

Card Acceptance Guide

Released August 2014

Revision 18

Global Payments Inc.
10 Glenlake Parkway NE
North Tower
Atlanta, GA 30328



This Guide contains information protected by copyright. No part of this material may be duplicated, reproduced or disclosed in any form without prior written consent from Global Payments.

The information contained in this guide is proprietary and confidential to Global Payments and merchants who have executed an Agreement with Global Payments for card payment services.

Global Payments reserves the rights to add, modify, or cancel any and all provisions described in this Guide, as it deems appropriate, with or without advance notice.

For the latest version of this guide, please visit our Web site:

globalpaymentsinc.com



This guide is part of your Global Payments Inc. (herein after referred to as Global Payments) Merchant Agreement and you must follow the procedures in this Guide to comply with your Agreement.

To order a printed copy of the Card Acceptance Guide, fill out the request form at <https://www.globalpaymentsinc.com/USA/customerSupport/cagform.html>.

Important Information

Global Payments Merchant Number

Global Payments' Account Representative Telephone Number

Global Payments Customer Service Telephone Number

Your Bank ID Number

Other Important Telephone Numbers

Code 10 Authorization Telephone Number
1-800-944-1111

To order additional products and services from Global Payments,
call 1-800-929-1245 ext. 3

Visit the Global Payments Web site:

globalpaymentsinc.com

To reach VISA® or MasterCard® or American Express®:

www.usa.visa.com

www.mastercard.com/us

www.americanexpress.com

Merchants Participating in Global Payments' American Express Full Acquiring Program click here.

https://www.globalpaymentsinc.com/GPDB/AccessDOC.aspx?SubDoc_ID=1383

Using the Card Acceptance Guide

The Global Payments Card Acceptance Guide was created to provide merchants a reference tool for important payment processing and industry information.

Please refer to the following list of **Top Ten Best Practices** merchants should be knowledgeable about before accepting card payments.

1. [Completing an Electronic Transaction – Page 10](#)
Learn the simple steps to complete a transaction fully and accurately.
2. [Managing Authorization Requests – Page 13](#)
Understand card issuer responses on authorization requests.
3. [Processing eCommerce Transactions – Pages 17-20](#)
Accept online payments from customers quickly and securely.
4. [General Merchant Best Practices – Pages 25-26](#)
Process card payments safely, efficiently and in compliance with all industry standards.
5. [Examples of Prohibited Transactions – Pages 27-28](#)
Avoid accepting transactions that will lead to loss or penalties.
6. [Providing Refunds – Pages 30-31](#)
Limit the hassle of return or exchange transactions.
7. [Chargeback Prevention Best Practices – Page 37](#)
Reduce the risk of receiving a chargeback notification with these precautions.
8. [Contacting Customer Care – Page 38](#)
Call Global Payments Customer Care for assistance with general inquiries or issues.
9. [Understanding Merchant Statements – Pages 39-40](#)
Accurately read and understand the various components of monthly merchant statements.
10. [Preventing Fraud and Spotting Counterfeit Cards – Sections 5 and 6](#)
Protect against fraudulent transactions and avoid accepting counterfeit cards.

Table of Contents

Introduction	1
Purpose	1
Global Payments – An Advocate in Payment Processing.....	1
Global Payments’ Role.....	2
Merchants’ Role.....	3
Need Assistance?	3
Section 1: Card-Present Transactions	5
Customer/Cardholder	5
Bankcards and Issuers.....	5
Merchants.....	5
How the Transaction Process Works.....	6
Authorization and Electronic Data Capture	6
Authorization and Capture – PIN Debit	7
Settlement	7
Merchant Funding.....	8
Electronic Data Capture and IVR Merchants	8
Retention of Sales Drafts.....	8
Draft Retrieval Requests	9
Sample Sales Draft Retrieval Request	9
Merchant Deposits	10
Completing an Electronic Transaction	10
Determining Card Validity	10
Visa Cards.....	10
MasterCard Cards	11
Discover Cards.....	12
American Express Cards.....	12
PayPal In-Store Payment Cards	12
Compare Account Numbers.....	12
Available Fraud Controls	12
Request Authorization.....	13
Print the Sales Draft	14

Obtain and Compare Signatures.....	15
Commercial Card Transaction	15
Section 2: Card-Not-Present Transactions	17
Completing Electronic Commerce Transactions	18
Merchant Web Site and Electronic Transaction Requirements.....	19
Transaction Receipt Requirements	19
Completing Mail Order and Telephone Order (MOTO) Transactions	20
Completing Recurring Bill Payment Transactions	21
What is a Recurring Payment?.....	21
How is a Recurring Payment Different from Other Forms of Payment?	21
What should be on an Order Form?	21
Other Requirements and Prohibitions for Recurring Transactions	22
Best Practices for Use of Convenience Fees.....	23
Section 3: Card Acceptance.....	25
Best Practices for Merchant Use	25
Point-of-Sale Protection	27
Personal Information	27
Prohibited Transactions	27
Examples of Prohibited Transactions	28
Accepting Debit and EBT Cards	28
EBT Processing.....	29
Returns and Exchanges.....	30
Limited Acceptance Merchants	31
Surcharging.....	31
Service Fee	32
Section 4: Operating Guidelines	34
Month-End Settlement	34
Draft Laundering or Factoring	34
Charge Restrictions	34
Protecting Cardholder Privacy.....	35
Proper Display of Signage	36
Chargebacks.....	36

Merchant’s Right to a Rebuttal36

Some Do’s and Don’ts of Chargebacks.....37

Supplies.....38

Customer Care.....38

Understanding the Merchant Statement.....39

Questions About the Merchant Statement39

Sample Merchant Statement40

Sample Merchant Statement Details.....41

Section 5: Preventing Fraud 42

Take Charge of Fraud42

Skimming45

Don’t Be Intimidated45

Deceptive Deliveries45

The Manual Key-In.....46

Borrowed Cards46

Disposal of Important Information46

The POS Device Repair Scam.....46

Fraudulent Returns.....47

International Credit Cards.....47

The Last Minute Shopper47

Counterfeit Cards47

Don’t Hesitate! Call In a Code 10.....48

Defeating Fraud Helps Merchants and Their Customers48

Payment Card Industry Security Standards Council (PCI SSC).....49

PCI DSS Program for Level 4 Merchants49

The Digital Dozen49

Section 6: Spotting Counterfeit/Altered Cards 51

Color51

Embossing51

Signature Panel51

Hologram.....51

MasterCard Formats.....52

Visa Card Formats.....53

Table of Contents

Discover Card Formats.....	54
JCB Card Formats.....	55
American Express Card Formats.....	56
PayPal In-Store Checkout Payment Card Formats	57
Pick Up Card Procedures	58
Exhibits and Addendums	60
Exhibit A: EBT Card Services Agreement	60
Exhibit B: eCommerce/Internet Services Addendum.....	68
Exhibit C: Telephone and Mail Order Services Addendum	73
Exhibit D: Lodging Visa/MasterCard Service Addendum	75
Exhibit E: Advance Lodging/Resort Deposit Service Addendum	79
Exhibit F: Priority/Express Check-Out Service Addendum	82
Glossary of Terms	84
Sponsoring Institutions.....	93

Introduction

Purpose

Congratulations! Accepting credit, debit, EBT, gift or commercial cards as a valid form of payment offers a valued service to a merchant's customers.

For today's merchant, accepting various payment cards has become both easier and at the same time, slightly more complex. Computerized terminals and leading-edge card acceptance devices make transaction processing automatic and seemingly easy, potentially increasing a merchant's profitability. However, these devices can also create increased probability for processing mistakes and fraudulent transactions resulting in copy requests and chargebacks.

Global Payments' Card Acceptance Guide is a comprehensive manual for all businesses that accept card-present and card-not-present transactions.

The purpose of this guide is to:

- Provide merchants and their staff the latest information on processing all types of transactions.
- Define requirements and best practices for doing business on the Web.
- Provide detailed information on the types of w and guidelines to follow to remedy or prevent them.

This Guide is part of the Global Payments' Merchant Agreement. Merchants must follow the procedures in this Guide to comply with their Merchant Agreement. Please keep the Merchant Agreement, other paperwork and telephone numbers associated with the Merchant Agreement in one location.

Global Payments wants all of its merchants to be comfortable with the card acceptance program, take advantage of all its features and ensure merchants have the information, card payment options and flexibility needed to grow their businesses. The information in this Guide has been provided to supplement the Merchant Agreement and will assist in the operation of the card acceptance program.

Global Payments – An Advocate in Payment Processing

Welcome, and thank you for choosing Global Payments for payment processing. Every day, more than one million merchant locations across North America, Europe and Asia rely on Global Payments to process billions of credit, debit, electronic benefits transfer (EBT), commercial card and check transactions through Global Payments' secure data networks, while also handling merchant settlement and accounting needs and providing point-of-sale (POS) device management.

