order entry and fulfillment, ticketing, reservations, etc. The application is either purchased or built by the merchant, and must be interfaced with a credit card authorization system in order to provide on-line transaction processing.

Private Label Cards:

Credit, debit, or stored-value cards that can be used only within a specific merchant's store. Also referred to as proprietary cards.

Point of Sale (POS):

A location where credit card transactions are performed with the cardholder present, such as a retail store. The card is read magnetically, and the cardholder's signature is obtained as insurance against the transaction. This is the most secure form of credit card commerce.

POS Terminal:

Equipment used to capture, transmit, and store credit card transactions at the point of sale. Examples are Verifone terminals.

Procurement/Purchasing Cards:

Charge cards used by businesses to cover purchasing expenses, such as raw materials or office supplies.

Real-Time Processing:

Real-time processing means that when a website's customer conducts an online purchase, the check or credit card information is conveyed to the Processor at that exact time so that an authorization can be requested and received at that moment. Real-time processing always implies that a Secure Payment Gateway is being utilized, whether proprietary or third party.

Reserve Account:

One method that ACH Processors use to mitigate risk is to require that merchants maintain a reserve account at the Processor's Sponsoring Bank. This allows the Processor to issue a hold on funds in this account when fraud has been detected or an excessively large number of returns are received. Merchants with good credit and history can usually meet the expectations of ACH Processors for covering returns and are not always required to keep a reserve account. In cases where a reserve is required, the minimum reserve balance in the account is set at about 20% of the anticipated processing volume. New merchants are usually allowed to build up their reserve by sending in transactions which are not withdrawn until the minimum reserve balance is achieved; after that, the merchant is allowed to withdraw the excess funds for transfer to their hometown bank.

Sales Draft (Ticket):

A form showing an obligation on the cardholder's part to pay money (i.e., the sales amount) to the card issuer. This is the piece of paper that is signed when making the purchase. Sales draft data can be captured electronically and sent to be processed over the phone lines. Also see Electronic Data Capture.

Secure Payment Gateway:

Secure Payment Gateway companies help other Processors conduct secure business on the internet using Secure Socket Layer (SSL) technology.

Settlement:

The process of sending a merchant's batch to the network for processing and payment. For non-bankcards, the issuer pays the merchant directly (less applicable fees) and then bills the cardholder. For bankcards, the acquirer pays the merchant (less applicable fees) with funds from Visa/MasterCard. The bankcard issuer then bills the cardholder for the amount of the sale. Also see Capture.

Shopping Cart Software:

These applications typically provide a means of capturing a client's credit card information, but they rely on the Software Module of the Secure Gateway Provider (in conjunction with the Secure Payment Gateway) in order to conduct secure credit card transactions online. Any given shopping cart can work with any given Secure Gateway Provider, the only requirement being that some computer code be written or provided to communicate with the Secure Gateway of choice, and that this code be integrated into the Shopping Cart Application.

Software:

A POS Terminal Application or PC or Internet Application that runs transactions and associated administration.

Smart Card:

A credit-type card that electronically stores account information in the card itself utilizing chip technology rather than a magnetic stripe.

Terminal:

Equipment used to capture, transmit, and store credit card transactions.

Terminal Software:

Programming that determines the characteristics and features of the terminal.

Terminal Identification Number (TID):

A unique number assigned to each POS terminal.

UNDERSTANDING YOUR RATES AND FEES

When a merchant processes a card, they are charged a fee called interchange. Interchange is the base rate dictated by Visa and MasterCard. Interchange is made up of varying tiers. These tiers describe costs for different kinds of credit cards when processed under different circumstances. The method of how a credit card is processed changes which tier of Interchange is applied. For example, a swiped credit card costs less to process than one keyed into a credit card terminal.

Each of a merchant's credit card transactions will be classified as qualified, mid-qualified or non-qualified. Transactions that do not satisfy all of the required qualified transaction conditions, as established by Visa and MasterCard, are assessed either a mid-qualified or a non-qualified surcharge. The type of credit card used in a transaction is one factor that establishes how a transaction is classified. For example, corporate cards are often considered high-risk. Therefore, a transaction done with a corporate card may cost a merchant a higher surcharge.

Other aspects that determine whether a transaction is classified as qualified, mid-qualified, or non-qualified are whether the address verification system (AVS) is used and whether the transaction is settled or batched on time. To ensure that a merchant is getting the best possible rate on transactions, they need to settle each night after transactions have been processed, enter the correct AVS information when asked, process through the correct account type, and use PIN-based debit when applicable. This will help to get the lowest rates possible on each transaction.

Qualified discount rate

This is the percentage that will be charged on all of a merchant's credit card sales. Swiped credit cards have a lower discount rate because the cardholder is present and the risk is lower. Most swiped transactions go through at a qualified rate unless they are a corporate or foreign card, or do not meet another regulation for qualified status.

