CLEARENT™
INTELLIGENT PROCESSING

Card Acceptance Guide

Released September 2006
Revised July 2015

Please Note: This guide is part of the Clearent Merchant Agreement and you must follow the procedures in this guide to comply with your agreement.

Important Information

Merchant ID (MID)

_____

Account Representative Telephone Number

_____

24-Hour Help Desk Number

_____

Voice Authorization Number

_____

Table of Contents

Clearent – Your Partner in Payment Processing

Welcome and thank you for choosing Clearent as your partner for all of your payment processing needs.

Our Role

We are committed to providing legendary customer service, value, and a comprehensive selection of POS solutions for fast, reliable processing and settlement.

Clearent offers a full range of merchant processing services in both traditional transaction processing and emerging payment technologies, including:

- Credit Card Processing
- Debit Card Processing
- Check Guarantee & Electronic Check Acceptance
- Electronic Benefits Transfer Processing
- Web-based Reporting Services
- Supplies
- Terminal Management & Support
- Web-based Transactions

Your Role

As a merchant it is important that you:

- Read, understand, and abide by your Merchant Agreement and this guide to accepting cards for payment
- Take all necessary steps to prevent fraud
- Follow best practices in accepting electronic payment methods
- Advise us of any changes related to your business, such as changes in status, changes in business structure, address or contact information
- Notify Clearent upon canceling or returning equipment
- Call your Account Executive to make any changes or cancellations
- Keep up to date on all industry news and policy changes

Introduction

This guide is part of your Merchant Agreement. **You must follow the procedures in this guide to comply with your agreement.** Please keep this guide handy for reference. We recommend you keep your merchant contract and other paperwork and telephone numbers associated with your Merchant Agreement with this guide.

Payment cards bearing the service mark of companies such as American Express®, Discover Network®, MasterCard®, or Visa® are the most popular type of payment. It is a good business decision to accept electronic payment methods since studies indicate that people who use credit and debit cards can be among your best customers.

When you offer your customers the flexibility that payment cards represent, you are taking an important step in offering customer service, while opening your doors to increased sales volume.

When you accept payment with credit, debit, EBT, prepaid and commercial cards, you gain a competitive edge as well as maintain a positive image, and have the potential to increase your bottom line.

We want you to be comfortable with your merchant services card acceptance program and take advantage of all its features to help your business grow and prosper. The information in this guide has been provided to supplement your Merchant Agreement and will assist you in the operation of your program.

We've included answers to the questions most frequently asked by card-accepting businesses like yours. If you have additional questions not covered in this guide, we encourage you to call and talk with your Account Executive.

Our goal is to provide you with a card acceptance program that is designed to grow with your business. Your comments and ideas help us to constantly develop new ways to meet your needs.

Parties Involved in the Transaction

Customer/Cardholder

The process that involves a customer presenting a payment card to pay for goods and services actually starts some time earlier when the customer opens an account with an issuer of American Express, Discover Network, MasterCard, or Visa cards. The customer, also called a cardholder, is an authorized user of one or more payment products supported by the particular card brand.

Payment Card Issuers

The following list of major brands is not exhaustive, but it covers the primary payment card types we support, and the vast majority of cards you may encounter.

American Express (Amex)

American Express is a financial services company that issues credit and prepaid card products. As a Participant in American Express OptBlue®, Clearent is able to offer our merchants an integrated service and competitive pricing for acceptance of Amex card products. Certain partners may also issue cards bearing the Amex brand that are subject to the same rules and regulations as cards issued by Amex, and Clearent is able to process these for its merchants as well.

The policies and procedures governing merchant acceptance of American Express Cards are contained in the American Express Merchant Operating Guide, a current copy of which can be found at www.americanexpress.com/merchantopguide. The Merchant Operating Guide is a part of, and is hereby incorporated by reference into, this Card Acceptance Guide, which in turn is a part of the Merchant Agreement. As a condition of your agreement to accept American Express Cards, you agree to be bound by and accept all provisions in the Merchant Operating Guide (as changed from time to time) as if fully set out in the Merchant Agreement.

Please also note the following:

- By choosing to accept American Express Cards when you apply for a merchant services account with Clearent, you permit us to disclose certain data to American Express, including contact information, and agree that American Express may send you commercial marketing messages, including important information about American Express products, services, and resources available to your business. More information about marketing communication, including how to opt-out of such communication, is provided in the Merchant Operating Guide (www.americanexpress.com/merchantopguide).
- Over the course of your processing relationship with Clearent, American Express may at some point determine that your annual Amex Charge Volume has exceeded $1,000,000.00 USD, and will notify us that you can no longer participate in the OptBlue program. At that point you will be considered an AXP Direct Merchant, and accordingly, will cease to be an OptBlue Program Merchant; instead, you will accept Amex Cards under, and be bound by, a Card Acceptance Agreement between you and American Express. In addition, American Express will provide you with a "Welcome Kit" containing the current Card Acceptance Agreement and any additional information it believes necessary to communicate to you about your direct Card acceptance relationship.

Discover Network

Discover markets and supports a full range of credit, debit and prepaid products, as well as consumer lending products. Cards bearing the Discover brand are issued by Discover Network or third party issuers. In addition, certain card brands, including Diners Club International ®, Japan Credit Bureau ® (JCB), and China Union Pay ® (CUP) are supported by Discover Network and can be accepted by Clearent merchants.

MasterCard

MasterCard is a technology company that operates a global payment processing network, connecting consumers, financial institutions, merchants, governments and businesses. Payment cards bearing the MasterCard brand are issued by financial institutions that operate under the MasterCard Rules.

Visa

Visa is a global payments technology company that connects consumers, businesses, financial institutions, and governments in more than 200 countries and territories to fast, secure and reliable electronic payments. Visa is not a bank and does not issue cards, extend credit or set rates and fees for consumers; payment cards bearing the Visa brand are issued by financial institutions that operate under the Visa International Operating Regulations.

Payment Cards

The payment card presented by a customer at the merchant's location may be a credit card, which means that the issuer has established a line of credit from which the customer may draw; or a debit card, which is tied to the amount of money actually on deposit for the customer, or a commercial card, which is used for business credit charges.

In most cases, the processing for these types of cards is similar. The issuer contracts with its cardholders for repayment of the transaction amount.

Merchant

Meanwhile, you or your business has opened a payment card transaction deposit account with your bank, and your business has been approved by Clearent for card acceptance. You are an authorized acceptor of cards for the payment of goods and services. Now you're ready for that first payment card customer.

Interchange and Wholesale Pricing

Interchange is a rate applied to each card transaction by Visa, MasterCard, and the Discover Network. These organizations set their rates according to transaction types and operating procedures in order to compensate for the risk and expenses involved in processing a transaction.

Under the American Express OptBlue program, Wholesale Pricing is applied to American Express Card transactions, according to the merchant's industry type and the dollar amount of each transaction, in order to compensate for the risk and expenses involved in processing American Express transactions.

Qualifying at the Best Rate

Card brand feesvary in amount based on numerous factors including industry type, transaction amount, whether the transaction was authorized at the time of the sale, and the timeliness of remitting a sale for payment. There are several rates that may apply to your transactions, depending on your method of processing each transaction. When setting rate qualification criteria, the governing card brand may consider the card product used in the transaction, how the transaction data is entered into the terminal, and the time of settlement versus the time of authorization.

Card Present Qualifying Requirements

- Card is present, full magnetic stripe is read by terminal, and signature is obtained
- One electronic authorization is made per transaction and the transaction date is equal to the authorization date
- Authorization transaction amount must match settled transaction amount (excluding restaurants)
- Additional data is required in the settled transaction on all commercial cards
- Transaction batch must be transmitted no later than one day from transaction date

Mail Order/Telephone Order/Internet Qualifying Requirements

- One electronic authorization request is made per transaction and the transaction date is equal to the shipping date
- For Internet transactions, the authorization request message must include the Address Verification Service (AVS) response
- Transaction/shipping date must be within seven calendar days of the authorization date
- Settled transaction amount must equal authorized amount
- Additional data is required for commercial card transactions
- Transaction batch must be transmitted on or one day after transaction/shipping date

Lodging & Car Rental Qualifying Requirement

- Incremental electronic authorization requests are permitted
- Settled transaction amount must be within 15% of the total authorized amount
- Transaction date must equal the hotel check out/car rental return date
- Anticipated duration of stay/car rental must be included in authorization
- All transactions must include the folio number/rental agreement number

- Transaction batch transmitted no later than one day from the hotel check out/car rental return date
- **Note:** Transaction requirements vary by industry. Please contact your Account Executive for specific requirements pertaining to your industry.

How the Transaction Process Works

Any payment card transaction ultimately begins and ends with the cardholder.

The cardholder presents the card as payment for goods or services, either at the point of sale (POS), or via telephone, mail, fax or over the Internet.

Authorization and Electronic Ticket Capture

Once the electronic capturing of or obtainment of the data from the card takes place, an electronic imprint of the card number, expiration date, and counterfeit detection value are passed to the processor for authorization.

The processor then electronically routes the electronic data from the card to the card issuer.