Global Payments' Role

Global Payments' most important role is serving as its merchants' advocate. Global Payments is committed to providing service, value and a comprehensive selection of POS solutions, for fast, reliable processing and settlement.

Global Payments will also handle merchant questions and concerns with prompt and courteous service through Global Payments' "Voice of the Customer" program.

In addition, Global Payments offers over four decades of expertise in payment processing and is a full-service provider of merchant processing services for:

- All major credit cards
- Debit cards
- EBT cards
- Commercial cards
- Gift cards
- Purchasing cards

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

- Card authorization
- Draft capture
- Chargeback handling
- Check verification, guarantee and recovery
- Credit card processing
- Debit card processing
- Electronic benefits transfer processing
- Help desk
- Merchant accounting
- Reconciliation
- Settlement
- Supplies
- Terminal management & support
- Web-based transactions
- Web-based reporting services

Supported Industries:

- ▶ Automotive
- ▶ Direct marketing
- ▶ eCommerce
- ▶ Education
- ▶ Government
- ▶ Healthcare
- ▶ Lodging and Hospitality
- ▶ Restaurant
- ▶ Retail

Merchants' Role

As a Global Payments merchant, it is important to:

- Read, understand and abide by the Merchant Agreement and this Card Acceptance Guide.
- Take all necessary steps to prevent fraud.
- Follow best practices in accepting electronic payment methods.
- Advise Global Payments of any changes related to the merchant's business, such as changes in status, changes in business structure, address or contact information, or cancellations.
- Notify Global Payments upon canceling or returning equipment.
- Keep up-to-date on all industry news and policy changes.
- Advise Global Payments of any changes to merchant payment application, hardware or software.

It is a merchant's responsibility to comply with all applicable laws and association rules and regulations. Please note that, while several guidelines in this Card Acceptance Guide reference or suggest obtaining certain information from a cardholder in the transaction process, merchants should consider and are responsible for compliance with any applicable state laws regarding obtaining personal information from a cardholder in connection with a card transaction.

Need Assistance?

Global Payments is here to help with fast and courteous service, 24 hours-a-day, seven days-a-week. The Global Payments Web site is also a source of information about Global Payments' products and services. To access the Web site go to www.globalpaymentsinc.com. Make sure to check the Industry Initiatives section of the Web site for information about card associations, regulations and industry updates. For information about obtaining additional products and services from Global Payments, please call: **1.800.828.7889**.



1: Card-Present Transactions

Parties Involved

Customer/Cardholder

A customer submits an application to an institution that issues Visa®, MasterCard® / Diners Club®, Discover®, JCB®, China Unionpay or American Express® payment cards to become a cardholder. The customer may be an individual or a business. The cardholder becomes an authorized user when the institution approves and issues a card.

Bankcards and Issuers

Visa and MasterCard cards are sometimes known as bankcards because individual financial institutions, such as banks, issue them. Other cards, such as American Express, are usually issued by the credit card company itself.



For merchants who also participate in ACH/Check programs, contact a Global Payments sales representative for more information.

The card may be:

- a credit card, which means that the bank has authorized a line of credit from which the customer may draw;
- a debit card (which includes signature debit and debit with PIN), which is tied to the amount of money actually on deposit for the customer; or
- a commercial card, which is used for business charges.

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

Card issuers also accept small business and corporate customer applications for commercial card issuance. These types of cards include small business, corporate and purchasing cards. Additionally, the Government Services Administration (GSA) issues cards to federal agency staff to cover purchase expenses.

Merchants

A merchant opens a business checking account with a bank connected to the ACH network. The merchant also applies for a merchant account either through a bank or a payment processing organization. Once the merchant has established a checking account and been approved for a merchant account, the merchant is an authorized acceptor of cards for the payment of goods and/or services. Now the merchant is prepared for the first cardholder to perform a transaction. For Lodging merchants, please refer to Exhibit D.

1: Card-Present Transactions

How the Transaction Process Works

Any bankcard transaction ultimately begins and ends with the cardholder. The illustration below shows the steps involved in an electronic payment transaction and how the various organizations interact to create a smoothly executed process.

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



*Fees per transaction are estimates and may vary.

Authorization and Electronic Data Capture

Once the POS device captures the data from the card (either electronically or manually keyed), the POS device passes an electronic imprint of the card number, expiration date and counterfeit detection value to Global Payments for authorization.

Global Payments then electronically routes the electronic data from the card to the card issuer and encrypts sensitive data in flight. The card issuer checks the cardholder account status and compares the requested authorization amount to the cardholder's available spending limit, reviews the transaction with fraud protection tools or memo posts and sends it back to Global Payments.

Due to regulatory concerns, Global Payments and card association rules permit only hotels and car rental merchants to perform authorizations for an estimated amount. Restaurant and other service industry merchants that accept gratuities may perform only one authorization for the pre-tip amount. Effective October 2009, if a merchant does a \$1.00 authorization (also called a status check), then the merchant may incur an additional fee referred to as a "Misuse of Authorization Fee."

At this point, Global Payments routes the card issuer's authorization response to the merchant. The POS device prints a transaction receipt for the cardholder and the cardholder signs the merchant transaction receipt – except where the transaction is eligible for “No Signature Required” (NSR). Merchants with a contactless reader may participate in the American Express No Signature Program, the Visa NSR and the MasterCard Quick Payment Service (QPS) programs.

These programs do not require a signature for transactions under \$50.00 where the card is recognized by the contactless reader or the magnetic stripe reader. Card association rules require that all electronically printed cardholder transaction receipts truncate the expiration date in its entirety and also truncate most of the cardholder account number. Certain states require card number and expiration date truncation on both the cardholder and merchant copies of receipts. Please be aware of your state's laws and see the Industry Initiatives section of our Web site (globalpaymentsinc.com) for more information on state and card association requirements regarding truncation.

Authorization and Capture – PIN Debit

If the POS device has an internal or external PIN Pad, then the merchant can accept PIN debit at the point of sale. Once the POS device captures the data from the card, it passes an electronic imprint of the card number, expiration date and counterfeit detection value and PIN block to Global Payments for authorization.

PIN debit transactions are processed using PCI PED compliant hardware and applications that use Triple DES encryption standard. Global Payments then routes the data from the card and the PIN data to the card issuer with all sensitive data encrypted “inflight.” Since the cardholder uses a PIN to authenticate the identity of the cardholder at the point of sale, no cardholder signature is required.

Settlement

The process of moving the transaction information from the merchant's business to the cardholder's financial institution is called settlement. Visa, MasterCard, American Express, Discover and the PIN debit networks maintain authorization and settlement networks for card processing and charge a fee for their use. This is the transaction percentage, and is the foundation for the discount rate.

Occasionally, a cardholder will have a question about, or will want to challenge, a transaction draft already deposited in the merchant's account. In that case, Global Payments may debit the merchant's account for the amount of the sale until the customer's question or challenge is resolved. This is called a chargeback and is described in more detail later in this Guide.



Remember, a merchant's deposit account at its bank is not just for deposits!

Global Payments subtracts each month's accumulated discount fees from the merchant's deposit account.

Global Payments also subtracts the settlement charges.

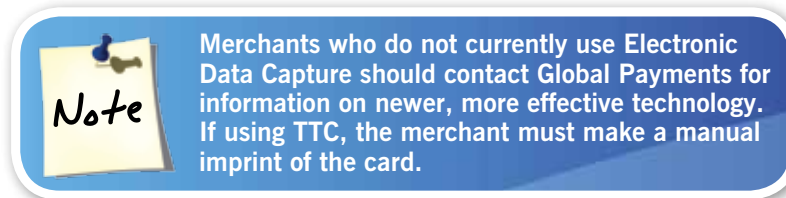
1: Card-Present Transactions

Merchant Funding

Global Payments prepares ACH files to electronically fund our merchants based on the number of approved transactions the merchants sends to Global Payments.

Electronic Data Capture and IVR Merchants

Electronic Data Capture (EDC) merchants use a POS device (e.g., terminal, Touch Tone Capture (TTC) also known as IVR, cash register or PC) to authorize and settle their transactions. The merchant can use the POS device to validate the amount of the settlement before transmitting the transactions to Global Payments at the end of the day.



Retention of Sales Drafts

Merchants must safeguard all stored sales drafts and other transaction data that contain full card numbers (i.e. reports, screen prints) and provide limited (and only authorized) access to these items. Global Payments has applications that truncate both copies of the transaction receipt and the middle six positions of the card number – making it easy for the merchant to locate transactions using the first six / last four digits on the report and then locating the merchant copy by the last four digits. Contact Global Payments for information on reporting tools which increase efficiency in merchant operations.

Merchants must keep all systems and media containing cardholder, account or transaction information (whether physical or electronic) in a restricted, secure manner to prevent access by or disclosure to any unauthorized party. At the end of the 18-month retention period, the merchant must render unreadable all transaction data, such as sales drafts, reports and other media with cardholder account data, prior to discarding it. If the merchant has used a PC to access transaction information, then the PC must not be disposed of until information has been rendered unreadable.