Mid-qualified surcharge

This applies to merchants who swipe credit cards but do not meet the requirements for a qualified level. For example, when a credit card is swiped and the magnetic strip cannot be read in the terminal, or when there is a telephone, mail, or internet order, a merchant will key in the transaction. A surcharge will be applied to the transaction because it does not meet the requirements of a qualified rate. Also, keyed credit cards will have a higher discount rate due to the fact that there is more risk involved in accepting the credit card because the cardholder is not present with a phone, mail, or internet order. It could also indicate fraud if the magnetic strip is not functioning.

Non-qualified surcharge

This applies to both swiped and keyed merchants. Whenever a corporate or foreign card is used, or the AVS system is not utilized when keying in a credit card, the non-qualified surcharge will apply.

Transaction Fee

This is a flat fee, and is charged each time a merchant runs a transaction. This is in addition to the discount rate surcharge.

Batch Header Fee

At the end of each day, a merchant will either manually close out for deposit (settle/batch), or the merchant account will automatically be set up to close out for deposit. Once this is done, the funds will travel through the ACH system electronically to deposit the funds into the merchant's checking account. The batch header fee is applied for each batch closed out for deposit. Some merchants try to "save money" by not batching every night to avoid this fee. This is not a smart plan of action, because if a terminal is not batched within 24 hours of the transaction processing, you will be charged a higher rate (mid-qualified). In order to receive the best rate, batch every day.

Wireless Access Fee

This fee is assessed for merchants utilizing a wireless terminal. Wireless access will allow a merchant to process transactions through the wireless network, rather than processing transactions through a telephone landline. Once a transaction is completed through the wireless terminal, it travels through the wireless network for processing.

Gateway Access Fee

This fee is assessed for merchants utilizing Internet processing or a virtual terminal. Once a transaction is completed by the customer on a merchant's website, or through the virtual terminal, it travels through the Internet gateway for processing

ROLE OF LOSS PREVENTION

Over holidays, tourist seasons, and just in everyday shopping, fraudulent transactions occur more than most people realize. According to the recently released 17th Annual Retail Theft Survey, U.S. retailers lost more than \$13.2 billion from employee theft and more than \$29 billion total last year.

What is Loss Prevention?

The Loss Prevention Department was created to protect merchants and help control fraud in their day-to-day transactions. Merchants are vulnerable to consumer scams but also losses due to dishonest employees.

Certain types of transactions will be red flags to the Loss Prevention team to alert the merchant of potential criminal activity.

Where Inventory Shrinkage Happens

- Employee Theft 44.5%
- Shoplifting 32.7%
- Administrative Error 17.5%
- Vendor Fraud 5.1%

As you can see by the statistics above, employee theft accounts for almost half of all loss. Part of this is directly related to credit card transactions. Merchants should be aware that their trusted employees could be committing crimes. There are many types of employee fraud, including:

- Employees processing returns on their own card for merchandise bought by a customer
- Employees processing a customer's credit card, saying it is declined when it is not, and then asking for another form of payment (usually cash which they keep for themselves)
- Sharing/selling card information to criminals
- Employees issuing credits to their own credit cards through the merchant's account, putting small amounts into their own bank account over a long period of time
- Voiding transactions after a sale to put money in their pocket from the register or provide "free" goods/services to friends

An ACFE research study shows that fraud is not usually committed by career criminals but by longtime employees who are high on the company's organizational chart. These employees have greater access to company funds and information, and tend to be more trusted or above suspicion than those lower in the ranks.

How Can I Protect Myself From Employee Fraud?

Merchants don't have to be paranoid that their employees are stealing from them, but should be aware of the risks to protect their businesses nonetheless. To help avoid internal fraud, merchants can:

- Distribute responsibilities among employees so that different employees collect receipts and make out deposit slips
- Review bank statements and write checks yourself
- Periodically open your own mail and compare payments received with deposits
- Hire an outside accountant to audit your books
- Require two signatures on checks over a certain amount
- Review billing error complaints from customers and require that original invoices be kept in the files

Consumer Fraud

In addition to internal fraud by employees, merchants should also be aware of consumer fraud. Although it is not as high on the list, it is easier to detect and the Loss Prevention team can help.

For instance, if a customer came into a store and attempted to make a very large purchase (the largest the merchant had seen to date), the Loss Prevention team would flag the transaction and contact the merchant. It could just be that the merchant had a larger-than-normal purchase by a non-fraudulent customer, but it could also be that customer was trying to use a stolen credit card, or was attempting one of many other scams.

To avoid having your bank account suspended, merchants must also be aware of their high ticket limit (V/MC) and not process transactions over that amount. If there is a determined customer wanting to process a large transaction over the limit, inform them that they can use a debit card, American Express, or Discover.

As we do not monitor the limits for those types of transactions, our Loss Prevention team will not flag a merchant's bank account for an over-the-limit transaction. If there is a transaction close to the limit, merchants should call their Loss Prevention team to inform them of the transaction.

The goal of the Loss Prevention team is to help merchants reduce these risks and keep losses due to fraud to a minimum.

RECONCILIATION HELP

What is Reconciliation?