The card issuer checks the cardholder's account status, and the requested authorization amount is compared to the cardholder's available spending limit and reviewed with fraud protection tools.

If the card is approved, the issuer posts the approved amount against the cardholder's credit line and the card issuer provides the authorization approval.

At this point, the authorization response is returned by the card issuer to the merchant and routed through the processor.

Funding

The process of moving the funds from the cardholder's account to the merchant's account is called funding. During funding, the issuing bank credits the merchant's account with the amount of the transaction.

The merchant deposits the transaction receipt with the merchant's bank.

The draft is routed to the cardholder's issuing bank, which debits the cardholder's account and sends the cardholder's monthly statement for payment.

Settlement

The process of moving the transaction information from your business to the cardholder's financial institution is called settlement. Each of the major card brands maintains its own authorization and settlement networks for payment card processing, and charge fees for their use.

Remember that your deposit account is not just for deposits! Clearent will subtract each month's accumulated fees from your deposit account.

Occasionally, a cardholder will have a question about a sales draft that has already been deposited in your account. In that case, Clearent may debit your account for the amount of the sale until the customer's question is resolved. This is called a chargeback and is described in more detail later in this guide.

Month-End Settlement Adjustments

Clearent normally debits month-end fees from your deposit account during the first week of every month. One way to ensure that sufficient funds exist in your bank account to cover chargebacks or reversals and fees is by keeping an amount equal to your average monthly discount range on deposit in your account. When planning for the possibility of chargebacks, a good rule of thumb is to keep at least twice your average ticket amount in your account.

Retention of Sales Drafts

In order to properly address chargeback issues, merchants must retain signed copies of sales drafts bearing cardholder signatures to address cardholder inquiries and requests for copies. Clearent requires retention for 36 months of your payment card transactions. Retention of the original draft, or a legible copy, can be stored for 36 months from the date you were paid for the transaction.

Stored sales drafts and other transaction data should be safeguarded with limited access. Merchants must keep all systems and media containing cardholder, account, or transaction information (whether physical or electronic) in a restricted, secure manner so as to prevent access by or disclosure to any unauthorized party. At the end of the 36 month retention period, transaction data such as sales drafts, reports, and other media with cardholder account data must be rendered unreadable prior to being discarded. If you have PC access to transaction information, then you must not dispose of the PC until information has been rendered unreadable or has been shredded.

You should always keep complete records for all credit card transactions for chargeback requests. Do not store sales drafts in alphabetical order by customer. The cardholder name is not part of the retrieval request record. We recommend using a storage system that is sorted chronologically by date, and then by cardholder account number.

Draft Retrieval Requests

Occasionally, the cardholder's issuing institution may require a copy of a sales draft for a billing question.

When a request is made for a sales draft from your records, we forward a retrieval request to you listing the following information:

- Cardholder's account number
- Reference number
- Dollar amount
- Date of the transaction

Forward a copy of the draft along with the request form to the appropriate processing center. To avoid chargebacks for a copy not received, you should always obtain a copy and mail or fax it to the requesting party within the specified time.

Respond to all retrieval requests within the number of days indicated or a chargeback may occur. You should give requests for draft copies top priority to avoid this type of chargeback.

Best Practices in Accepting Payment Cards

When you follow best practices in accepting credit and debit cards, it will help to assist you in treating all customers fairly and in honoring cards without discrimination. It will also help you to be vigilant about security.

To follow best practices:

Do

- Use a PCI compliant terminal or third party terminal provider service that truncates the card expiration date and all but the last four digits of the card number on the cardholder copy of the receipt; Store all materials containing cardholder account information in a restricted/secure area
- Limit access to sales drafts, reports, or other sources of cardholder data to your employees on a need to know basis
- Render materials containing cardholder account information unreadable prior to discarding
- Retain legal control over cardholder transaction data and personal cardholder information if you use a third party vendor
- Immediately notify Clearent of suspected or confirmed loss or theft of materials or records that contain account information retained by a merchant or its third party
- Immediately notify Clearent of the use of an agent or third party provider not identified on the Merchant Application
- Require your third party provider to adhere to PCI, DSR, CISP, DISC and SDP data security requirements
- Retain sales drafts for 36 months
- Display proper signage

Don't

- Process cash advance transactions unless you are a financial institution approved to do so through your merchant account
- Assign a minimum transaction amount over $10 for credit card transactions
- Assign a minimum transaction amount for debit card transactions (including PIN and Signature)
- Require a cardholder to complete a postcard or similar article that includes the cardholder's account number, card expiration date, signature or any other card account data in plain view when mailed
- Restrict payment card use for a sale or discounted item
- Use a payment card to guarantee a check
- List a cardholder's personal information on a payment card sales slip (unless the authorization operator requests it)
- Record CVV2/CVC2/CID (3-digit value code printed on the signature panel of card) on sales draft (only the one-digit result code can be recorded or retained)
- Retain sensitive cardholder data if expressly prohibited, including complete contents of a card's magnetic stripe (subsequent to the authorization)

- Sell, transfer, or disclose cardholder account information or personal information; (this information should be released only to Clearent or as specifically required by law; if you want to participate in a loyalty program, the loyalty vendor must be PCI compliant and implemented in accordance with processes and procedures)
- Deny a purchase because a cardholder refuses to provide additional identification such as telephone number, address, Social Security Number or driver's license number
- Use any other telephone number other than the official number provided for authorization of a transaction

You May Ask for Personal Information When...

- Store policy is to request it for all payment methods including checks and cash; you cannot make providing information a condition of the sale, unless local laws allow
- You need this information to deliver an order
- The authorization operator specifically requests you to obtain it
- The card is not signed and you must have the cardholder sign it and check the signature against another piece of identification

Never Honor a Payment Card When...

- The customer does not have the actual payment card
- The card appears to have been altered or tampered with
- Authorization is declined, or you're told to pickup the card
- The signatures do not match

Operating Guidelines

Although credit and debit cards offer one of the simplest, most risk-free forms of payment in existence today, there are some guidelines and precautions that you should consider to help prevent inaccurate or fraudulent transactions.

Draft Laundering or Factoring

Depositing drafts belonging to another business is in violation of your Clearent Merchant Agreement and is against the law in many states. "Helping out" another merchant who offers to pay you a fee or commission by depositing their payment card drafts in your account can be very dangerous and is strictly prohibited. The transactions are often questionable or even fraudulent. Schemes such as this are often referred to as "draft laundering" or "factoring" and typically result in a flood of chargebacks. It could cause automatic funds reversal from your bank account. Remember, the merchant who deposits another merchant's drafts is ultimately legally responsible for any problems resulting from the deposit.

We want to help protect you from this dangerous fraud scheme and the potentially devastating losses. Draft laundering will likely result in the termination of your card acceptance privileges. We urge you to educate your staff about this serious problem and report third party draft laundering propositions to Clearent and to the U.S. Secret Service immediately.

Charge Restrictions

Payment card brands no longer restrict assessing a minimum or maximum amount or adding a surcharge to credit card transactions (except where prohibited by state law). However, they may restrict assigning a surcharge amount on a debit or prepaid card transaction. A merchant should weigh the business impact (advantages and disadvantages) of assessing minimum or maximum amounts or assessing surcharges prior to implementing the practice. If assessing a minimum or maximum or assessing a surcharge, the cardholder must be informed by placing a sign in a visible location near the register and the cardholder must be given the opportunity to refuse the purchase. Surcharge amounts must show as a separate line item on the sales receipt.

Charge customers typically spend more than cash customers because of the available line of credit and the purchasing freedom credit cards represent. Encouraging patronage and not penalizing customers for paying with a credit card makes good business sense. If you feel strongly about compensating your cash customers for the fee you pay on charge purchases, you may want to consider offering a cash discount.

Adding a surcharge to credit transactions is against the law in California, Colorado, Connecticut, Florida, Kansas, Maine, Massachusetts, New York, Oklahoma and Texas.

For further requirements pertaining to surcharges, please visit the following links:

- http://usa.visa.com/merchants/merchant-support/merchant-surcharging.jsp
- http://www.mastercard.us/merchants/support/surcharge-rules.html

You may assign a minimum purchase amount on credit card transactions, but the minimum is not to exceed $10. Assigning minimum purchase amount on a debit card transaction, whether PIN or Signature, is strictly prohibited.

For further information pertaining to minimum transaction amounts please visit the following links:

- http://usa.visa.com/download/merchants/minimum-transactions-credit-card.pdf
- http://www.mastercard.com/us/merchant/support/minmax_trans_amts.html

Protecting Cardholder Privacy

Both customers and merchants often overlook the fact that the addition of personal or confidential cardholder information on the credit card draft can open the door to fraud or other criminal activity. Card Brand rules and regulations prohibit listing the cardholder's personal information on the credit card draft and require that the card expiration date be suppressed and the account number be truncated on the merchant and cardholder copies of electronically printed receipts.

Keep cardholder numbers and personal information confidential. This information should be released only to Clearent, as specifically required by law, or in response to a government request. Safeguard your customers by ensuring that you provide confidential cardholder information only to authorized sources. You must have written agreements with a provider supported by Clearent for loyalty programs or fraud control services.