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

MasterCard: Sales slip retention time frame is 13 months

PayPal: Sales slip retention time frame is one (1) year from the Transaction Date, or two (2) years from the Transaction Date if the Transaction was subject to Dispute or as required by Applicable Law.

American Express: The retention time frame for Charge Records is twenty-four (24) months from the date Merchant submitted the corresponding Charge to American Express.

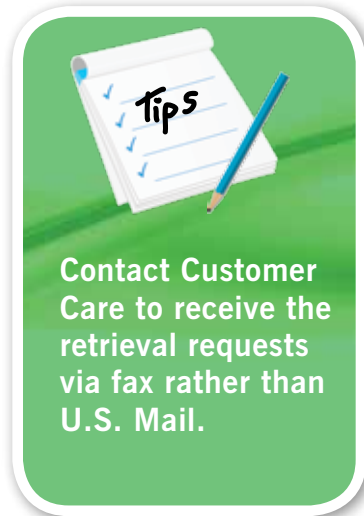
Draft Retrieval Requests

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 the merchant's records, Global Payments will forward a retrieval request 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 retrieval request form to the appropriate processing center. Always obtain a copy and mail or fax it to the Global Payments' requesting party within the time specified in the retrieval request to avoid chargebacks because the requesting institution did not receive the copy in time.



Sample Sales Draft Retrieval Request

A sample retrieval request letter is shown below.

5/25/2006

RETRIEVAL SALES DRAFT REQUEST

NICKS BOATING ADVENTURES
NICK A. KNIGHT
1234 FANTASY LANE
LAS VEGAS, NV 65432

GLOBAL PAYMENTS
DEPARTMENT CBR
10705 RED RUN BOULEVARD
OWINGS MILLS, MD 21117
(800) 367-2638
FAX (443) 394-1915

This is a request for copies of sales drafts. To preserve your reversal rights, please respond by 6/3/2006. Timely and accurate fulfillment is critical to avoid an unnecessary debit to your account.

PLEASE COMPLY WITH THE FOLLOWING HANDLING PROCEDURES:

- Please supply a clear and legible copy of the sales slip(s) requested.
- Hotels supply guest folio.
- Car Rentals include rental agreement.
- List case number (provided below) for each sales draft.
- The following items MUST be legible:
 - Cardholder Account Number
 - Transaction Amount
 - Transaction Date
 - Merchant Name/Location
 - Expiration Date
 - Cardholder Signature
- Mail phone order and e-commerce merchants are not required to provide cardholder signature. However, a substitute draft and/or order form must be supplied.

1.				
Merchant Number	Cardholder Number	Processing Reference	Invoice/Ticket	Case Number
999888777666	4321432156785678	12345678901234567890999		1614400305
Merchant Reference	Tran Amt	Tran Date	Post Date	CP Date
7992622	\$55.00	3/19/2006	3/20/2006	5/23/2006
Reason: Fraud analysis request				
2.				
Merchant Number	Cardholder Number	Processing Reference	Invoice/Ticket	Case Number
999888777666	4444555566667777	11122233344455566677788		1614400419
Merchant Reference	Tran Amt	Tran Date	Post Date	CP Date
10837586	\$61.00	4/17/2006	4/18/2006	5/23/2006
Reason: Fraud analysis request				
3.				
Merchant Number	Cardholder Number	Processing Reference	Invoice/Ticket	Case Number
999888777666	5678567856785678	12341234123412341234567		1614400454
Merchant Reference	Tran Amt	Tran Date	Post Date	CP Date
11738854	\$43.00	4/26/2006	4/27/2006	5/23/2006
Reason: Fraud analysis request				

Merchant Deposits

For merchants who use Electronic Data Capture (EDC) to process credit card transactions or Touch Tone Capture, DO NOT submit paper sales drafts for deposit into the bank deposit account. Transaction information should be transmitted to Global Payments using POS settlement at the end of each business day. Refer to the POS device manual provided with the welcome kit for information on completing the settlement procedures. If a merchant is unable to complete a settlement, the merchant should contact the Help Desk for further instructions.

Completing an Electronic Transaction

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

Use the following steps to complete an electronic transaction:

- Make sure the card is valid.
- Swipe the card to request the transaction authorization.
- Compare account numbers.
- 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.
- Obtain a valid authorization.
- Print the sales draft.
- Obtain and compare signatures.
- Press clear before sliding another card.
- Use the POS device manual or call the Help Desk if the system develops problems.

The transaction date should fall between the effective date and the card's expiration date (if an effective date is printed on the card). If there is no effective date visible on the card, the transaction date should fall prior to the card's expiration date. If the current date is not within the specified range, do not accept the card. Follow the authorization procedures as described in the POS device manual.

Determining Card Validity

Visa Cards

All Visa account numbers begin with the number four (4). The embossing on all digits must be clear, even and the same size/shape. A three-dimensional dove hologram appears to move on the label as the card is rotated or tilted. The last raised card numbers appear on top of the hologram. A 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 flying “V” is an embossed security character beside the “Good Through” date. If the V is not italicized or is missing, the card is counterfeit.

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, which is 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.

Some Visa gift, prepaid, and reloadable cards may have the card number printed on the front of the card, but not embossed. If this is the case, the card is permitted for fully authorized transactions.

MasterCard Cards

All MasterCard account numbers begin with the number five (5), followed by zero through five (i.e. 50-55). The embossing should be clear and uniform in size and spacing. MasterCard now supports unembossed cards by issuer. Presently, the unembossed issued card account information will appear on the front of the card as an indent, laser or thermal (heat-induced) print. 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 three-digit card validation code (CVC2).

The card should not be physically altered in any way. Some MasterCard gift, pre-paid and reloadable cards may have the card number printed on the front of the card, but not embossed. If this is the case, the card is permitted for fully authorized transactions.

1: Card-Present Transactions

Discover Cards

The embossed numbers in the card number should be clear and uniform in size and spacing within grouping. An underprint of “VOID” on the signature panel becomes visible if erasure of the signature is attempted. The card number on the back of the card is followed by the Card Identification Data or “CID.” If the merchant receives settled funds for Discover transactions directly from Discover, then please refer to the Discover Card Acceptance Guide for more information.

Some Discover gift, pre-paid and reloadable cards may have the card number printed on the front of the card, but not embossed. If this is the case, the card is permitted for fully authorized transactions.

American Express Cards

An American Express Card Acceptance Procedures Guide is available [online](#). Questions on fraud prevention and safeguarding cardholder data can be emailed to American Express Fraud Protection Center at spooof@americanexpress.com.

PayPal In-Store Payment Cards

PayPal In-Store Payment Cards are unembossed cards that should have two-color marks or a grayscale mark when necessary and a PayPal-provided acceptance mark. Printed on the back of the card are the last 4 digits of the Account Number, PayPal Account Holder Name, expiration date, tamper proof signature panel, along with the Card Identification Data or “CID.”

Compare Account Numbers

While processing the transaction, check the card’s features and security elements (per the specifications listed for each issuer) to make sure the card is valid and has not been altered.

Compare the last four digits of the account numbers printed on the sales draft to the embossed (or printed if a MasterCard) number on the customer’s card. If the numbers match, enter the amount of the transaction into the POS device and request authorization. If the numbers do not match, call the Voice Authorization Center and say, “Code IO.” Follow the instructions the operator gives over the telephone.

Available Fraud Controls

Most POS devices have the ability to perform fraud checks. This functionality will help in identifying potentially counterfeit credit cards and assist in avoiding potential chargeback losses to the merchant account. If the controls are ‘on,’ the merchant will be prompted to enter the last four digits of the card number that is embossed or printed on the front of the card after initially swiping the card. If the POS device does not detect a problem, the transaction will proceed as normal. If there is a possible problem, the POS device will display a ‘mismatch’ message (See “Request Authorization” section below). If the POS device cannot capture the electronic imprint (magnetic stripe) of an unembossed card, then the merchant must request another form of payment since a manual imprint of the card is not available.

If a contactless reader is used and the transaction qualifies as a NSR transaction, then the cardholder may keep the card in his or her possession. Contactless readers have special means of verifying that a contactless card was used at the point of sale.

Request Authorization

In the authorization process, the card issuer approves or declines a transaction. In most cases, transactions are quickly approved and processed electronically.