Reconciliation is the process of balancing the transactions you've run that come in your monthly statement against your bank's records. For example, you might want to make sure that your merchant statement balance matches your online banking balance to ensure that your account information is up to date.

While we try to make it very straightforward to record deposits that correspond to individual customer payments, it can be difficult to match these individual transactions to the batched deposit totals that appear on your bank account statement.

Why Reconcile?

Many businesses get by without reconciling their merchant statement balances with their bank account balances. However, this can lead to confusing differences and questions about how much money is actually in your account at a given time.

Ultimately, the decision to reconcile is yours, based on your business needs. If you've been able to make do despite discrepancies, reconciliation may not be necessary for your business. That said, if reconciliation can help you make more efficient use of your cash flow, it may be worth taking the time to get your accounts reconciled and keep them balanced. If you're thinking reconciliation sounds like something that would be good for your business but hard to accomplish, now is a good time to give reconciliation another look.

Daily Discount Billing

If you are on daily discount billing, your fees are taken out on a daily basis. For example, if you ran a \$100.00 transaction, and you only saw \$98.00 on your bank statement, the fees are taken out daily. This is nice for smaller businesses that do not always have a bulk sum of money at the end of the month for monthly discount fees.

Monthly Discount Billing

If you are on monthly discount billing, your fees are taken out on a monthly basis. For example, if you ran a \$100.00 transaction, you will see a \$100.00 transaction on your bank statement. At the end of the month, you will see the \$2.00 fee deducted. This is nice for larger businesses who will have a lump sum of money at the end of the month, and who have run many transactions.

MONEY SAVING TIPS

AVS:

AVS stands for "Address Verification Service." It is a validation system that determines whether or not the street number and zip code entered by the purchaser is actually a match with the issuing bank's "on file" information for that same cardholder.

It is important to know that AVS does not work on most foreign cards, and the AVS service is not available overseas. This is one of the reasons why foreign transactions are considered "higher risk" by U.S. banks and why such transactions have a higher cost.

When you key in a card, try to get the correct street number (example: If the address is 400 N 100 W, the street number would be 400) and the correct zip code. This will help the transaction get approved on the lowest possible discount rate.

Understanding a Batch:

Whenever you run through one or more sales transactions, you are granted an "authorization code" for each successful one. These authorization codes and transactions are grouped together into a "batch."

At the end of each day, you may be set up to automatically "settle" your batch - which means we transmit the list of orders through the bankcard network which subsequently serves to begin the funds transfer process between the cardholder's bank and our merchant bank.

Or, you may have chosen to enter the batch manually. Either way, batching on time will prevent your transactions from downgrading due to failing to batch within 24 hours of a transaction.

PIN Debit:

Often overlooked is the PIN debit system. Using this system, your customers can choose to enter their PIN (Personal Identification Number) into a PINpad similar to using an ATM

machine. Using PIN debit will reduce your overall processing fees, and will also completely eliminate any potential downgrades for PIN Debit transactions.

CHARGEBACK AND RETRIEVAL FAQs

What is a "chargeback?"

Occasionally, a cardholder will dispute a charge that appears on their monthly bankcard statement and/or it may be discovered that the proper bankcard acceptance and authorization procedures were not followed at the point of sale.

If this happens, the merchant's bank or processor will notify them of the dispute and debit the amount from the deposit account. This is called a "chargeback."

I just received a retrieval request. What do I do with it?

A merchant should immediately gather their originating documentation for this transaction.

I just received a Notification of Chargeback. What is it and what do I do with it?

A Notification of Chargeback is notification to a merchant that a chargeback has been initiated. A merchant should read the reason for the dispute on the letter, and if it is incorrect, immediately fax supporting documentation and the Notification of Chargeback to your processing company.

If the issuing bank accepts the documentation, the chargeback has been resolved and no funds have been deducted from the merchant's account. If the cardholder disputes the reversal, a second chargeback may be initiated. In addition, if the processor has information to contradict the claim, or if the documentation does not support the case, the chargeback will be debited from the merchant's account.

Your processing company has a unique way of managing chargebacks. When a chargeback is initiated, the card issuing bank posts a debit to the processor for the amount of the chargeback. Most processors immediately debit the merchant. However, in most cases, your processing company does not post the chargeback to the merchant's account until the entire process is complete. Certain types of chargebacks (for example: Declined Authorization or Non-receipt of Draft) are immediately posted to the merchant, as the merchant has no chance of prevailing in the dispute.

Our process provides the merchant time to gather and submit the proper information to dispute the chargeback. If the merchant wins the dispute, no money has ever been deducted from their account. If the chargeback is valid, the merchant is debited.

Why couldn't this chargeback be taken out of my reserve account instead of my regular checking account?

A reserve is set up for security purposes to protect the merchant account processor from losses due to chargebacks. The reserve is usually for merchants who accept non-face-to-face transactions (phone, mail, and Internet orders). The reserve is held in case of default by a merchant.

When will I be notified of a chargeback and when are funds removed from my checking account?