You must not request or use account number information for any purpose the cardholder did not authorize or that may be fraudulent. If you accept other card types not described in this guide, you may release transaction information to them as required.

You must not sell, transfer, purchase, provide, exchange or in any manner disclose account number information or a cardholder's name or other personal information, even in the event of failure or other suspension of business operations. This prohibition applies to card imprints, transaction receipts, carbon copies, mailing lists, tapes or other media obtained as a result of a card transaction. The penalty for noncompliance can be up to U.S. $50,000.

If you use a third party terminal provider and they have access to cardholder account information, then your agreement with them must indicate that you retain legal control of the data. If information can be accessed over the Internet, then adequate controls must be adhered to and a third party security audit may be necessary. If cardholder transaction data or personal cardholder information is compromised, penalties for noncompliance will be assessed.

Never retain or store the:

- Complete contents of a card's magnetic stripe (subsequent to the authorization)
- CVV2, CVC2, or CID (American Express and Discover Network) card validation code numbers

Listing cardholder information, such as a phone number, driver's license or Social Security Number on the charge draft is unnecessary and discouraged. If you are suspicious that the transaction is not valid, do not hesitate to ask for additional identification – preferably a photo ID. If you must list the identifying data, write it elsewhere (such as your copy of the sales receipt) rather than on the charge draft where vulnerable account number information is printed. Thousands of dollars worth of damage can be done with only a few pieces of personal information. Keeping a cardholder's information confidential is a service that your customers will appreciate.

Proper Display of Signage

When you agree to accept payment cards at your place of business or website, you should display the proper signage to indicate that service is available, including at the point of sale. Use the sign and decals included in your merchant welcome kit.

Maintaining Data Security

As a condition of accepting payment cards, you must establish and maintain ongoing compliance with the applicable data security policies of each card brand. These include, but are not limited to, the following:

- American Express Data Security Requirements (DSR): Visit www.americanexpress.com/dsr for a copy of the Data Security Requirements you must follow in order to accept American Express Cards.
- Discover Information Security and Compliance (DISC): Information about this program is located at www.discovernetwork.com/merchants/data-security/disc.html.
- MasterCard Site Data Protection Program (SDP): Information about this program is located at www.mastercard.com/sdp.
- Visa Cardholder Information Security Program (CISP): Information about this program is located at www.visa.com/cisp.

Card Present Transactions

Electronic Ticket Capture (ETC) merchants use a terminal or other electronic device (e.g., cash register or PC) to authorize and settle their transactions. Using ETC is preferable to using paper drafts since an electronic record of your credit and debit card transactions is maintained throughout the business day.

The terminal can be used to validate your totals before settling with Clearent at the end of the day.

If you currently do not use Electronic Ticket Capture, contact Clearent for information on how you can improve your business with newer, more effective technology.

Completing an Electronic Transaction

It is very important to complete a transaction accurately and fully. The quality of the transaction is critical to your business's financial success and your customers' satisfaction.

There are six steps to complete an electronic transaction:

- Make sure the card is valid
- Swipe the card
- Compare account numbers
- Request authorization
- Print the sales draft
- Obtain and compare signatures

Determining Card Validity

Follow these steps to make sure the card is valid:

Discover Network Cards

Most standard, rectangular Discover Network Cards display the Discover Network Acceptance mark in the lower right corner of both sides of the Card, or through October 2008, the Discover/Novus Acceptance mark only on the back of the card. After October 2008, however, Discover Network Cards will only display the Discover Network Acceptance mark on both sides of the Card. The words "DISCOVER" or "DISCOVER NETWORK" appear in ultraviolet ink on the front of the card, which becomes visible when held under an ultraviolet light. Discover Network account numbers are sixteen (16) digits embossed in clear and uniform size and spacing, and where a hologram is present, the last four digits of the account number extended into the hologram. Cards issued before April 15, 2006 will display either a circular or rectangular three-dimensional hologram of a globe with an arrow through it. Newer Cards will have a holographic magnetic stripe, and the holographic globe art on the front of the Card will not be present. The embossed expiration date, if present, appears in a MM/YY format below the words "Valid Thru." An underprint of the word "VOID" becomes visible on the signature line of Discover Network Cards if erasure of the signature is attempted. Most standard, rectangular Discover Network Cards have the cardholder's name embossed on the front of the Card and a scripted "D" embossed beneath the account number on the front of the card on the same line as the embossed expiration date. Also, for most standard, rectangular Cards the account number or last four (4) digits of the account number appear in reverse indent printing on the signature panel and must match the last four (4) digits of the account number embossed on the front of the Card. Standard, rectangular plastic, stored valued Cards are not

required to bear the cardholder name, and for certain merchants, may not bear the globe pattern hologram or the Discover Network Acceptance Mark. Valid Cards will not always be rectangular in shape (e.g., Discover 2GO™ Cards). Discover Network may implement new Card designs and/or features. You are required to remain familiar with Discover Network Card designs and you may reference the document "Discover Network Security Features." You may download the document free of charge from Discover Network's website at http://www.discovernetwork.com/merchant/home/data/index.html.

Visa Cards

Embossed account number begins with 4. All digits must be clear, even, and the same size/shape. A three-dimensional dove hologram appears to move on the label as you rotate or tilt the card. The last raised card numbers appear on top of the hologram. Four-digit number must be printed directly below the embossed account number. This printed number should match exactly with the first four digits of the account number.

The signature panel should be white with the word "Visa" repeated in a diagonal pattern in blue and gold print. The words "Authorized Signature" and "Not Valid Unless Signed" must appear above, below, or beside the signature panel.

CVV2, the three-digit value code printed on the signature panel after the full or truncated account number helps mail order, telephone, and Internet order merchants validate that the customer has a Visa card and that the card account is legitimate.

MasterCard Cards

All MasterCard account numbers begin with either a 5 or a 2.

The embossing should be clear and uniform in size and spacing.

The MasterCard logo may appear on the front or the back of the card along with a hologram. Whether on the front or back of the card, a hologram with interlocking globes showing the continents should appear three-dimensional and move when the card is tilted. The word "MasterCard" will appear in the background of the hologram. The letters "MC" are micro-engraved around the two rings.

A four-digit number may be pre-printed on the card. It must match the first four digits of the embossed account number.

MasterCard cards have a stylized "MC" embossed on the line next to the valid dates.

The word "MasterCard" is printed in multi-colors at a 45 degree angle on a tamper-evident signature panel on the back of the card. All or a portion of the 16-digit account number is indent printed in reverse italics on the signature panel and is followed by a 3-digit card validation code (CVC2).

The card is not physically altered in any way.

The transaction falls between the effective date and the card's expiration date. If the current date is not within the specified range, do not accept the card.

Follow the terminal authorization procedures as described in your Quick Reference Guide.

American Express Cards

Procedures for accepting American Express Cards can be found in the Merchant Operating Guide, the latest copy of which can be found at:

www.americanexpress.com/merchantopguide

Swiping the Card

- Swipe the card to request the transaction authorization
- Hold the card through the entire transaction
- Avoid sliding the card back and forth
- Slide the card only once unless prompted to do otherwise by the device
- Press clear before sliding another card
- Use the manual or call the help desk if the system develops problems

Compare Account Numbers

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

Compare account numbers displayed on the terminal or printed on the sales draft to the embossed number on the customer's card. If the numbers match, enter the amount of the transaction into the terminal and request authorization. If the numbers do not match, call the authorization center and say, “Code l0.” Follow the instructions the operator gives over the telephone.

Available Fraud Controls

Most point-of-sale devices have the ability to perform fraud controls. This functionality will help in identifying potentially counterfeit credit cards, and assist in avoiding potential chargeback losses to your merchant account. If the controls are “on,” you will be prompted to input the last four digits of the card number after initially swiping the card. If there are no issues identified, the transaction will proceed as normal. If there is a possible problem, the point-of-sale device will display a “mismatch” message (see “Request Authorization” below). If you would like to know more about these controls, please contact your point-of-sale help desk.

Request Authorization

In the authorization process, the issuer approves or declines a transaction. In most cases, transactions are quickly processed electronically. However, to protect against fraud, the issuer may request information about the transaction.

Typically, the authorization process is quick and easy, taking just a few seconds. Ninety-five percent of all authorization requests are approved.

When requesting authorization, you may receive one of the following or similarly worded responses:

- Approved: This response means the issuer approves the transaction. If you have a terminal printer, the approval is noted automatically. If you do not have a terminal printer, write the authorization code clearly on the sales receipt.
- Declined or Card Not Accepted: Issuer does not approve the transaction. Do not process this transaction. Quietly inform the cardholder that the card has been declined. Ask if the cardholder

would prefer to use an alternative form of payment. Do not attempt to authorize for lower amounts.