The following are typical of the responses on authorization requests:

- **Approved:** This response means the card issuer approves the transaction. The approval is noted automatically when using a POS device printer. Write the authorization code clearly on the sales receipt when a POS device printer is not used.
- **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 re-authorize or authorize for a smaller amount.
- **Call or Call Center, or Referral:** The sales associate must call the issuer for authorization. Call the Voice Authorization Center at 1-800-944-1111 and follow the operator's instructions. Inform the cardholder that phone authorization is required to protect him or her against fraud.
- **Pickup:** The issuer requires the sales associate to keep the card. The merchant should try to retain the card; however, merchants should never put themselves in any danger.
- **Mismatch:** When using the available fraud-control features on a POS device (see "Available Fraud Controls" above), if the four digits entered do not match the information embedded on the card's magnetic stripe, the 'Mismatch' message displays. Start the transaction again, re-enter the four digits as requested. If the message displays again, the card is potentially counterfeit or fraudulent. In this case, follow Code 10 procedures by calling the Voice Authorization Center at 1-800-944-1111 and saying, "Code 10." Follow the instructions the operator gives over the telephone and don't accept the card as a form of payment.



1: Card-Present Transactions

Print the Sales Draft

Follow these steps if USING a printer:

- ▶ Have the cardholder sign the printer-generated sales draft.
- ▶ Compare the signature on the sales draft with the signature on the back of the card. Make sure that the signatures match. If this is a NSR or QPS transaction, no signature is required.
- ▶ If the signatures match, hand the cardholder the customer copy of the sales draft and return the card. The sale is now complete.
- ▶ If the signature looks suspicious, or if the merchant is suspicious about the card, call the Voice Authorization Center at 1.800.944.1111 and request a Code 10 authorization. The merchant must also take a manual imprint of the transaction.
- ▶ If the response to the authorization is CALL, call the Voice Authorization Center number at 1.800.944.1111. When the authorization operator answers, give the following information:
 - Merchant identification number (MID)
 - Cardholder account number
 - Amount of sale (dollars and cents)
 - Expiration date on the card
- ▶ Write the authorization code on the provided space on the sales draft.

Follow these steps if NOT USING a printer:

- ▶ Place the card face up on the imprinter. Make sure the card is properly positioned so that all information embossed on the card and the merchant identification plate are legible on the sales draft.
- ▶ Place the sales draft face up over the card in the imprinter, making sure that the imprinter's guides hold the draft properly.
- ▶ Move the imprinter handle completely across the draft with a quick, firm motion and return the handle to its original position.
- ▶ Be sure that the imprinted information is legible on ALL copies of the draft. If information is illegible, attempt the imprint again on a new draft copy and destroy the old one.
- ▶ Truncation mandates – where the full card account number isn't visible – don't apply to manual card imprints, only electronically printed cardholder receipts.
- ▶ Use a ballpoint pen (not a soft felt tip), to enter the date, description of merchandise or services, sales amount, approval code, tax, total and sales associate's initials on the draft
- ▶ Have the cardholder sign the sales draft.
- ▶ Compare the signature on the sales draft with the signature on the back of the card. They must match.
- ▶ Hand the cardholder the customer copy of the sales draft and return the card. The sale is now complete.

All transactions authorized by phone need to be re-entered into the POS device to be electronically deposited. Follow the instructions in the POS device manual for Force transactions. Remember to manually imprint and fully complete a sales slip for all sales that are forced into the POS device. If the POS device is out of order, contact the Help Desk.



If an electronic swipe of the card is unsuccessful, obtain an imprint of the card on a sales draft. Complete the sales draft, including a signature, and attach a copy to the printer-generated draft for filing.

Obtain and Compare Signatures

Have the cardholder sign the draft. Compare the signatures on the card and the draft. If the two match, return the card with the copy of the draft. If they do not match ask for additional identification, such as a driver's license or another credit card and call the Voice Authorization Center for instructions.

If there is no signature, ask for (but do not store or retain) additional identification and have the cardholder sign the card and then compare the signature to a signature on the government-issued ID (such as a driver's license).

Retain a copy of the sales draft for protection against possible disputes.

Commercial Card Transaction

Retail, MOTO and electronic commerce merchants that accept a commercial card may have their POS application prompt for sales tax and customer code. Enter the actual sales tax amount (or zeroes if tax exempt) and enter the customer code provided by the customer. If the customer does not know the code, enter zeroes. If the merchant supports commercial and purchase card line-item detail, then include this information on the transaction receipt.



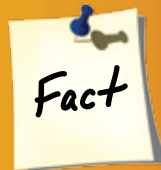
To reduce the risk of incurring a chargeback on a fraudulent card, the issuing bank requests an authorization through a voice operator. Contact Global Payments' Voice Authorization Center and speak directly to an operator. Do not use the Automated Response Unit (ARU) on these voice referral transactions.



2: 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)
- by telephone (also referred to as Telephone Order/TO)
- by fax
- over the Internet (also referred to as eCommerce)
- with commercial and purchase cards with line-item detail



Merchants cannot accept Card-Not-Present transactions unless Global Payments has agreed to process this type of transaction and such agreement is reflected in the merchant's Merchant Agreement.

Take precautions to guard against compromising data 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 Global Payments.

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

Two security tools are available to assist merchants in the detection and prevention of fraudulent activity – verification of cardholder billing address (AVS) and authentication that the card is in the customer's 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.

Note

Merchants that perform AVS as a stand-alone request may incur higher fees versus AVS with authorization.

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

2: Card-Not-Present Transactions

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 may see a reduction in fraud-related chargebacks. AMEX CID was made available to all merchants in October 2009.

MasterCard and Visa have additional tools to authenticate cardholders during electronic commerce transactions. MasterCard SecureCode™ authenticates cardholders with their issuer and Verified by Visa similarly authenticates cardholders with their issuer and merchant prior to requesting an authorization. Merchants participating in these programs may pay nominal participation fees to vendors (i.e. Cardinal Commerce); however, merchants may realize savings on their merchant discount, reduction in chargebacks and improved consumer perceptions.

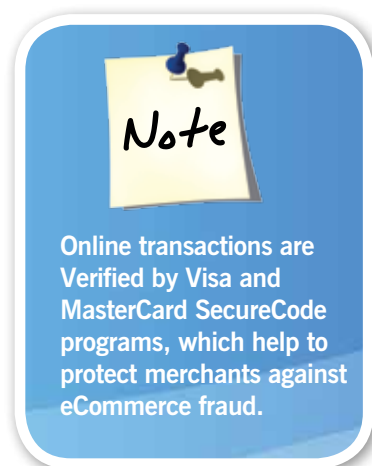
Completing Electronic Commerce Transactions

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, customers want to feel safe and secure while conducting Internet transactions. Global Payments is aware of the growing popularity of Web-based businesses and has developed flexible, secure Internet payment processing options that help merchants and their customers feel at ease.

MasterCard, Visa, American Express and Discover Operating Regulations define an electronic commerce transaction as a transaction conducted over the Internet or other network using a cardholder access device, such as a personal computer or Web-based device (i.e. phone). 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. An In Flight Terminal (IFT) may be considered under a separate category of Cardholder Activated Terminal devices.

Global Payments requires that merchants identify their electronic commerce transactions under a separate merchant number to ensure compliance with MasterCard, Visa and Discover Operating Regulations. American Express and Discover also have directed Global Payments to use separate service establishment numbers for their electronic commerce transactions.

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 Web Site and Electronic Transaction Requirements

A merchant's Web site must contain the following information:

- Merchant outlet address
- 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 the checkout screen. Policy must be displayed on checkout screen and cannot take cardholder to a separate screen.
- Consumer data privacy policy and method of transaction security used during the ordering and payment process
- Customer service contact including e-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

Transaction Receipt Requirements

A transaction receipt must contain the following information:

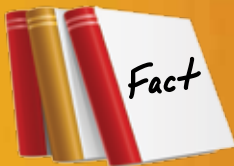
- Merchant name most recognizable to consumers
 - Doing Business As (DBA) name as used on website;
 - Merchant Universal Resource Locator (URL); or
 - Merchant name used in the Clearing Record
- Customer Service contact, including telephone number (If merchant delivers goods internationally, include 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
- Complete and accurate description of the goods or services offered
- Merchant online address
- Description of merchandise/services
- Transaction amount
- Transaction date

2: Card-Not-Present Transactions

- 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)

Completing Mail Order and Telephone Order (MOTO) Transactions

1. Obtain the cardholder's name, card account number and expiration date, and record these on the sales draft. Obtain the cardholder's billing address and zip code. (Merchants may need to provide this information when they request an authorization.)
2. Request the three-digit card authentication number (CVV2/CVC2/CID) from the signature panel (or the four-digit American Express CID number appearing on the front of the card). **Merchant retention of this authentication number is strictly prohibited. However, merchants 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 POS device. Refer to the POS device manual 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 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. Shipments to an address different from the one verified as the cardholder's may result in an increase of chargebacks.

Merchants may verify the billing address of the cardholder with the Voice Authorization Center or the cardholder's bank. Customer Care can provide the number of the cardholder's bank, if necessary.

Completing Recurring Bill Payment Transactions

When Global Payments approves a merchant for Recurring Bill Payment services, the merchant must follow the procedures set out in the MOTO section above, in the MOTO Exhibit in the back of this Guide and any written directions issued by Global Payments relating to MOTO 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 pre-determined 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
- Email 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 18 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.