Your processing company will mail a Notification of Chargeback when the debit is transmitted to a merchant's bank. If the chargeback is valid, it takes 2-3 business days for a debit to reach the merchant's checking account.

Is the risk of chargeback greater if I manually enter the credit card number?

If the merchant is a general retail merchant where a card is present, but does not get an imprint (manual or electronic), they may lose money through a chargeback when the cardholder disputes the transaction.

Who is going to pay for my bounced check fees because this chargeback was taken from my account?

Per the merchant's contract with the processor, the merchant should keep enough money in his account to cover any chargebacks.

I issued a credit and I still received a chargeback. Why?

In these cases, for some reason the issuer did not see the credit issued by the merchant. Sometimes the credit is issued after the chargeback was initiated and they 'cross'. All the merchant has to do is represent the item and it will be credited to the merchant's account.

I was told that an authorization guaranteed payment.

An authorization will only verify that an account is open and that there are funds available. However, if a card has been stolen and the loss has not yet been reported, any charges made by the criminal can later be charged back by the cardholder.

What can I do to prevent this from happening?

General retail merchants usually do not have problems with chargebacks. Mail, phone, and Internet merchants can minimize chargebacks by making sure the name under which they advertise and the name they use to process are the same, or by printing the processing name in a prominent place on the receipt. Be sure to include a receipt with any product sent to the customer. Reply promptly to retrieval requests. Authorize every transaction and use the AVS if possible. If the merchant uses AVS, they should not ship to an address different than the address verified.

MERCHANTS GUIDE TO RISK MANAGEMENT

We are committed to helping you to control and prevent fraud. With the growth of e-commerce and the rise of identify theft, fraud prevention has never been as critical. It is not just e-commerce and mail order transactions that require extra diligence. Face to face transactions are also subject to continuing fraud attempts.

Scam artists are more savvy than ever before and understand the latest security features that Visa and MasterCard are creating to control this problem. Merchants must be alert and take extra precautions wherever possible, because they are financially responsible for fraudulent transactions, including those approved by the bank that issues the consumer's credit card.

Through the accompanying documents and links, we hope to provide the basic information you will need to help prevent fraud from occurring in your business.

Visa/MasterCard Terminal Response Codes

Response

Approved

Ask the customer to sign the sales receipt.

Declined

Return the card to customer and ask for another Visa card.

Call or Call Center

Call your voice authorization center and tell the operator that you have a "Call" or "Call Center" response. Follow the operator instructions. Note: In most cases, a "Call" or "Call Center" message just means the card Issuer needs some additional information before the transaction can be approved.

Pick Up

Keep the card if you can do so peacefully.

No Match

Swipe the card and re-key the last four digits.

If "no match" response appears again, keep the card if you can do so peacefully. Request a Code 10 authorization.

Introduction to the Chargeback Process

Chargeback

As a general rule, cardholders have the right to dispute any transaction processed on a Visa/MasterCard. These disputes are called chargebacks, and are governed by a series of rules set forth by these entities. In the chargeback process, the burden of proof lies with the merchant.

The merchant will be given the opportunity to provide supporting documentation to prove the legitimacy of the transaction. If the merchant is successful, the transaction is credited back to his account. If the merchant is unsuccessful, or does not respond in a timely fashion, they will be financial responsible for returning funds to the consumer who filed the dispute.

Summary of Chargeback Process

When a chargeback is initiated, the Issuer gives the cardholder provisional credit. In turn, the Issuer sends a request to the merchant's Acquiring Bank. The Issuing Bank is often required to submit the documents that support the customer's dispute. To facilitate the handling of the dispute, we use an "auto-resolve" database that automatically places the chargeback in a pending status, waiting for the Issuing Bank documents to arrive.

The system will auto-resolve the case in the event the bank documents do not arrive and will send the chargeback back to the Issuer. When the bank documents are received, the system may place the case in a queue for a chargeback operator to process, or automatically debit the merchant and generate the chargeback letter.

The chargeback letter gives the merchant about 8-10 days to respond. No second warning is sent in absence of a response. At times, the request comes in at a later time. It is **IMPORTANT** that the merchant always checks the "**Respond by**" date on top of the communication letter to insure that the response is sent on time.

A **case number** is assigned to each disputed item. The merchant must attach the correct case number to each page of the rebuttal paperwork. Cardholders may dispute a charge for various reasons (i.e. "Non-Authorization", "Merchandise not received"), and often attach a letter of explanation to the output package. Merchant's rebuttal must address each one of the customer's complaints.

A rebuttal letter containing the merchant's point of view should always accompany the paperwork. As a default, we send the letters to the business address indicated by the merchant. Once the rebuttal paperwork is received by the chargeback department, the case is reviewed and, if applicable, it is reversed back to the Issuer.

A credit to the merchant for the transaction amount will be granted in that instance. In the event the documents do not provide a valid reason to reverse the dispute, the Chargeback Department will try to contact the merchant for more information.