- Call or Call Center, or Referral: This means that the issuer wants the associate to call. Call the Voice Authorization Center and follow the operator's instructions. Most of these transactions are authorized, and you may want to inform the cardholder this is to protect against fraud.
- Pickup: Means that the issuer wants the sales associate to keep the card. If you can, try to retain the card; however, never put yourself in any danger.
- Mismatch: When using the available fraud control features (see “Available Fraud Controls” above), if the 4 digits that were entered do not match the information imbedded on the magnetic stripe, this message appears. Start the transaction again, reentering the 4 digits as requested. If the message appears again, the card is potentially counterfeit or fraud. In this case, follow Code 10 procedures, and do not accept the card as a form of payment.

Obtaining an authorization does not guarantee against chargebacks.

Obtain and Compare Signatures

Have the cardholder sign the receipt. Compare the signatures on the card and the receipt. If the two match, return the card with the copy of the receipt. If they don't match ask for additional information, such as a driver's license or another credit card and call voice authorization center for instructions.

If there is no signature, ask for additional information. The card is not valid unless it is signed.

Retain a copy of the sales receipt for your records and for protection against possible disputes.

Accepting Debit and EBT Cards

In order to accept debit and/or EBT cards, you must first sign an agreement with Clearent and abide by the policies and regulations in the agreement.

Debit cards are becoming the most popular form of non-cash payment. There are two types of debit transactions – online and offline.

Online debit or PIN-secured transactions require customers to enter a secret PIN at the point-of-sale terminal and the amount of the transaction is debited from the customer's checking account.

Offline debit transactions or (signature-authorized transactions) do not require customers to enter a secret PIN, but instead sign a receipt authorizing their financial institution to debit their account for the amount of the transaction. This type of transaction can be made with an ATM/debit card bearing a PULSE, Discover Network, MasterCard, or Visa logo on the front.

When you offer debit as a form of payment, you are supplied a number of debit network logos, which are to be displayed at terminal locations and storefront doors or windows, and are to be of a size no smaller than the logo of any of the other card types accepted.

As a debit merchant, you are required to follow certain other procedures, in order to offer debit as a payment option, and they are listed below:

- The merchant is required to honor all valid debit network cards with terms no less favorable than the terms under which the merchant accepts other card types.
- The merchant must not set minimum or maximum transaction amounts for debit card transactions, or a minimum amount as a condition for accepting the card.
- For PIN-based transactions, the payment terminal shall be equipped with a Personal Identification Number (PIN) entry device for use by cardholders to enter their PINs.
- The PIN entry device must be at or in close proximity to the point-of-sale device.
- The point-of-sale device must be capable of reading the entire Track II from the cardholder's card.
- The merchant may not require or request a cardholder signature. The cardholder's PIN is their electronic signature.
- The merchant may not ask the cardholder to disclose their Personal Identification Number.
- The receipt for debit transactions are to be produced by a receipt printer and be made available to the cardholder at the time the transaction is completed.
- The merchant copies of debit card transaction records are to be retained for a period of 36 months.
- With an offline debit transaction, always compare the signature on the back of the card with that of the receipt.
- Do not provide cash back during an offline transaction.

EBT Processing

Clearent supports Electronic Benefits Transfer (EBT) processing because we recognize the value to merchants and their customers. Accepting an EBT card at the point of sale is similar to accepting other electronic payment card types. EBT transactions are PIN-based, just like debit cards.

An EBT card is a magnetic-striped plastic card that electronically delivers federal and state funded food stamps and cash benefits to qualified EBT recipients.

An EBT card electronically replaces paper food stamps and unemployment insurance checks, as well as other cash benefits so it eliminates paper processing of food stamps, making it more efficient. It is of similar size and appearance as other types of payment cards, so that the user does not feel awkward using it.

Card Not Present Transactions

Card Not Present transactions are those that occur when there is no face-to-face contact with the cardholder. These transactions typically include purchases made:

- By Mail (also referred to as Mail Order/MO/TO)
- By Telephone (also referred to as Telephone Order/MO/TO)
- By Fax
- Over the Internet (also referred to as eCommerce)

You cannot accept Card Not Present transactions unless Clearent has agreed to process these for you and such provision is contained in your Clearent Merchant Agreement.

Take precautions to guard against data compromise when taking orders over the Internet, by telephone, mail or fax.

Since a visual identification cannot be made for cardholders requesting fax, mail, phone or Internet card transactions, some personal information must be obtained in order to receive authorization from Clearent.

When processing fax, telephone, mail or Electronic Commerce/Internet transactions, you should always remain aware of the increased risk of fraud because the cardholder is not present. (See the "Working Together to Prevent Fraud" section for additional information.)

Two security tools are available today to assist you in the detection and prevention of fraudulent activity – verification of cardholder billing address (AVS) and authentication that the customer has the card in their possession (CVV2/CVC2/CID).

Address Verification Service (AVS) is an automated program that allows a merchant to check a cardholder's billing address as part of the electronic authorization process. Fraudsters often do not know the correct billing address for the cards they are using, thereby yielding a clue that the transaction may not be valid.

Card authentication is termed Card Verification Value 2(CVV2/CVC2) to distinguish it from CVV1/CVC1/CVV encoded on the card's magnetic stripe, and is a three-digit code number imprinted on the signature panel of payment cards to help authenticate that the customer has a genuine card in their possession. Discover cards also have the three-digit code, called CID, printed on the signature panel.

American Express has a four-digit code printed on the front of the card. American Express implements merchants for four-digit CID authentication on a case-by-case basis.

Merchants who submit the CVV2/CVC2/CID code as a part of their authorization request can reduce fraud-related chargebacks.

Also, the Payment Card Industry Data Security Standards (PCI-DSS) provides a list of Best Practices and other tips. The following twelve controls help you to remain in compliance with your card acceptance agreements when accepting payments over the Internet.

Follow these guidelines:

1. Install and maintain a working network firewall.
2. Keep security patches current.
3. Encrypt stored data.
4. Encrypt data sent via open networks.

5. Always use updated anti-virus software.
6. Restrict access to data to a “need to know” basis.
7. Assign a unique ID to each user.
8. Track access to the data by that unique ID.
9. Never use vendor-supplied defaults as passwords or other security features.
10. Test the security system and processes regularly.
11. Maintain a security policy for employees and contractors.
12. Restrict physical access to cardholder information.

Electronic Commerce Transactions

The Internet has rapidly become an alternative-shopping destination for consumers and businesses.

Offering services via the Internet presents unique opportunities for merchants to expand their businesses. At the same time, your customers want to feel safe and secure while conducting Internet transactions. Clearent is aware of the growing popularity of web-based business and has developed flexible, secure Internet payment processing options that help you and your customers feel at ease.

An electronic commerce transaction is a transaction conducted over the Internet or other network using a cardholder access device, such as a personal computer or terminal. This definition relates to the interaction between the cardholder and the merchant. It is not concerned with how the merchant processes the transaction after the account information is received.

Merchant transactions must properly identify electronic commerce transactions in both authorization and settlement data. Failure to comply may result in fines and penalties. The accuracy of this information is essential as it may have an impact on interchange qualification and pricing.

Merchant Website and Electronic Transaction Requirements

A merchant's website must contain the following information:

- Your merchant outlet address
- Your merchant outlet country and country of domicile must be disclosed prior to the cardholder accessing payment instructions
- Complete description of the goods or services offered
- Merchandise return and refund policy clearly displayed on either the checkout screen, or on a separate screen that allows the purchaser to click an acceptance button
- Your consumer data privacy policy and method of transaction security used during the ordering and payment process
- Customer service contact including electronic mail and/or telephone number
- Transaction currency (e.g., U.S. dollars, Canadian dollars)
- Export or legal restrictions (if known)
- Delivery policy
- Card acceptance brand marks in full color

In addition, a Transaction Receipt must include:

- Merchant name most recognizable to consumers, meaning your “doing business as” (DBA) name as used on your website
- Merchant Universal Resource Locator (URL)

- Merchant name used in the Clearing Record
- Customer service contact, including telephone number; (if you deliver goods internationally, include both local and internationally accessible numbers)
- Properly disclosed terms and conditions of the sale, if restricted
- Exact date that free trial period ends, if offered
- Properly disclosed cancellation policies
- A complete and accurate description of the goods or services offered
- Merchant online address
- Description of merchandise/services
- Transaction amount
- Transaction date
- Transaction type (purchase or credit)
- Purchaser name
- Authorization code
- Unique transaction identification number
- Terms and conditions of sale, if restricted
- Return/refund policy (if restricted)

You may access the American Express Data Security Requirements (DSR) at www.americanexpress.com/dsr, Discover Network DISC program at www.discovernetwork.com, Visa Cardholder Information Security Program at www.visa.com/cisp or the MasterCard Site Data Protection Program at www.mastercardmerchant.com for additional information on securing cardholder data.