2: Card-Not-Present Transactions

Other Requirements and Prohibitions for Recurring Transactions

Additional requirements for recurring transactions include the following:

- Partial payment for goods or services purchased in a single transaction is NOT allowed.
- Convenience Fees are not permitted on a recurring transaction.
- Can NOT be deposited if the cardholder has cancelled the payment arrangement.
- Can NOT 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. A new authorization is required for each recurring charge.
- The floor limit for recurring bill payments is \$0.00. Merchants must always obtain an authorization and identify recurring bill payments in the authorization request as required by MasterCard, Visa, American Express and Discover.
- Only submit authorized recurring bill payment transactions.
- Identify recurring bill payment transactions in authorization and clearing records as required by MasterCard, Visa and Discover.
- Clearing records 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.
- Use a product that supports the “bill payment indicator.”



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 preventing chargebacks.

Best Practices for Use of Convenience Fees

Card association rules prohibit merchants from billing consumers a fee for using a credit card. This is considered surcharging. The prohibition on surcharging ensures that credit cardholders are not discriminated against at the point of sale. However, discounts on cash purchases are permitted. Also, surcharging is different from convenience fees. Convenience fees may be imposed in certain cases by governments or schools for using specific alternative payment modes, such as the Internet and telephone.

The card associations have found that convenience fees are a barrier to card acceptance and the associations have established requirements regarding their use. The requirements vary by card association and the following guidelines and best practices are based on acceptance of all card brands.

A merchant that charges a convenience fee must ensure that the fee is:

- Charged for a bona fide convenience in the form of an alternative payment channel (i.e. Internet payments, IVR payments) outside the merchant's customary payment channels.
- Disclosed to the cardholder as a charge for the alternative payment channel convenience.
- Added only to a non face-to-face transaction.
- A flat or fixed amount, regardless of the value of the payment due.
- Applicable to all forms of payments accepted in the alternative payment channel, including electronic checks, ACH, etc.
- Disclosed prior to the completion of the transaction and the cardholder is given the opportunity to cancel.
- Included as a part of the total amount of the transaction.

Be aware of the potential for changes to current policy and procedures. Effective April 2005, a special Visa program was launched for registered utilities (Merchant Category Code (MCC) 4900) who affirm they will abstain from charging convenience fees associated with bill payments. If a utility merchant wishes to charge a convenience fee, it may not register for the utility program and it will receive card-present or card-not-present interchange on its Visa transactions.

MasterCard has put in place a convenience fee program for participating pre-certified government and education entities, or their third-party agents. Participants in the program will be permitted to assess a convenience fee for MasterCard transactions, whether conducted in person, Internet, phone, mail or kiosk, but not on cash, check, Automated Clearing House (ACH), and Personal Identification Number (PIN) based debit. Eligible MCC's are as follows:

2: Card-Not-Present Transactions

- MCC 8211 (Schools, Elementary and Secondary) and MCC 8220 (Colleges and Universities, Professional Schools and Junior Colleges)
- MCC 9211 (Court Costs including Alimony & Child Support) and MCC 9222 (Fines)
- MCC 9311 (Tax Payments) and MCC 9399 (Government Services—not elsewhere classified)

In the normal course of business, the card associations do not monitor other merchant fees 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.

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 (aggregators) are subject to additional requirements and require registration and interaction between Global Payments and the card association.



For merchants who offer an alternate payment channel (i.e., mail, telephone, or e-commerce) for customers to pay for goods or services, a convenience fee may be added to the transaction amount.

Example: The merchant provides utility services to its customers, and the customary way to pay is by mail or in person at the merchant's location. For the convenience of its customers, the merchant also offers a website for payments. In this example, the merchant may apply a convenience fee to payments made via the Web site.

Merchants whose payment channels are exclusively non face-to-face may NOT impose a convenience fee.

3: Card Acceptance

Best Practices for Merchant Use

Best practices in accepting credit and debit cards help in assisting and treating all customers fairly and in honoring cards without discrimination. It helps merchants to be vigilant about security. To follow best practices:

DO	DON'T
<ul style="list-style-type: none">✓ Use a POS device or third-party device 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*.	<ul style="list-style-type: none">✗ Process cash disbursement transactions unless the merchant is a financial institution approved to do so through its merchant account.
<ul style="list-style-type: none">✓ Store all materials containing cardholder account information in a restricted/secure area.	<ul style="list-style-type: none">✗ Assign a minimum or maximum purchase amount. Merchants are permitted to set a minimum transaction threshold, not to exceed \$10, for credit card transactions only.
<ul style="list-style-type: none">✓ Limit access to sales drafts, reports or other sources of cardholder data to employees on a need-to-know basis.	<ul style="list-style-type: none">✗ Restrict bankcard use (for a sale or discounted item).
<ul style="list-style-type: none">✓ Render materials containing cardholder account information unreadable prior to discarding.	<ul style="list-style-type: none">✗ Use a bankcard to guarantee a check.
<ul style="list-style-type: none">✓ Retain legal control over cardholder transaction data and personal cardholder information if the merchant uses a third party service provider.	<ul style="list-style-type: none">✗ List a cardholder's personal information on a bankcard sales slip (unless the authorization operator requests it).
<ul style="list-style-type: none">✓ Limit access to Global Payments' systems requiring unique operator log-in and notify Global Payments immediately of staff terminations or changes.	<ul style="list-style-type: none">✗ Record CVV2/CVC2/CID on sales draft (only the one-digit result code can be recorded or retained).
<ul style="list-style-type: none">✓ Immediately notify Global Payments' Risk Management team of any suspected or confirmed loss or theft of materials or records that contain account information retained by merchant or its third party service provider.	<ul style="list-style-type: none">✗ Retain sensitive cardholder data if expressly prohibited, including complete contents of a card's magnetic stripe (subsequent to the authorization).
<ul style="list-style-type: none">✓ Immediately notify Global Payments of the use of an agent or third party service provider not identified on the Merchant Application.	<ul style="list-style-type: none">✗ Add a surcharge unless allowed by state law✗ Add a surcharge to a PayPal transaction.

*Certain states require card number and expiration date truncation on both the cardholder and merchant copies of receipts. Please be aware of your state's laws and see the Industry Initiatives section of our Web site (globalpaymentsinc.com) for more information on state and card association requirements regarding truncation.

3: Card Acceptance

(Continued) Best Practices for Merchant Use

DO	DON'T
<p>✓ Communicate these requirements to the third party service provider and/or POS device application provider and direct them to card association information, publications and or Web sites regarding safeguarding cardholder transaction data.</p>	<p>✗ Sell, transfer or disclose cardholder account information or personal information. (This information should be released only to Global Payments or Member, or as specifically required by law. If merchants want to participate in loyalty programs, the loyalty vendor must be compliant with PCI DSS requirements and registered by the acquirer with MasterCard and Visa.)</p>
<p>✓ Require third party service providers to adhere to PCI DSS, AIS, American Express and MasterCard data security requirements (available on PCI Web site).</p>	<p>✗ Deny a purchase because a cardholder refuses to provide additional identification, such as telephone number, address, social security number or driver's license.</p> <p>✗ Use any other telephone number other than the official number provided for authorization of a transaction.</p>
<p>✓ Only use service providers that are PCI DSS compliant.</p>	<p>✗ Merchants are prohibited from introducing illegal transactions into the payment system. The Member Sponsor and Global merchant acquisition policy prohibits the signing of prospective merchants that engage in illegal activities. These can include, but are not limited to, prohibitions in the following merchant markets and merchant category codes (MCCs)</p> <ul style="list-style-type: none"> • Internet Gambling • Child Pornography • Copyrighted or Trademark infringed items (i.e., "knock off" Rolex watches)
<p>✓ If merchant internal systems receive, pass or store cardholder and transaction data, ensure that:</p> <ul style="list-style-type: none"> • a working network firewall is in place • security patches are current • stored data is encrypted • anti-virus software is used • vendor supplied default passwords are NOT used • vendor payment application software in use effective July 1, 2010 is on the PCI SSC PA DSS Web site or merchant must validate PCI DSS compliance**. • validate data security compliance, if requested by Global Payments or Member. 	
<p>✓ Retain sales drafts for 18 months.</p>	
<p>✓ Display proper signage.</p>	
<p>✓ Retain sales drafts bearing the cardholder's signature. If a chargeback arises, the merchant may need to provide a signed copy of the sales draft or respond to a cardholder inquiry. Global Payments requires merchants to retain an original draft or legible copy of Visa, MasterCard and Discover transactions for 18 months from the date paid for the transaction.</p>	
<p>✓ Immediately notify Global Payments of the use of payment application software and version not identified on the Merchant Application.</p>	

**This means that existing merchants using a payment application NOT listed on the PA DSS list must either contact their vendor for an upgrade, migrate to another payment application on the validated list, or the merchant must undergo PCI DSS validation and scans and provide passing results to Global Payments.