Chargeback fees will apply on each disputed item. Fees are debited as follows:

MO/TO - Internet accounts: fees are debited **immediately** when the chargeback is initiated by the Issuing Bank.

Retail accounts: fees are charged when the chargeback is in the working stage at EVO, and the merchant is given the time to respond. In the event the chargeback comes in, but it is immediately reversed back to the Issuer with no request of documentation on the merchant's side, no charge will apply.

Chargeback Cycle

Visa

- First Chargeback initiated by Issuer
- Representment (rebuttal) initiated by Acquirer
- If there is no resolution, the Issuer can request the Pre-Arbitration/Arbitration

MasterCard

- First Chargeback initiated by Issuer
- Representment (rebuttal) initiated by Acquirer
- Second Chargeback initiated by Issuer
- Pre-Arbitration/Arbitration can be initiated by Acquirer.

Summary of Retrieval Process

Often the first step in the chargeback process is a request made by the Issuing Bank for the **transaction information document (TID)**, or receipt. This request is called retrieval. The Acquirer is obligated to fulfill this request by providing a copy of the transaction receipt.

Alternatively the merchant should respond to the Issuer explaining the reason he cannot honor the request. A retrieval request can simply be a request for the information, or could indicate that the Issuer will initiate a chargeback in the near future.

Upon notification of the retrieval request, a letter is automatically generated to the merchant. This letter states that the merchant has a certain number of days (usually 10 days) to respond by providing the indicated sales draft. On the 11th day, a second and last letter is generated, and sent to the merchant. The sales draft must be submitted to the Issuer on the 28th day from the moment the request has been initiated.

A **case number** is assigned to each request. The merchant must include the correct case number on top of the TID. Once the merchant has responded to the retrieval, a chargeback analyst will review the received documentation. In the event the sales draft is illegible, wrong, or has missing items, the analyst will notify the merchant via phone or fax, when available. If the merchant does not respond within the given timeframe, no notification will be sent to the merchant. A Good Faith Collection letter will be submitted to the Issuing Bank when:

- The transaction has a POS entry of 90 (swiped), and the signed sales slip is available;

- For MO/TO transactions, the merchant matches the AVS (Address Verification), and provides signed proof of delivery.

No partial credit is granted to the customer in the event of a retrieval request. As a result, the merchant will not be debited for the transaction amount, unless the request turns into a chargeback due to non response.

Chargeback Details

I. First Chargeback Phase:

A Cardholder writes a letter or fills out a “Dispute Resolution Form” and submits it to their Credit Card Issuing Bank. The Issuing Bank then processes a chargeback along with the “Chargeback Documentation” (i.e. Cardholder letter) through the corresponding Association (Visa or MasterCard) and thus is credited the disputed transaction amount.

The Acquirer or “Merchant Bank” then receives notification of the Chargeback upon receipt of the “Chargeback Documentation” and is subsequently debited for the disputed transaction amount. At this point the Acquirer internal database assesses the Merchant a “Chargeback fee”. Acquirer’s systems then run the Chargeback through a series of simple filters to check to see if the Merchant issued credit and for certain technical errors. At this point one of two scenarios occurs:

1. If, via the filters, the Chargeback is deemed invalid, Acquirer “Reverses” the Chargeback back through the Association and eventually back to the Issuing Bank along with a debit for the disputed amount. The Acquirer is then credited for the amount in dispute. The Chargeback fee remains on the Merchant’s account as this is a fee charged by the Associations as a cost for processing the Chargeback. This “First Chargeback” phase of the dispute is then considered “Resolved To the Issuing Bank” and will remain closed unless the Issuing Bank initiates a “Pre-Arbitration” notification (Visa) or a Second Chargeback (MasterCard).
2. If, via the filters, the Chargeback is deemed valid, the Merchant’s business checking account is immediately debited for the amount in dispute and a letter is sent to the Merchant the same day advising of the debit and explaining what, if any, documentation is required to “Reverse” this Chargeback. This “First Chargeback” phase of the dispute is then considered “Resolved to the Merchant” and will remain closed until the Merchant responds back to the letter sent to them.

II. First Reversal Phase:

If the merchant does indeed respond with a “Merchant Letter” back to the Acquirer, a “Reversal Phase” of the dispute is opened and a Chargebacks Analyst will review the Merchant Letter and will see if the merchant’s response and the overall dispute qualify to be “Reversed” back to the Issuing Bank. At this point, one of two scenarios will occur:

1. If the Chargebacks Analyst deems the Merchant’s response as **invalid**, they will close out this phase as “Request Denied” and will mail a letter to the Merchant explaining why

the Chargeback cannot be reversed back to the Issuing Bank at that time.

2. If the Chargeback Analyst deems the Merchant's response as **valid**, the Acquirer "Reverses" the Chargeback back through the Association and eventually back to the Issuing Bank along with a debit for the disputed amount. The Acquirer is then credited for the amount in dispute and in turn credits the Merchant's business checking account. The Chargeback fee remains on the Merchant's account as this is a fee charged by the Associations as a cost for processing the Chargeback. This "First Reversal" phase of the dispute is then considered "Resolved To the Issuing Bank" and will remain closed unless the Issuing Bank initiates a "Pre-Arbitration" notification (Visa) or a Second Chargeback (MasterCard).