Completing Mail and Telephone Order Transactions

1. Obtain the cardholder's name, card account number, and expiration date and record these on your sales draft. You must also obtain the cardholder's billing address and Zip code. (You may need to provide this information when you request authorization.)
2. Request the three-digit card authentication number (CVV2/CVC2/CID) from the signature panel (or the four-digit number if approved for American Express CID participation). Note: Merchant retention of this authentication number is strictly prohibited. However, you may record and retain the one-character result code.
3. Fill in a brief description of the goods sold and show the amount of the sale in the space marked “Total.”
4. Write TO (telephone order) or MO (mail order) on the signature line of the sales draft.
5. Enter transaction information into terminal or PC. Refer to your Quick Reference Guide for instructions on manually entering sales transactions.
6. Provide a copy of the sales draft to the cardholder, either with the cardholder order (if being shipped to the cardholder) or separately (i.e., if purchase is a gift). The transaction date is the date goods were shipped to the cardholder. Electronically printed sales receipts provided to the cardholder should truncate or mask the account number and the expiration date.

An authorization for a phone order, mail order, fax or Internet transaction does not guarantee against chargebacks. Please ship only to the address verified as the cardholder's address. Shipment to a different address jeopardizes your protection from chargebacks. You may verify the billing

address of the cardholder with the Authorization Center or the cardholder's bank. The Customer Support team can provide you with the number of the cardholder's bank if necessary.

Lodging Merchants Best Practices

Because of the nature of the lodging market, and the Travel and Entertainment (T&E) industry, lodging merchants require special authorization and transaction procedures when accepting credit and debit cards for reservation deposits and payment for accommodations and services.

Clearent has provided both best practices and requirements that can be found in the exhibit section.

Key Dates for Lodging Merchants:

- Check-In Date
- Initial Authorization date
  - Must be after “valid from” date on card
  - Must be prior to “expiration date” on card
- Checkout Date
  - Transaction Date on the transaction receipt and other documents

Delayed or Amended Charges

If the cardholder has consented to be liable for delayed or amended charges (i.e., costs for room, food, or beverage charges), they must be processed to the cardholder's account within 90 calendar days of checkout date. This must not include charges for loss, theft, or damage.

Complete the transaction and include the words “Signature on File” on the signature line. Send the cardholder a copy of any amended or additional charges added to a Transaction Receipt within 5 days of entering the charge. Send to the address shown on the folio.

Completing Recurring Bill Payment Transactions

If you have been approved by Clearent for Recurring Bill Payment services, you must follow these procedures, those set out in the Mail Order/Telephone Order section above, and any written directions issued by Clearent relating to mail order, telephone order, and recurring bill payment services.

What is a "Recurring Payment?"

A recurring payment is an arrangement in which a consumer preauthorizes a merchant to bill the consumer's credit card account at predetermined or variable intervals (i.e., monthly, quarterly, annually). The amount can be the same each time (such as monthly fees for memberships, Internet service providers, or insurance premiums) or can fluctuate from one payment to another based on usage (such as phone service or utility bills). Other recurring payments may occur for newspaper subscriptions, cable TV service, cleaning service, lawn service, etc.

How is a "Recurring Payment" different from other forms of payment?

A recurring payment agreement differs from other forms of payment because it is initiated only when the cardholder establishes an ongoing card payment relationship with a merchant. The cardholder is free to continue the arrangement for a finite period of time or until one or both parties cancel the recurring payment arrangement.

A recurring services merchant must obtain a completed Order Form from the cardholder containing a written request for the goods or services to be charged to the cardholder's account.

An Order Form is a document bearing the cardholder's signature, either written or electronic, authorizing goods or services to be periodically charged to his/her account for recurring services. An Order Form may be any of the following:

- Mail order form
- Recurring transaction form
- Preauthorized healthcare transaction form
- E-mail or other electronic record that meets the requirements of applicable law

What should be on an Order Form?

The Order Form must include, but is not limited to, the following:

- Transaction amount, unless the recurring transactions are for varying amounts
- Frequency of the recurring charges
- Duration of time for which cardholder permission is granted

Retain the Order Form for the duration of the recurring services (plus an additional 36 months to substantiate any requests for copy). Provide a copy in the event of a retrieval request. Provide a subsequent Order Form when a recurring transaction is renewed.

Are There Other Requirements or Prohibitions for Recurring Transactions?

- Partial payment for goods or services purchased in a single transaction is NOT allowed.
- Finance charges are not permitted on a recurring transaction.
- A recurring transaction CANNOT be deposited if the cardholder has cancelled the payment arrangement.
- A recurring transaction CANNOT be deposited if an authorization request receives a negative response. (Forced depositing of declined authorization requests is PROHIBITED.)
- The account number may not be used for any purpose other than for a recurring payment.
- An authorization approval code may only be used once.
- The floor limit for recurring bill payments is $0.
- You must always obtain an authorization and identify recurring bill payments in the authorization request.
- Only deposit authorized recurring bill payment transactions.
- Identify recurring bill payment transactions the clearing.
- The clearing record for recurring transactions must contain merchant contact information in the merchant name or city field to enable the cardholder to contact the merchant directly.
- Transaction receipt for recurring electronic commerce transactions must include the frequency and duration of the recurring transactions as agreed to by the cardholder on the transaction receipt.
- "Recurring Transaction" must be written on the signature line of the transaction receipt.

Because recurring payment transactions occur without face-to-face contact with the cardholder, the merchant assumes additional risk in processing these transactions. Remember, obtaining an authorization does not guarantee against chargebacks.

Returns and Exchanges

Returns and exchanges can be used for the return of merchandise for credit only. NO CASH OR CHECK REFUNDS are permitted on a credit card purchase.

Any conditions or requirements that limit the cardholder's ability to return merchandise, i.e., special sale event, etc., must be clearly stated in bold print in letters .25 inches high near the cardholder signature on the sales draft or on the order form if for mail order. In-store signs are not sufficient to establish that the cardholder is aware and accepts the special conditions/or restrictions.

Follow these steps to process a return or an exchange transaction:

Credit Card Refunds

1. Ask the cardholder for the card used in the original transaction, and compare the account number on that card with the account number on the copy of original sales draft. They must be identical.
2. If the cardholder does not have the card used for the original purchase, use the information on the original sales draft to record the card number, customer name, and expiration date on the credit draft.
3. If you are using a printer, follow terminal procedures for processing a credit located on your Quick Reference Guide.
4. If you are not using a printer, place the credit draft on the imprinter and imprint the merchant identification plate (and payment card, if available). Be sure that the imprinted information is legible on ALL copies. If not, write the complete information above (not over) the imprinted information.

If the exchange is for merchandise of lesser or greater value, you must prepare a credit draft for the total amount of the return. Then prepare a sales draft for the new purchase. Authorization procedures must be followed to complete a new purchase.

Debit Card Refunds

1. Ask the cardholder for the card used in the original transaction, and compare the account number on that card with the account number on the copy of the original sales draft. They must be identical.
2. If you are using a printer, follow terminal procedures for processing a credit, located in your Quick Reference Guide.
3. If you are not using a printer, place the credit draft on the imprinter and imprint the merchant identification plate (and payment card, if available). Be sure that the imprinted information is legible on ALL copies. If not, write the complete information above (not over) the imprinted information.

Returns and exchanges made with debit cards should be handled at the merchant's discretion – either cash refund or refund to the cardholder's account.

All other returns or exchanges incurring chargebacks and adjustments should follow existing guidelines.

Best Practices for Merchant Use of Convenience Fees

A convenience fee is a charge in addition to the original transaction amount for the convenience of using a payment method outside of the merchant's customary payment channel, such as a merchant who generally accepts credit card payments in person at the time of the sale or service, but is allowing payment to be made by mail, telephone, or Internet as a convenience to their customer. American Express, Discover Network, MasterCard, and Visa all allow for convenience fees. Rules and regulations pertaining to convenience fees vary by card brand, which can complicate a merchant's practice of assessing convenience fees.

Discover Network does not have its own specific requirements for convenience fee assessment. Discover will allow convenience fees so long as it is applied in like manner across all card brands.

MasterCard restricts convenience fees to only Government and Higher Education entities. Assessing convenience fees to all other merchant entities is prohibited.

- The merchant must be one of the following Government and Educational Institution categories or their third party agents
    - Elementary and secondary schools for tuition and related fees, and school-maintained room and board
    - College, universities, professional schools or junior colleges for tuition and related fees, and school-maintained room and board
    - Local, state, and federal courts of law that administer and process court fines, alimony, and child support payments.
    - Government entities that administer and process local, state, and federal fines
    - Local, state, and federal entities that engage in financial administration and taxation
    - Government Services; merchant that provides general support services for the government.
- The fee
    - Can be flat rate, a variable, or a fixed percentage rate of the amount owed
    - Can be assessed on Card Present and Card Not Present transactions
    - Cannot be assessed on PIN Based Debit transactions
    - Assessment to Debit and Commercial Debit can be different than fees assessed for consumer and commercial credit transactions providing that the fee for the consumer and commercial credit are the same.
- Must clearly disclose the amount of the convenience fee to the customer
- Customer must be given the opportunity to cancel prior to completion of the transaction
- The convenience fee cannot discriminate against the brand relative to the other payment cards.

Visa allows for convenience fees to be assessed to any merchant who is charging the fee for allowing use of an alternative payment channel outside their customary payment channel.