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. Do not record private information. For merchants that must list the identifying information, write it elsewhere (such as on the merchant copy of the sales receipt or on a store invoice). Keep these pieces of information secure, not accessible to anyone. Thermal printers can further safeguard customer information since only the merchant copy of the sales draft will have the cardholder signature.

Personal Information

A merchant can request personal information from a customer when permitted by state law AND when:

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

Prohibited Transactions

Merchants who accept credit cards must be aware of prohibited transactions and the penalties that can be imposed if they complete them. A prohibited transaction is one that does not comply with the operating regulations of the Visa, MasterCard, American Express and Discover associations 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 Merchant Agreement, perhaps immediately!

Merchants must educate their staffs 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.

Never Honor a Card When:

- ▶ The customer does not have the actual card.
- ▶ The card appears to have been altered or tampered with.
- ▶ Authorization is declined or merchant is instructed to pick up the card.
- ▶ The signatures do not match.
- ▶ The merchant is suspicious – Call in a Code 10.

3: Card Acceptance

Examples of Prohibited Transactions

- Processing transactions to cover previously incurred debts, or bad debts, such as bounced checks, or payment for returned merchandise. Visa permits this practice if the existing debt transactions are identified properly and the account is not in collection.
- Processing a sale on a previously charged back transaction.
- Accepting transactions that are declined by the Voice 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 unless set up for cash back.
- 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 card and the one on the sales draft are not the same.
- Engaging in factoring (draft laundering) or accepting or depositing drafts from other banks, merchants or businesses which the merchant may own or purchase, but are not explicitly listed in the current Merchant Agreement (or supplements to it) currently on file with Global Payments. Laundering of deposit drafts will likely result in the immediate termination of the merchant's bankcard privileges.
- Depositing a sales draft twice.
- Depositing a sales draft in one or more financial institutions for payment before or after it is deposited with Global Payments.

Accepting Debit and EBT Cards

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 and the amount of the transaction is debited from the customers' checking account.

Offline (or signature-authorized) debit 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 transaction amount. This type of transaction can be made with an ATM/debit card bearing a MasterCard or Visa logo on the front.



Note

See the EBT amendment in the Exhibits section of this Guide for complete details.

When merchants offer debit as a form of payment, they are supplied a number of debit network logos, which are to be displayed at 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.

In order to offer debit as a payment option, merchants are required to follow certain other procedures 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 may not impose a separate fee as a condition for accepting the debit card.
- 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 device must be equipped with a Personal Identification Number (PIN) entry device for the cardholder to enter his or her PIN. The PIN entry device must be at or in close proximity to the POS device.
- The POS 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 for online debit. The cardholder's PIN is the electronic signature.
- The merchant may not ask cardholders to disclose their PIN.
- The debit transaction receipts must be produced by an electronic 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 18 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

Global Payments supports electronic benefits transfer (EBT) processing because of its 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. The EBT card eliminates paper processing of food stamps,

3: Card Acceptance

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.

The EBT card has dual capabilities in a retail environment. An EBT food stamp customer is able to purchase eligible food items from grocery and convenience stores. The EBT card can also be used like a debit card for cash benefits. The user can pay for goods and services, as well as receive cash back from participating merchants.

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. This also includes NO CASH BACK at the time of the original sale. If the original purchase was completed with a gift or prepaid card, then cash refunds up to \$25.00 may be permitted.

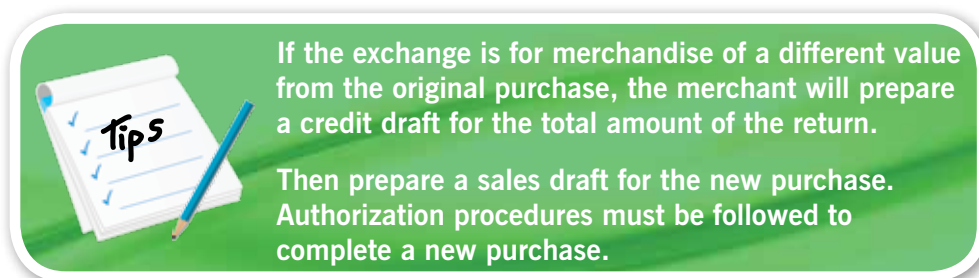
Refund policies must treat all card brands equally. The refund policy must be disclosed to the cardholder at the time of purchase, and in compliance with Applicable Law.

Any conditions or requirements that limit the cardholder's ability to return merchandise, i.e. special sale event, etc., must be clearly stated 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:

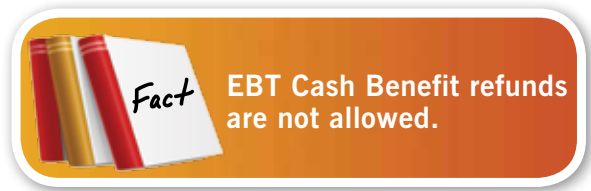
Credit Card Refunds

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 the merchant is using a printer, follow procedures for processing a credit, located in the POS device manual.
4. If the merchant is not using a printer, place the credit draft on the imprinter and imprint the merchant identification plate (and bankcard, 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.



Debit Card and EBT Food Stamps 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. Follow procedures for processing a credit, located in the POS device manual.



Debit card returns and exchanges 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.

Limited Acceptance Merchants

It is a merchant's decision to accept certain types of cards. **For more information on card acceptance policies, please see the Industry Initiatives section of the Global Payments Web site at www.globalpaymentsinc.com.**

With respect to MasterCard, Visa and Discover products, merchants may elect to accept or limit acceptance of credit cards or debit/prepaid cards, or both, by notifying Global Payments in writing. The merchant agrees to pay and the merchant's account(s) will be charged pursuant to the Merchant Agreement for any additional fees incurred as a result of the merchant's subsequent acceptance of transactions with any Visa, MasterCard or Discover product that it has elected not to accept.

Surcharging

Due to the Visa and MasterCard Antitrust Settlement, effective January 27, 2013, Visa and MasterCard have modified their Operating Regulations and Rules which will enable merchants to add a surcharge fee to consumer and commercial credit card transactions subject to acquirer notification, merchant registration (MasterCard), transaction, point-of-sale disclosure requirements and state laws regarding surcharging. The modified rules do not apply to debit transactions, including prepaid debit.

There are ten states that prohibit surcharging which supersede Visa and MasterCard Operating Regulations: California, Colorado, Connecticut, Florida, Kansas, Maine, Massachusetts, New York, Oklahoma and Texas.

For further information, please visit our Industry Initiative Homepage on our Internet Site at www.globalpaymentsinc.com

3: Card Acceptance

Service Fee

The Visa Government and Higher Education Payment Program allow participating merchants to assess cardholder fees on approved transaction types. The program allows a variable service fee on Visa consumer debit, Visa consumer credit, and Visa commercial products in card present and card not present environments. Eligible MCC's are as follows:

- Government merchants (MCC 9311-Tax; 9222-Fines; 9211-Court Costs; 9399-Miscellaneous Government Services)
- Higher education tuition and related payments (MCC 8220-College Tuition; 8244-Business; 8249-Trade Schools)



A Merchant participating in the Government and Higher Education Payment Program and that assesses a U.S. Credit Card Surcharge must not assess a Service Fee in addition to the U.S. Credit Card Surcharge.



4: 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 merchants should consider to help prevent inaccurate or fraudulent transactions.

Month-End Settlement

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

Draft Laundering or Factoring

Depositing drafts belonging to another business is in violation of the Merchant Agreement and against the law in many states. "Helping out" another merchant who offers to pay a fee or commission by having a merchant deposit this other business's MasterCard or Visa drafts 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 the merchant's bank account. Remember, the merchant who deposits another merchant's drafts is ultimately legally responsible for any problems resulting from the deposit.

Global Payments wants to help protect merchants from this dangerous fraud scheme and the potential devastating losses. Draft laundering will likely result in the termination of the merchant's card acceptance privileges. Global Payments urges its merchants to educate staff about this serious problem and report third party draft laundering propositions to Global Payments and to the U.S. Secret Service immediately.

Charge Restrictions

Merchants are able to set a minimum transaction threshold for credit card transactions only. The minimum amount must not exceed \$10.00 (a merchant could set a smaller minimum if they wish). The law also allows merchants who are federal agencies or institutions of higher education to set maximum transaction amounts on credit card transactions. Merchants should be cautioned that minimum and maximum transaction amounts do not apply to debit card transactions under this law, and setting minimum or maximum transaction amounts for debit card transactions can still result in violations of applicable rules and regulations.

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 a merchant feels strongly about compensating cash customers for the discount fee the merchant pays on charge purchases, the merchant may want to consider offering a cash discount.



Adding a surcharge to credit transactions is against the law in many states and is subject to MasterCard, Visa, Discover, and American Express rules.