III. Second Chargeback and Second Reversal Phase (MasterCard only):

Once a Reversal (and the subsequent debit) is received back at the Issuing Bank, they will then forward the "Merchant's Letter" back to their Cardholder for a response. If the Cardholder wishes to pursue the dispute further, they then send in a "Rebuttal Letter" back to the Issuing Bank and if the Issuing Bank feels that their response is valid, will submit a **Second Chargeback**.

A Second Chargeback functions just like a First Chargeback, except a Chargeback fee is not assessed and the disputed amount is immediately debited out of the Merchant's business checking account. The Merchant is sent another letter explaining what, if any, documentation is required to pursue this dispute further. This "Second Chargeback" phase of the dispute is then considered "Resolved to the Merchant" and will remain closed until the Merchant responds back to the letter sent to them. If the Merchant does indeed respond to the letter sent to them a "**Second Reversal**" phase of the dispute is opened. An Acquirer Chargeback Analyst will then review the letter and one of two scenarios will occur:

1. If the Chargeback Analyst deems the Merchant's response as **invalid**, they will close out this phase as "Request Denied" and will mail a letter to the Merchant explaining why the Chargeback cannot be pursued further at that time.
2. If the Chargeback Analyst deems the Merchant's response as **valid**, they will submit a "**Pre-Arbitration**" letter directly to the Issuing bank advising that the Acquirer believes the Merchant's claim is valid and that Acquirer will request MasterCard to make an Arbitration ruling on the dispute if the Issuer disagrees with the Merchant's claim.
 - a. If the Issuing Bank agrees with the Merchant's claim, they will simply forward the funds back to the Acquirer and the Acquirer will then credit the Merchant's business checking account accordingly. The dispute at this point is considered "Successful" and cannot be re-opened.

IV. Issuing Bank Pre-Arbitration Phase (Visa only):

Once a Reversal (and the subsequent debit) is received back at the Issuing Bank, they will then forward the "Merchant's Letter" back to their Cardholder for a response. If the Cardholder wishes to pursue the dispute further, they then send in a "Rebuttal Letter" back to the Issuing Bank and if the Issuing Bank feels that their response is valid, will submit a "**Pre-Arbitration**"

letter directly to the Acquirer advising that they feel that their Cardholder's claim is valid that they will request Visa make an Arbitration ruling on the dispute if the Acquirer disagrees with the Cardholder's claim. The Merchant is then sent another letter along with the Cardholder's rebuttal advising that they need to respond within 10 days. If the Merchant does not respond to the letter within the specified timeframes, the Acquirer Chargeback Analyst will credit the Issuing Bank back for the disputed amount and in turn debit the Merchant's business checking account. This phase of the dispute will then be closed as "Unsuccessful". If the merchant does indeed respond within the specified timeframe, one of two scenarios will occur:

1. If the Chargeback Analyst deems the Merchant's response as **invalid**, they will close out this phase as "Request Denied" and will credit the Issuing Bank back for the disputed amount and in turn debit the Merchant's business checking account. The Chargebacks Analyst will also mail a letter to the Merchant advising of the debit and will also explain why the Chargeback cannot be pursued further at that time.
2. If the Chargeback Analyst deems the Merchant's response as **valid**, the Acquirer will then send a form to the Merchant requesting that they sign the form which makes the Merchant liable for Arbitration filing fees. (When Visa makes an Arbitration ruling, it assesses a \$400.00 filing fee to the loser of the dispute) If the Merchant does not agree to the fees, the Acquirer simply closes out the Pre-Arbitration phase of the case as "Unsuccessful" and will credit the Issuing Bank back for the disputed amount and in turn debit the Merchant's business checking account. If the Merchant does indeed agree to the fees and submits the signed form, the Acquirer then responds to the Issuing Bank advising them that they do not agree with the Cardholder's claim. The Issuing bank then submits an Arbitration Request directly to Visa.
 - a. If Visa rules in the Merchant's favor, all funds remain where they are and in addition, The Issuing Bank is assessed the \$400.00 in filing fees. The Acquirer then closes this phase of the dispute as "Successful"
 - b. If Visa rules in the Issuing Bank's favor, they are immediately credited for the amount in dispute and the Acquirer is immediately debited for the same amount and in turn this amount is immediately debited from the Merchant's business checking account along with the \$400.00 in filing fees. The Acquirer then closes this phase of the dispute as "Unsuccessful"

Preventing Chargebacks

Most chargeback situations arise at the point of transaction—at the time the transaction is completed—and most can be prevented with a little training.

Consider these tips to avoid potential chargebacks...

Card Present Transactions

1. **Do not complete a transaction if the authorization request was declined.** Do not repeat the authorization request after receiving a decline.