- The fee is charged for a bonafide convenience of using an alternative payment channel (i.e., IVR or Internet) outside the merchant's normal business practice
- The fee:

    - Must be disclosed as a charge for alternative payment channel convenience and not a fee that is being charged to recoup processing fees
    - Is applied only to a non-face-to-face transaction
    - Must be a flat or fixed amount regardless of the amount of payment due
    - Is included as part of the total transaction amount
    - Cannot be added to recurring transactions
    - Cannot be added to Utility (MCC 4900) payment transactions
    - Is assessed by the merchant providing the goods and services to the cardholder and not by a third party
- The customer must be given the opportunity to cancel prior to completion of the transaction

Visa Government and Higher Education merchants may assess convenience fees within their customary payment channels and must meet the following requirements:

- The merchant must be assigned one of the following MCC's
    - 9311 – Tax
    - 9222 – Fines
    - 9399 – Misc. Government
    - 8220 – College Tuition
    - 8244 – Business School
    - 8249 – Trade School
- Merchant registration is required with Visa
- The fee:
    - Merchant must clearly disclose the amount of the convenience fee to the customer
    - Must be a flat or fixed amount regardless of payment due
    - Can be assessed on Card Present and Card Not Present transactions
    - Must be processed as a separate transaction
    - Must be labeled as a "Service Fee," not a "Convenience Fee" or "Surcharge Fee"
- Customer must be given the opportunity to cancel prior to completion of the transaction

Discounts on cash purchases are also permitted.

American Express regulations governing convenience fees are described in the Merchant Operating Guide, a current copy of which can be found at www.americanexpress.com/merchantopguide.

Also, surcharging is different from a situation in which particular business cases (i.e., governments or schools) may warrant imposition of a convenience fee for utilization of specific alternative payment modes, such as Internet and telephone.

A merchant should weigh the business impact (advantages and disadvantages) of assessing convenience fees prior to implementing the process.

In the normal course of business, the card brands do not set requirements on other merchant fees that are uniformly applied to all payment types, such as shipping and handling fees or student registration fees, since they do not discriminate or limit card acceptance. However, some merchants, such as ticket sellers and travel agents, may charge consumers for costs associated with the value-added services they provide and the merchant name and other transaction data must indicate the merchant of record.

Businesses that facilitate credit card payments for other merchants are subject to additional requirements and require registration.

The requirement for an alternate payment channel means that MOTO and electronic commerce merchants whose payment channels are exclusively non face-to-face may NOT impose a Convenience Fee. A merchant who accepts face-to-face payments is not required to accept cards through this payment channel to meet the above requirement.

Chargebacks

A chargeback is a previous transaction that is being disputed by the cardholder or their issuer. A chargeback occurs when a cardholder disputes a charge or when proper payment card acceptance and authorization procedures were not followed. If you receive a chargeback, your deposit account is debited for the indicated amount. In addition to the chargeback, you may incur a $50.00 fee if you failed to follow card acceptance and authorization procedures. Reasons for chargebacks include a cardholder dispute or an error in handling on the part of a merchant's staff. Chargebacks are rare if proper authorizations and processing procedures are followed.

Some Do's and Don'ts of Chargebacks

You can significantly reduce the chance of receiving a chargeback notification by taking the following precautions:

- Do not charge a cardholder before shipping the merchandise
- Do not accept sales that are declined, and if a sale is declined, do not attempt authorization a second time on a declined sale
- Do not accept sales that are not authorized for the exact amount
- Do not accept an expired card
- Do not accept a card before the effective date on a dual dated card
- Do not process a credit as a sale
- Do not participate in a suspicious transaction
- Do not obtain an authorization by using multiple transaction/split sales drafts
- Do not accept a card where the account number obtained off the magnetic stripe does not match the account number on the draft
- Do understand that you assume all responsibility for the identity of the cardholder for all fax, Internet, mail order and telephone order sales
- Do prepare and submit a written rebuttal within the time specified on the chargeback notification
- Do accept cards where the cardholder account number is valid
- Do authorize all sales
- Do charge the cardholder for the correct amount
- Do credit the cardholder for the returned merchandise
- Do credit the cardholder for a canceled order
- Do verify that the signature on the sales receipt matches the signature on the card
- Do verify the authorization code

Chargeback Fees:

Each of the major card brands have established additional fees for items that result in a chargeback. You may be subject to these Chargeback Fees if you failed to follow card acceptance and authorization procedures and the card issuer has a valid chargeback.

Your Right to a Rebuttal

If you receive notification of a chargeback, you have the right to request a rebuttal. A rebuttal is a merchant's written reply to a chargeback that provides documentation proving that the sale was valid and that proper merchant procedures were followed. Rebuttals must be completed within the number of days indicated on the chargeback notification. Contact Clearent Customer Support for more information on rebuttal procedures.

Terminated Merchant File

Clearent has the right to place you in the Terminated Merchant File if your agreement has been terminated for one of the following reasons:

- You were convicted of credit or debit card fraud
- You have deposited excessive counterfeit transactions
- You have deposited excessive transactions unauthorized by cardholders
- You have deposited transaction receipts representing the sale of goods or services generated by another merchant (laundering)
- Clearent has received an excessive number of chargebacks due to the merchant’s business practices or procedures

Only the acquirer that has placed you on the Terminated Merchant File may request your deletion from the file.

Understanding Your Statement

The following section provides instruction and contact information to help you better understand the monthly statement you will receive.

Questions Regarding Your Statement

If you think your statement is incorrect, or if you need more information about a transaction on your statement, please contact us via letter. We must hear from you no later than 60 days after the first bill, on which the error or problem appeared, was sent.

In your letter, please provide the following information to insure a prompt and accurate response:

- Your Clearent merchant number and business name
- Your name
- A telephone number where you can be contacted
- The amount of suspected error
- Describe the error and explain, if you can, why you believe there is an error; if you need more information, describe the item in question

Please note that chargebacks require a response with appropriate rebuttal information within 10 days from the date your account has been debited. Chargebacks are not considered a “billing error.”

Working Together to Prevent Fraud

We take your business seriously. As your partner, Clearent utilizes a sophisticated fraud detection system that monitors all card transactions in real time, 24 hours a day, seven days a week. This fraud detection system is one way Clearent protects your business.

Reading and complying with the standards and the policies in this guide will be your best defense against fraud and help you remain in compliance with your Merchant Agreement.

While it is not always possible to prevent fraud from happening, education and awareness are the best ways to avoid it.

This information is provided to make you aware of the many ways that fraudulent activity occurs, what to watch for, and the things you and your employees can do to protect your business.

Our commitment to providing security for credit transactions helps both you and your customers feel safe about using payment cards; however, there are precautions that can significantly decrease the probability of fraud or another credit-related crime from occurring.

Prohibited Transactions

Merchants who accept credit cards must be aware of prohibited transactions and the penalties that can be imposed if a prohibited transaction is completed. A prohibited transaction is one that does not comply with the operating regulations of the card brand under which the card was issued, and/or policies and procedures as defined in the Merchant Agreement. If deposited, sale drafts involving prohibited transactions will be subject to chargeback and may lead to termination of the Clearent Merchant Agreement, perhaps immediately!

The following are examples of prohibited transactions:

- Processing transactions to cover previously incurred debts or bad debt such as bounced checks, or payment for returned merchandise
- Processing credit (refund) transactions without a preceding debit transaction
- Disbursing funds in the form of travelers cheques, if the sole purpose is to allow the cardholder to make cash purchase of goods or services from your establishment
- Acceptance of a Visa Card or Visa Electron Card for the purchase of a scrip
- Accepting a Visa TravelMoney Card or Visa Electron Card for a Manual Cash Disbursement
- Processing a sale on a previously charged back transaction
- Accepting transactions that are declined by the Authorization Center
- Attempting multiple authorization requests following a decline
- Accepting cards with an invalid effective date
- Accepting expired cards
- Using a split sale to avoid authorization requirements
- Giving cash to the cardholder
- Delivering goods or performing services after notice of a cancellation by the cardholder of a pre-authorized order
- Billing card after notice of cancellation of recurring payment

- Accepting transactions where the signature on the payment card and the one on the sales receipt are not the same
- Engaging in factoring (draft laundering) or accepting or depositing drafts from other banks, merchants or businesses which you may own or purchase, but are not explicitly listed in your current application (or supplements to it) currently on file with us
- Laundering of deposit drafts will likely result in the immediate termination of your payment card privileges

Educate your staff about prohibited transactions to reduce the risk of accepting counterfeit or fraudulent card transactions. A fraudulent transaction could involve an invalid account number, or a valid number with unauthorized use.

Unauthorized use of a lost or stolen card is one of the greatest contributors to fraud losses.

In the case of stolen cards, fraud normally occurs within hours of the loss or theft – before most victims have called to report the loss. Checking the signature becomes very important in these first few hours of loss. Also, keep in mind that the thief may have altered the signature panel or re-embossed the card to change the account number slightly.

Card Not Present Scams

The risk of fraud increases greatly if your customer and their credit card are not present at the time a purchase is made because you don't have the opportunity to inspect the card.

“Card Not Present” transactions typically occur over the telephone or fax, through the mail or over the Internet.