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. MasterCard, Visa, American Express and Discover 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 cardholder copy of electronically printed receipts. Certain states require card number and expiration date truncation on both the cardholder and merchant copies of receipts. Please be aware of your state's laws and see the Industry Initiatives section of our Web site (globalpaymentsinc.com) for more information on state and card association requirements regarding truncation.

Keep cardholder numbers and personal information confidential. This information should be released only to the merchant bank or processor, as specifically required by law, or in response to a government request. Safeguard customers by ensuring that their confidential cardholder information is only released to authorized sources. Merchants must have written agreements with a provider supported by Global Payments for loyalty program or fraud control services.

Merchants must not request or use account number information for any purpose the cardholder did not authorize. If merchants accept other card types (American Express, Discover, JCB, etc.) they may release transaction information to those networks as required.

A merchant must not, in the event of its failure, including bankruptcy, insolvency, or other suspension of business operations, sell, transfer, purchase, provide, exchange or in any manner disclose any materials that contain cardholder and payment transaction information to another party, even in the event of failure or other suspension of business operations. The merchant must return this information to Global Payments or provide acceptable proof of destruction of this information to Global Payments.

If a merchant uses a third party provider and the third party has access to cardholder account information, then the merchant must have an agreement with the third party provider that indicates that the merchant retains 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, card association penalties for noncompliance may be assessed to the merchant (who is responsible for any penalties).

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) card validation code numbers

Listing cardholder information, such as a phone number, driver's license or social security number, on the sales draft is unnecessary and discouraged. If a merchant is suspicious that the transaction is not valid, do not hesitate to ask for additional identification – preferably a

4: Operating Guidelines

photo ID. If a merchant must list the identifying data, write it elsewhere (such as the copy of the sales receipt) rather than on the sales 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 the merchant's customers will appreciate.

Proper Display of Signage

When merchants agree to accept Visa, MasterCard, American Express or Discover, they should display the proper signage to indicate that service is available, whether at a physical address or Web site. MasterCard, Visa, American Express and Discover require clearly displayed signs at the point of sale. Use the sign and decals included in the Global Payments merchant welcome kit. Additional signage is available through Global Payments or for order on the card association Web sites.

Chargebacks

Chargebacks are previous transactions that are disputed by the cardholder or the cardholder's issuing institution. A chargeback occurs when a cardholder disputes a charge or when proper card acceptance and authorization procedures were not followed. When a merchant receives a chargeback, its deposit account is debited for the indicated amount. In addition to the chargeback, the merchant may incur a fee if it 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 can be minimized by obtaining proper authorization and adhering to correct processing procedures.

Merchant's Right to a Rebuttal

Merchants who receive notification of a chargeback 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 Customer Care for more information on rebuttal procedures.



The card associations permit the cardholder bank to collect additional fees for items that result in a chargeback. Merchants may be subject to these association chargeback fees if the merchant failed to follow card acceptance and authorization procedures and the card issuer has a valid chargeback.

Some Do's and Don'ts of Chargebacks

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

DO	DON'T
✓ Understand that the merchant assumes all responsibility for the identity of the cardholder for all types of transactions (card-present and card-not-present).	✗ Charge a cardholder before shipping the merchandise.
✓ Prepare and submit a written rebuttal within the time specified on the chargeback notification.	✗ Accept sales that are declined and if a sale is declined, do not attempt authorization a second time on a declined sale*.
✓ Accept cards where the cardholder account number is valid.	✗ Accept sales that are not authorized for the exact amount.
✓ Authorize all sales.	✗ Accept an expired card.
✓ Verify arithmetic on sales drafts.	✗ Accept a card before the effective date on a dual dated card.
✓ Charge the cardholder for the correct amount.	✗ Process a credit as a sale.
✓ Deposit the sales draft before the contractual time limit.	✗ Deposit the sales draft more than once.
✓ Credit the cardholder for the returned merchandise.	✗ Deposit an incomplete sales draft.
✓ Credit the cardholder for a canceled order.	✗ Accept a sales draft without a cardholder signature.
✓ Verify that the signature on the sales draft matches the signature on the card.	✗ Participate in a suspicious transaction.
✓ Verify the authorization code.	✗ Obtain an authorization by using multiple transaction/split sales drafts.
✓ Obtain a manual imprint, if unable to capture card data from the magnetic stripe.	✗ Accept a card where the account number obtained off the magnetic stripe does not match the account number on the draft.

*The cardholder bank may collect a fee if a merchant fails to follow card acceptance and authorization procedures.

4: Operating Guidelines

Supplies

Merchants can order all point of sale merchant supplies from Global Payments. While most orders will arrive within seven days, please allow two weeks for processing and shipping times. Cost of supplies will appear on the merchant's statement.

Customer Care

Toll-free, 24-hour customer support and voice authorization is available through Global Payments. For general inquiries, call 1-800-367-2638. For all other questions, refer to the POS device manual and merchant authorization stickers for a listing of customer care phone numbers.

Forward merchant account inquiries regarding policies to:

Global Payments Inc.
Attention: Customer Care
10705 Red Run Blvd
Owings Mills, MD 21117

Call Customer Care to Order these Additional Supplies:

- ▶ Imprinter
- ▶ Terminal
- ▶ Printer (required for EDC merchants processing debit transactions)
- ▶ PIN Pads
- ▶ MasterCard/Visa/ American Express/ Discover window decals and cash register signs
- ▶ Merchant plate
- ▶ Authorization stickers
- ▶ Transaction forms
- ▶ Envelopes
- ▶ Sales slips
- ▶ Paper
- ▶ Ribbons

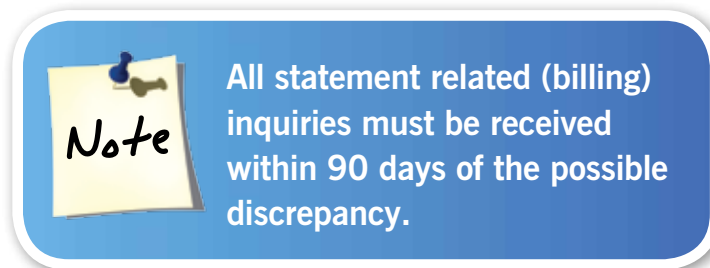
Please include the merchant number and daytime telephone number with all inquiries.

Understanding the Merchant Statement

The following section provides instructions, contact information, and a sample statement to help merchants better understand their monthly statements.

Questions About the Merchant Statement

Merchants who think the statement is incorrect, or if they need more information about a transaction on the statement, should contact Global Payments in writing via letter. Global Payments must receive notification no later than 90 days after the first bill was sent on which the error or problem appeared. Merchants can phone Global Payments but calling does not preserve the merchant's rights.



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

- Global Payments' merchant identification number (MID) and business name
- Name of the person writing the letter
- A contact telephone number
- The amount of the suspected error
- A description of the error and explanation, if possible, why the merchant believes there is an error. If necessary, describe the item in question.


Letters should be sent to:

Global Payments Inc.
10705 Red Run Blvd
Owings Mills, MD 21117

Please note that chargebacks require a response with appropriate rebuttal information within the timeframe noted on the chargeback adjustment advice. Chargebacks are not considered a billing error.

4: Operating Guidelines

Sample Merchant Statement



Merchant Statement

ABC RESTAURANT
JOHN SMITH
123 ANYWHERE ST.
CITY PROV COUNTRY PC

1	Statement Date	12/31/09
	Page	1 of 1
	Merchant Number	12345678901

GLOBAL PAYMENTS INC.

DEPOSITS 2

DAY	REF NO.	ITEMS	SALES	CREDITS	DISCOUNT	NET DEPOSIT
02	00000001231	29	\$2,185.31	\$0.00	\$0.00	\$2,185.31
03	00000001232	18	\$1,375.63	\$0.00	\$0.00	\$1,375.63
...30	00000001233	550	\$41,245.45	\$0.00	\$0.00	\$41,245.45
TOTAL		597	\$44,806.39	\$0.00	\$0.00	\$44,806.39

DEPOSIT ITEM SUMMARY

SALES :	597	DB ADJ. :	0	TOTAL :	\$0.00
CREDITS :	0	CB ADJ. :	0	TOTAL :	\$0.00
TOTAL :	597	TOTAL :	0	TOTAL :	\$0.00

SETTLEMENT / DISCOUNT 3

DESCRIPTION	ITEMS	AMOUNT	AVG TICKET	DISC RATE	ITEM RATE	FEE AMOUNT
VISA	164	\$12,139.28	\$74.02	2.08	0.00	\$252.50
VIBS	41	\$3,256.63	\$79.43	2.81	0.00	\$91.51
VDBT	144	\$10,811.52	\$75.08	1.70	0.00	\$183.80
MC	123	\$9,089.70	\$73.90	2.08	0.00	\$189.07
MCBS	26	\$2,075.32	\$79.82	2.83	0.00	\$58.73
MDBT	84	\$6,298.32	\$74.98	1.70	0.00	\$107.07
DISC	1	\$83.76	\$83.76	1.82	0.00	\$1.52
ASSESS VS	349	\$26,207.43	\$75.08	0.00	0.00	\$0.00
ASSESS MC	233	\$17,463.34	\$74.98	0.00	0.00	\$0.00
ASSESS DS	1	\$83.76	\$83.76	0.00	0.00	\$0.00
DISC NETWORK ACCESS FEE	1		\$0.00	0.00	0.02	\$0.02
TOTAL						\$884.21