2. **If you receive a “Call” message in response to an authorization request, call your authorization center.** Be prepared to answer questions. The operator may ask to speak with the cardholder. If approved, write the authorization code on the sales receipt. If declined, ask the cardholder for another Visa card.
3. **Make an imprint for all card-present transactions.** If you have a point-of-sale terminal with a magnetic-stripe reader, swipe the card through the reader for every face-to-face transaction. If the terminal isn't working or a card's magnetic stripe cannot be read, key-enter the account information and make an imprint of the embossed information onto the sales receipt using a manual imprinter. Even if the transaction is authorized and the cardholder signs the receipt, if the receipt does not have an imprint of the embossed account number and expiration date, the transaction may be charged back to you for “no imprint” if the cardholder later denies participating in the transaction.
4. **Obtain cardholder signature.** The cardholder's signature on card-present transactions is required. Failure to obtain the cardholder's signature could result in a chargeback for “no signature” if the cardholder denies authorizing or participating in the transaction. Always compare the signature on the sales slip and the signature on the back of the card. If the card does not carry any signature, ask the customer to show you a picture ID, and have him sign the card at the time of purchase.
5. **Make only one imprint of the card for each transaction.** Making more than one imprint can lead to duplicate deposits and increase the chance of a chargeback. If you need to redo a sales receipt because of an error, write “VOID” across the incorrect sales receipt, inform the cardholder, and tear up the incorrect sales receipt in view of the customer.
6. **Ensure that transactions are entered into point-of-sale terminals only once—and deposited only once.** Entering the same transaction into a terminal more than once, or depositing both the merchant copy and the bank copy of the sales receipt with your acquirer, or depositing the same transaction with more than one merchant bank can all result in “duplicate transaction” chargebacks.
7. **Ensure that incorrect sale receipts are voided and that transactions are processed only once.**
8. **If your establishment has policies regarding merchandise returns, refunds, or service cancellation, disclose these policies to the cardholder at the time of the transaction.** Your policy should be pre-printed on your sales receipts within ¼ inch of cardholder's signature; if not, write or stamp your refund/return policy information on the sales receipt near the customer signature line before the customer signs (be sure the policy shows clearly on all copies of the sales receipt). Failure to disclose such policies at the time of the transaction will be to your disadvantage should the customer return the merchandise.
9. **Deposit sales receipts with your merchant bank as quickly as possible, preferably within one to five days of the transaction date—do not hold on to them.** Failure to deposit in a timely manner can result in chargebacks for “late presentment.”

- 10. Deposit credit receipts with your acquirer as quickly as possible, preferably the same day as the credit transaction is generated.** Failure to process credits in a timely manner can result in chargebacks for "credit not issued."
- 11. Keep customers informed on the status of their transactions.**
- 12. If the merchandise or service to be provided to the cardholder will be delayed, advise the cardholder in writing of the delay and the new expected delivery or service date.**
- 13. If the merchandise ordered by the cardholder is out of stock and delivery will be delayed or this item is no longer available, advise the cardholder in writing and offer the cardholder the option of purchasing a similar item or canceling the transaction.** Do not substitute another item unless the customer agrees to accept it. By giving the customer notice and the option to cancel, you may help avoid a customer dispute regarding the merchandise and a possible chargeback.
- 14. Ship merchandise before depositing transaction.** Don't deposit transactions with your merchant bank until you have shipped the related merchandise. If customers see a transaction on their monthly Visa statement before they receive the merchandise, it could lead to a preventable chargeback.
- 15. When refunding a customer, always credit the same card that was used for the corresponding sale.**
- 16. Respond to all sales draft requests.** Should you receive a request for copy of sales draft, respond immediately. Failure to send in copy will result in a chargeback with no representment rights.
- 17. Change printer ribbon frequently- illegible sales drafts can also initiate chargebacks**

Card-not present Transactions:

- 1. Do not complete a transaction if the authorization request was declined.** Do not repeat the authorization request after receiving a decline.
- 2. If a customer requests cancellation of a recurring transaction which is billed periodically (monthly, quarterly, annually), always respond to the request and cancel the transaction immediately or as specified by the customer.** As a customer service, advise the customer in writing that the service, subscription, or membership has been cancelled and state the effective date of the cancellation. Failure to respond to customer cancellation requests almost always leads to chargebacks.
- 3. If the merchandise or the service to be provided to the cardholder will be delayed, advise the cardholder in writing (e-mail for e-commerce merchants) of the delay and the new expected delivery or service date. Also, if the item is out of stock or no longer available, offer the cardholder the option of purchasing a similar item or canceling the transaction.** Do not substitute another item unless the customer

agrees to accept it. By giving the customer notice and the option to cancel, you may help avoid a possible chargeback.