Without the card in hand, you are unable to inspect the card, check for suspicious markings or verify the customer's signature. As a merchant, you put yourself and your company at greater risk by accepting Card Not Present transactions without the proper Merchant Agreement in place to protect you in a fraudulent situation.

If you are processing card transactions by telephone, mail, fax or Internet, make sure that you have signed the specific Merchant Agreement required to perform these transactions where the card is not present. Even after you have the proper agreement in place, it is crucial that you take the precautionary steps to prevent potential chargebacks.

Skimming

In many instances, thieves are reaping the benefits of our rapidly growing world of technology. One example of skimming is when the fraudster uses a device to read the data on the magnetic stripe of a credit card, a process known as “skimming.” Other times the information is received by tapping into phone lines. Regardless of the method used, skimming is responsible for millions of dollars of losses.

Be on the lookout for devices used to swipe credit cards. They are usually box-shaped cordless devices and fit in the palm of your hand, although laptop computers have been used to accomplish the same thing.

Don't Be Bullied

A customer may attempt to intimidate the cashier by causing a fuss at the register so that the purchase is rushed, which may lead to improper check out. They may tell you that the card won't read and not to bother running it through so that you'll have to key it in manually. In such instances,

customers have also been known to complain about the service or length of the line. They may even demand to see a manager, anything to keep the cashier's attention off the authorization of the credit card.

By creating a tense atmosphere, the cashier is often prone to rush the person through the process just to get the customer out of the store. This is when criminal activity takes place. The result is usually a costly chargeback for the merchant.

Use only the authorization numbers provided by Clearent. Never call a telephone number given by the cardholder for authorization.

Don't be intimidated by these bullies; always take your time and make sure the correct procedure is followed when authorizing the card. You may not be losing a sale by making the impatient customer wait – you may be saving your company the cost of a chargeback later.

Deceptive Deliveries

An easy way to spot a situation that may be fraudulent is to look at the delivery address. Often thieves will have a package delivered to an address that is not permanent or requires the package to be left at a front desk. Look carefully at orders that require deliveries to office complexes, hotel lobbies, or post office boxes, as they are almost impossible to trace if the transaction is questioned. In this situation, it is best to call the customer and ask for a permanent address.

The Manual Key-In

Often fraud occurs when the thief damages the card on purpose so that you are forced to manually enter the number in the electronic point-of-sale terminal. Fraudulent cards are often damaged in order to bypass the antifraud features that are placed on them – the magnetic stripe cannot be swiped and transmitted to the verification center for authorization in the case of a manual key-in.

If you have an electronic point-of-sale terminal, swipe every card that you come across, no matter how damaged or worn.

And be wary of customers who let you know right away that their card won't read. If the card doesn't work and you end up keying in the number, make sure you take an imprint of the card. If the card is severely damaged, simply ask for another form of payment.

Borrowed Cards

Beware of people waving letters of authorization for use of a credit card. Under no circumstances are these letters an acceptable form of verification or authorization. Don't fall for children borrowing their parent's card either. Friends, coworkers, and spouses are not permitted to borrow each other's cards. The only person who should be presenting the card to you is the person whose name is on the front of the card and signature on the back of the card. Most often, the rightful owner gets the statement and a chargeback inevitably occurs.

One Person's Trash Is Another's Gold Mine

The garbage is probably the last place you would think to protect. Thieves look in your trash for credit card slips, banking information, warranty information, credit applications or returned slips – anything that has personal information such as a name, address, or phone number.

Your “trash” could be a thief's treasure with all of the information a criminal needs to make a false card, as well as information about your company that could hurt you later if it fell into the wrong hands. Recognize materials that may contain private information and dispose of them properly.

Destroy any documents that have any personal information on them with a paper shredder before declaring them trash.

Protecting your customers and your business is worth a few extra seconds.

The Terminal Repair Scam

This is the oldest scam in the book, but also one of the most popular and most effective ways for thieves to lift confidential information. We're all familiar with the “bait and switch” technique. They come into your business and tell you that your POS terminal needs to be repaired – offsite. But don't worry; they'll replace your broken one with a loaner. Once the loaner is in place, all of the information you scan through is recorded, and now the information is theirs.

You may not even see it coming, as these criminals often pretend to work for POS companies or say that they are attending to other official business. Any attempt to repair your terminal should be reported to the police, and no replacement terminals should be accepted. The safest thing you can do is to be cautious and report any suspicious happenings immediately by calling Clearent. We will check to see if there is a replacement request noted for your location.

Fraudulent Returns

Fraudulent returns are a major problem associated with fraud and theft. Staff members have been caught returning items that were never purchased and pocketing the money. In some cases, merchants don't even realize they have been victimized until it is too late. Make sure your employees take the necessary steps to ensure this doesn't happen in your business.

Your terminal can also limit access to returns by requiring the use of passwords. (See the terminal documentation section.)

- Keep your point-of-sale terminal passwords confidential and stored in a safe place.
- Change your password often to protect yourself in case someone does get into your system.
- Don't share your terminal.
- Make sure to follow the proper procedures when it is time to shut down.
- Keep a record of your balances each day so you can identify a problem as soon as it occurs.

International Credit Cards

Take extra care when accepting international credit cards.

Thieves use foreign cards because cashiers are not as familiar with them. The criminal searches for a busy merchant who may overlook irregularities in a card issued by a foreign bank rather than become suspicious.

Inspect the card thoroughly, checking to make sure the card is valid, and always swipe it. The main elements of the card – logo, hologram, clear embossing and so on – should be the same despite where the card originated. Check to make sure the signature matches the name on the card, and that once swiped, the number on the terminal matches the number on the card. Also, watch out for customers who check out the cashiers first before getting in line – criminals often look for an

inexperienced clerk or someone who may be easily intimidated. If anything seems suspicious during the transaction, call in a Code 10.

Office Products Scams

Watch out for companies trying to sell office products such as copy paper, ink cartridges, stationery and other supplies to your business. They may try to appear as if they are working for a reputable company. In reality, they will overcharge you for inferior merchandise. Deceptive telemarketing is a violation of the law – report any suspicious persons immediately.

Phone Fraud

Like the paper scammers, you may not see the phone fraud coming until it is too late. Of course, there are the telemarketers who use the phone to further their illegitimate businesses and scam money, but what about the criminals that aren't selling anything at all?

These crooks still use the phone to swindle merchandise from the retailer. Most of the time the criminal will phone a store, telling the clerk he has picked out the items he wants but cannot come to pick them up for some reason or another. He will ask the clerk to run his credit card through and assure the clerk that a courier will be by to pick up the merchandise.

Once the merchandise has left the store, there is no way of knowing to whom it actually went or where it was going.

Often these phone fraudsters pose as respected individuals with high profile jobs and qualifications. It is not uncommon, however, to find out the person has stolen a credit card and is using someone else's identity to receive the desired merchandise. There is no real way of knowing if the card is legitimate in a situation where the cardholder is not able to show up. It is safest to stick to the rules in these situations – don't take credit card numbers over the phone, and reject a credit card that is not being handed to you by its lawful owner.

Point-of-Sale Protection

Research shows that some businesses repeatedly expose their customers to fraud by asking them to provide a phone number with a credit card transaction or a credit card number as a voucher for a personal check. Shield your customers from card thieves by not recording private information. If you must list the identifying information, write it elsewhere (such as your copy of the sales receipt or on a store invoice). Keep these pieces of information somewhere that is not accessible to just anyone. Your customers will appreciate the fact that you are looking after their best interests. Thermal printers can further safeguard your customers since only the merchant copy of the sales draft will have the cardholder signature.

The Last Minute Shopper

Be on the lookout for the shopper who is purchasing expensive items just before closing time, or someone who is hurriedly filling a shopping cart with this type of item, without paying much attention to price, size, or quality. These are the shoppers whose transactions need to be handled with your utmost attention.

Counterfeit Cards

Stolen and counterfeit cards are a huge problem for merchants and credit card issuers alike. Because of the technology available to them, counterfeiters are able to reproduce false cards that are high quality, even without the benefit of the original. All they really need is personal information and

technology to produce credit cards, debit cards, and smart cards. The result is a huge financial loss to businesses around the globe. You must never retain magnetic-stripe or card authentication numbers (CVV2/CVC2/CID) since this information, if stolen, could be used to counterfeit cards.

Protect your business by teaching your staff to recognize the signs of a false card.

When to call in a Code 10:

- If the embossing on the card is illegible
- If the last few numbers are not embossed on the hologram, or if these numbers do not match the account number on the sales draft or at the terminal
- If there is no Bank Identification Number (BIN) above or below the first four digits
- If the name on the card does not match the signature or there is a misspelling
- If the hologram is not clear or the picture in the hologram does not move
- If the card does not have an expiration date
- If the card does not start with the correct numeric digit – all Visa-branded cards should start with a 4, all MasterCardbranded cards with a 2 or a 5, all American Express-branded cards with a 37 or 34, and all Discover Network cards with a 6
- Be aware of cards that don't swipe – check these cards for other security features
- If a card does swipe, make sure the card number and the number that appears on the terminal match
- If you receive any message other than “approved” or “declined”

Don't Hesitate! Call In a Code 10

Any time you have doubts about something – a fraudulent card, a signature or even a customer's behavior – call in a Code 10. A Code 10 allows you to call for an authorization without the customer becoming suspicious.

After dialing the authorization center, inform the operator that you have a Code 10. The operator will put you through to the correct person, who will ask you a series of “yes” or “no” questions. Hold on to the card if possible while making the call. If the operator decides something is amiss, he or she will deny authorization. The operator may even request to speak with the cardholder to ask account information questions that only the true owner of the card would know.

A Code 10 can be used any time you feel a transaction may not be legitimate, even if you have already gotten approval on a transaction or if the customer had already left the premises.

Defeating Fraud Helps You and Your Customers

Whether it's a different twist on an old scam or a new scam altogether, there will always be someone who tries to pull the wool over your eyes. If you and your staff are well prepared with the skills to recognize suspicious transactions, and know how to correct the situation, then you're beating fraudsters at their own game.

Take the extra steps to stop fraud before it starts. After all, it is the merchant – not the consumer – that stands to lose the most from credit card fraud. The most important thing you can do is stay educated on the ways fraud occurs and follow your instincts when you find yourself in a suspicious situation. The majority of the time, plain old common sense can prevent losses.

By following the information in this guide and working together, we increase the chances of successfully protecting your business against fraud!

Glossary

Address Verification Service (AVS): Service that verifies the cardholder's billing address in order to help combat non-face-to-face fraud.

Authorization: Verification of a payment card transaction by a payment card-issuing bank or other institution, or by an approved independent service provider. Authorization is initiated by accessing (by voice or electronic terminal, as appropriate) Clearent's designated authorization center(s).

Authorization is based on the cardholder account status and available credit.

Authorization Code: The alpha/numeric code designated by the issuer given to a sales transaction as verification that the sale has been authorized. The authorization code is always included on the merchant sales draft.

Payment Cards or Cards: Credit and/or debit cards issued by a payment technology or financial services company or a financial institution.

Payment Card Transaction or Transaction: Transactions between a merchant and a cardholder for the sale or rental of goods, the provision of services evidenced by a sales draft or credit draft, or where permitted by agreement between Clearent and merchant, or by an electronic equivalent of a sales draft or credit draft, which is presented to Clearent by the merchant for processing through the Interchange Systems.

CVV2 (and CVC2) Card Verification Value 2 and CID: Three-digit codes that appear in the signature panel on the back of payment cards. Some American Express Cards have four-digit CID codes printed on the front of the card. They are valuable fraud detection and prevention tools for card-not-present transactions. See Card Not Present section for more detail.

Cardholder: Sometimes referred to as "Card Member" in Card Brand materials, the person or entity whose name is embossed on card or whose name appears on a payment card as an authorized user.

Card Truncation: Printer suppresses or masks the expiration date and all but 4 digits of account number on cardholder receipt.

Chargeback: A chargeback is a previous transaction that is being disputed by the cardholder or their issuing institution. A chargeback occurs when a cardholder disputes a charge or when proper payment card acceptance and authorization procedures were not followed.

When used as a noun, a payment card transaction which is debited to the deposit account by Clearent, set-off against any other account maintained by the merchant with Clearent or presented directly to the merchant by Clearent for repayment when the deposit account does not contain sufficient funds.

When used as a verb, the act of debiting the deposit account, setting-off against another account or otherwise recovering, or seeking to recover, the value of the transaction.

Chargeback Fees: Fees charged under card brand rules for items that result in a chargeback. You may be subject to these fees if you failed to follow card acceptance and authorization procedures and the card issuer presents a valid chargeback.

Chargeback Reason Code: A numerical code, which identifies the specific reason for the chargeback.

Check-In Date: The date the cardholder arrives at the lodging establishment.

Check-Out Date: The date the cardholder checks out of the hotel. Also considered to be the transaction date.

Code 10: A universal code that provides merchants with a way to alert the authorization center that a suspicious transaction is occurring without alerting the cardholder (or other person presenting the payment card). The Code 10 operator asks a series of questions that can be answered with yes or no response. Follow the operator's instructions. NEVER ENDANGER YOURSELF.

Commercial Card: A Business Card, Corporate Card, Fleet Card or Purchase Card issued for Commercial use, often with a higher discount expense than consumer cards. Non-T&E (Travel & Entertainment) merchants accepting a large volume of Commercial Cards should utilize a product that will support entry of sales tax and customer code.

Consumer Card: A card issued to a consumer.

Consumer Rewards Cards: Visa Infinite Card, Visa Signature Card, Visa Rewards Card and MasterCard World Cards issued to consumers have additional perks. T&E merchants incur additional discount expense for these upscale cards.

Consumer Rewards Cards used at non-T&E merchants may be subject to higher interchange expenses.

Credit Draft: Records of returns or credit transactions presented to Clearent by the merchant for processing through the Interchange System for crediting to the cardholder's account and debiting to the deposit account.

Debit Card: A plastic card used to initiate a debit transaction.

In general, these transactions are used primarily for goods and services and to obtain cash, for which the cardholder's checking account is debited by the card-issuing institution.

Deposit Account: A business checking account designated by the merchant through which all payment card transactions and adjustments are processed by Clearent.

Factoring or Draft Laundering: A merchant's presentation to Clearent of what would otherwise be a sales draft but is not, because the underlying transaction is not between the merchant and the cardholder. This includes, but is not limited to, merchant's processing, debiting, negotiating or obtaining payment pursuant to the Clearent Merchant Agreement in connection with a purported transaction if the merchant did not furnish, or agree to furnish at some later time, the goods or services comprising the purported transaction.

Floor Limit: A dollar amount set by the acquirer in accordance with payment card brand rules and regulations. The merchant must obtain authorization for any transaction over the floor limit.

Interchange System: Processing systems, which facilitate the interchange and payment of transactions between cardholders and persons, and entities (including merchants) that accept cards.

Issuer: The financial institution that holds contractual agreements with and issues cards to cardholders.

Limited Acceptance Merchant: A merchant who elects to accept credit cards or debit/prepaid cards, or both, by so notifying Clearent in writing.

Magnetic Stripe: A stripe (on the payment card) of magnetically encoded cardholder account information.

Merchant: A person or entity entering into a Merchant Agreement with Clearent, as well as all personnel, agents, and representatives of the merchant.

Merchant Identification Number: A 16-digit number each merchant is provided under the Clearent Merchant Agreement.

Merchant Summary: A form on which the merchant imprints the merchant's identification number, and which provides a summary of the merchant's payment card deposits.

Negative Deposit: What occurs when the dollar amount of a credit draft submitted for deposit to the deposit account exceeds the dollar amount of the sales drafts submitted for deposit.

Off-Line Debit Card: A payment card, used to purchase goods and services and to obtain cash, which debits the cardholder's personal deposit account. No PIN number is required to process off-line debit cards.

On-Line Debit Card: A payment card that debits the cardholder's personal deposit account and is used to purchase goods and services and to obtain cash. A PIN number is required to process on-line debit cards.

Operating Regulations or Regulations: Unless specifically referred to as the operating regulations of Discover Network, Visa, or MasterCard, the current operating regulations of Discover Network, Visa, and MasterCard.

Payment Card Industry Data Security Standards (PCI DSS): Common standards for merchants and third parties supported by all major card brands with the goal of protecting payment card account data wherever it is received or stored.

PIN: Personal Identification Number. The confidential individual number or code used by a cardholder to authenticate card ownership for ATM or POS terminal transactions.

POS: Point of Sale. The location of a merchant from whom the customer makes a purchase.

Pre-authorized Order: A cardholder's written authorization to make one or more charges to the cardholder's card account at a future date.

Purchasing Card: Designed to help companies maintain control of small purchases while reducing whatever administrative costs are associated with authorizing, tracking, paying and reconciling those purchases.

Recurring Payments: A series of transactions in which sales drafts will be processed by the merchant on an ongoing basis, unless and until canceled by the cardholder.

Retrieval Request: The request for either an original or legible copy of the transaction information document or substitute draft as identified in the electronic record.

Sales Receipt: A paper or electronic record of a sale, rental, or service transaction which the merchant presents for processing, through the Interchange System or otherwise, so that the cardholder's card account can be debited and the deposit account may be credited.

Split Sale: Preparation of two or more sales drafts for a single transaction on one card account in order to avoid authorization procedures.

T&E Travel and Entertainment: Hospitality Industry segment.

Includes: lodging, car rental, cruise ships, travel agent, transportation, and restaurants.

Third Party Provider: Any organization, software integrator, or service provider (such as a third party terminal provider) that assists merchants in completing credit card transactions. The third party is not a member of a card association, nor a Participant in a card brand program (such as Amex OptBlue), nor is it directly connected to any card brands, but it provide(s) the following service(s):

- Authorization and/or transaction processing [including pre-authorization, authorization, AVS CVV2/CVC2/CID, cardholder authentication (Verified by Visa, MasterCard Secure Code, etc.)]
- Voice Authorization: Authorization obtained by telephoning a voice operator.