4. **Ship merchandise before depositing transaction.** Don't deposit transactions with your merchant bank until you are about to or have shipped the related merchandise. If customers see a transaction on their monthly Visa statement before they receive the merchandise, it could lead to a preventable chargeback.
5. **When refunding a customer, always credit the same card that was used for the corresponding sale.** Do not offer a check or other form of payment in place of a refund.
6. **Use the Address Verification tool (AVS) and require a perfect match on cardholder's billing address.** Partial AVS match will not stand in a "non authorization" chargeback scenario. If you need assistance in setting the AVS properly on your Gateway, contact your payment gateway provider or the Loss Prevention department of your credit card Processor for assistance.
7. **Make sure the billing and the shipping address are the same.** If not, make sure you verify the shipping address. You can search through the Yellow-White pages, ask for a copy of a utility bill, or a copy of a Driver's License to validate the shipping address. You can also ask the customer to call the Issuer and add the new address to the billing information
8. **Obtain and verify the Card Code (CVV2/CVC2).** This is the 3-4 digits number on the back of your card (on the front for American Express). This information can be captured only if your shopping cart, and your gateway are set up for it. Please, contact your webmaster and/or Gateway provider for details.
9. **Cancellation/Return Policy needs to be acknowledged by cardholder.** Policy needs to be acknowledged by the customer. For telephone or mail order merchants, policy must be acknowledged with a signature on the order form, contract, or invoice. For e-commerce merchants, policy can be incorporated in the online Terms and Conditions of the sale, and require the cardholder to click on an "I agree" button before completing the order.
10. **Generate an RMA number for submitted cancellations.**
11. **Obtain signed proof of delivery.** Tracking numbers without a signature are not considered valid proof of delivery.
12. **Verify the Internet Protocol (IP) address.** Even though the IP verification is not a 100% guarantee, adding this feature will help you detect fraud. Your Gateway provider and/or other software vendor should be able to help you get started with this validation process. There is a variety of IP validation software that can be downloaded at no cost.

12 potential signs of Card Not Present Fraud

Keep your eyes open for the following fraud indicators. When more than one is true during a card-not-present transaction, fraud might be involved. Follow up, just in case.

1. **First-time shopper:** Criminals are always looking for new victims.
2. **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, fraudsters need to maximize the size of their purchase.
3. **Orders that include several of the same items:** Having multiples of the same item increases a criminal's profits.
4. **Orders made up of "big-ticket" items:** These items have maximum resale value and therefore maximum profit potential.
5. **"Rush" or "overnight" shipping:** Crooks want these fraudulently obtained items as soon as possible for the quickest possible resale, and aren't concerned about extra delivery charges.
6. **Shipping to an international address:** A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the U.S. Visa/MC address verification (AVS) can't validate non-U.S., except in Canada and the United Kingdom or few other banks who participate in the US AVS program.
7. **Transactions with similar card account numbers:** Particularly useful if the account numbers used have been generated using software available on the Internet.
8. **Shipping to a single address, but transactions placed on multiple cards:** Could involve an account number generated using special software, or even a batch of stolen cards.
9. **Multiple transactions on one card over a very short period of time:** Could be an attempt to "run a card" until the account is closed.
10. **Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses:** Could represent organized activity, rather than one individual at work.
11. **In online transactions, multiple cards used from a single IP (Internet Protocol) address:** More than one or two cards could definitely indicate a fraud scheme.
12. **Orders from Internet addresses that make use of free e-mail services:** These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

Visa – MasterCard Card Not Present fraud prevention tools

Appropriate preventive action can help reduce fraudulent transactions and potential customer disputes. Make use of these Visa tools and controls to verify the legitimacy of the Visa cardholder and the card in every card-not-present transaction.

Address Verification Service (AVS)

Allows card-not-present merchants to check a cardholder's billing address with the card Issuer. The merchant includes an AVS request as part of the authorization and receives a result code indicating whether the address given by the cardholder matches the address on file with the Issuer.

Card Code Verification (CVV2- CVC2)

This is a three-digit number imprinted on the signature panel of Visa-MasterCard cards to help card-not-present merchants verify that the customer has a legitimate card in hand at the time of the order. The merchant asks the customer for the card code and then sends it to the card Issuer as part of the authorization request. The card Issuer checks the card code to determine its validity, then sends a result back to the merchant along with the authorization.

Verified by Visa (VbV)

Enables e-commerce merchants validate a cardholder's ownership of an account in real-time during an online Visa card transaction. When the cardholder clicks "buy" at the checkout of a participating merchant, the merchant server recognizes the registered Visa card and the "[Verified by Visa](#)" screen automatically appears on the cardholder's desktop. The cardholder enters a password to verify his or her identity and the Visa card. The Issuer then confirms the cardholder's identity.

MasterCard SecureCode

MasterCard enables e-commerce merchants to actually validate that a MasterCard cardholder is authorized to use the card and qualify the transaction for a guaranteed payment that protects against cardholder unauthorized chargebacks.

MasterCard SecureCode runs on your website and interacts with both the customer and their card Issuer. When your customer is checking out, a simple pop-up box appears asking them to enter a private code that has been registered with their bank.

Their bank then validates that code and provides you with a means of achieving a fully guaranteed transaction.

For more information, visit <http://www.mastercardmerchant.com/securecode/index.html>