SURCHARGES 4

DESCRIPTION	ITEMS	AMOUNT	FEE AMOUNT
NQS-DISCOVER REWARDS RETAIL	1	\$83.76	\$0.38
NQS-VS KEY ENTERED	10	\$733.28	\$7.33
NQSVS SIGNATURE CARD	8	\$616.92	\$6.17
NQS-VS REWARDS 2	13	\$969.24	\$9.69
NQS-MC KEY ENTERED	4	\$296.48	\$2.96
NQS- MC WORLD CARD	9	\$681.63	\$6.82
TOTAL			\$33.35

OTHER FEES 5

CARD	CHARGE	DESCRIPTION	NUMBER	RATE	FEE AMOUNT
AMEX		PER - ITEM	11	.1000	\$1.10
DISC		PER - ITEM	2	.2900	\$0.58
VISA		PER - ITEM	14	.2900	\$4.06
MC		PER - ITEM	14	.2900	\$4.06
	309	GLOBAL ATL	20	.2000	\$4.00
TOTAL OTHER FEES :					\$13.80

YOUR ACCOUNT HAS BEEN DEBITED : 6 **\$931.36**

MESSAGES

The Messages Section contains merchant information regarding services, special offers and much more.

Sample Merchant Statement Details

1 Merchant Profile

Once you become a Global Payments customer, an account profile with information about your business and merchant setup is created for you

Statement	
Statement Date	12/31/09
Page	1 of 1
Merchant Number	12345678901

2 Deposits and Item Summary

Details and summarizes your monthly sales, returns and deposit information

DEPOSITS			
ITEMS	SALES	CREDITS	DISCOUNT
29	\$2,185.31	\$0.00	\$0.00
18	\$1,375.63	\$0.00	\$0.00
550	\$41,245.45	\$0.00	\$0.00
597	\$44,806.39	\$0.00	\$0.00

DEPOSIT ITEM SUMMARY			
597		DB ADJ.	:
0		CB ADJ.	:
597		TOTAL	:

3 Discount

Volume details by major credit type and associated discount fees assessed

VISA - Visa Consumer Cards

VIBS - Visa Business Cards

VDBT - Visa Check Cards

MC - MasterCard Consumer Cards

MCBS - MasterCard Business Cards

MDBT - MasterCard Check Cards

DISC - Discover Cards

ASSESS VS - Visa assessments

ASSESS MC - MasterCard assessments

DISC NETWORK ACCESS FEE - Discover Card Access

SETTLEMENT / DISCOUNT				
DESCRIPTION	ITEMS	AMOUNT	AVG TICKET	DISC
VISA	164	\$12,139.28	\$74.02	
VIBS	41	\$3,256.63	\$79.43	
VDBT	144	\$10,811.52	\$75.08	
MC	123	\$9,089.70	\$73.90	
MCBS	26	\$2,075.32	\$79.82	
MDBT	84	\$6,298.32	\$74.98	
DISC	1	\$83.76	\$83.76	
ASSESS VS	349	\$26,207.43	\$75.08	
ASSESS MC	233	\$17,463.34	\$74.98	
ASSESS DS	1	\$83.76	\$83.76	
DISC NETWORK ACCESS FEE	1		\$0.00	

4 Surcharges

Provides transaction descriptions, item quantities, and expense adjustments charged

SURCHARGES		
DESCRIPTION	ITEMS	AMOUNT
NQS-DISCOVER REWARDS RETAIL	1	\$83.76
NQS-VS KEY ENTERED	10	\$733.28
NQS-VS SIGNATURE CARD	8	\$616.92
NQS-VS REWARDS 2	13	\$969.24
DIS-MC KEY ENTERED	4	\$296.48
NQS-MC WORLD CARD	9	\$681.63

TOTAL		OTHER FEES	
CARD	CHARGE	DESCRIPTION	NUMBER
AMEX		PER - ITEM	11
DISC		PER - ITEM	2
VISA		PER - ITEM	11

5 Other Fees

Presents a breakdown of other fees charged for services, such as statement, settlement, non-bankcard, etc.

EDITED :	
MESSAGES	
Information regarding services, special offers and much more	

6 Messages

Contains important information for your business, such as updates to services and special offers

Please note:

As part of your customized statement, only those statement sections reflecting your activity will appear.

This statement is a sample only. Actual statements may vary from sample.

5: Preventing Fraud

Global Payments, as its merchants' advocate, uses a sophisticated fraud detection system that monitors card transactions and authorizations. This fraud detection system is one way Global Payments assists in protecting merchants' businesses. Reading and complying with the standards and the policies in this guide are a merchant's best defense against fraud, while helping the merchant remain in compliance with the Merchant Agreement.

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

Global Payments' commitment to providing security for electronic transactions helps both merchants and their 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.

New MasterCard, Visa and Discover Internet transaction security initiatives offer protection against fraud.

Follow the guidelines in the eCommerce/Internet Services addendum section in the back of this Guide.

Take Charge of Fraud

Fraud costs merchants millions of dollars a year through chargebacks. For example, some fraudsters, appearing to be legitimate customers, take both the merchant copy and customer copy of the sales slip after they have signed it. When they receive their credit card statement, they dispute the charge. Since the merchant has no record of the transaction (both copies of the sales receipt are missing), the issuer credits the full amount to the consumer and the merchant loses money.

There are steps merchants can take to prevent chargebacks and fraud from occurring. Here are some examples based on the card processing method used:

Processing Transactions Manually with an Imprinter

- For merchants who process transactions manually or use IVR/TTC, always take an imprint of the card every time a purchase is made with a credit card.
- Be sure to use TTC or call for authorization for every credit card transaction.
- Make sure to neatly print the sales draft so that it is clear and easy to read.
- Write or imprint the merchant number on the draft.
- Have the customer sign the receipt and verify that this signature matches the one on the back of the card.

- Don't divide one purchase into more than one sales draft.
- Do not change or alter the sales draft after the customer has signed it. If there is a dispute, the customer's copy is treated as correct.
- If the customer cancels a transaction, take the required steps to stop, reverse or stop the billing immediately.
- Be sure to display the return policy at the point of sale and on the sales slip; remember, it is the merchant's responsibility to inform customers of this policy.
- Maintain a well-trained staff and ensure that they follow check-out procedures correctly.
- Save all copies of sales drafts in case of future disputes.

Processing Transactions through an Electronic Point-of-Sale Device

- Be sure to always swipe the card through an electronic point-of-sale device whenever possible. Keying cardholder information increases exposure to chargebacks and costs more on interchange.
- Be certain the return policy is stated clearly on all materials or receipts.
- Keep point-of-sale equipment clean and operating efficiently.
- Merchants who have an internal or external PIN Pad should promote customers to use their PIN at the point of sale. It may be less costly than a credit card transaction in addition to being safer, as there is no cardholder signature to obtain and the PIN is used to authenticate the cardholder.

Phone Fraud

Phone fraud uses the phone to swindle merchandise from retailers. Most of the time, the criminal phones 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 asks the clerk to put the charges on his credit card and assures the clerk that a courier will 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 present. It is safest to stick to the rules in these situations:

- Avoid taking credit card numbers over the phone, if possible.
- Reject a credit card that is not in the possession of its lawful owner.

5: Preventing Fraud

Mail and Telephone Orders

- If possible, establish the customer's identity by writing his or her name, address, credit card number and expiration date on the sales draft.
- Be sure to obtain an authorization for every sales transaction.
- For orders over the phone, fax, Internet or by mail, only ship items to permanent addresses. Steer clear of post office boxes, hotel lobbies or freight forwarders.
- Always send a copy of the sales draft and order form to the customer, either when the product is ordered or when it is shipped, and be sure to maintain copies.

Protecting eBusiness

Internet merchants should be just as aware of the risks of fraud as traditional merchants and should consider ways to prevent fraud.

For merchants creating or operating an online store, be sure to learn about security risks by assessing the company's shopping cart procedures, securing online transactions and letting customers know that Web site transactions are safe.

In addition, here are some key ways to prevent Internet fraud:

- Post purchase policies on the Web site where customers can see them clearly.
- Start by taking a few extra steps to confirm each order and reject orders that leave out important information.
- Be careful when dealing with orders that have different "ship to" and "bill to" addresses.
- Avoid shipping to post office boxes, hotel lobbies or other addresses that are not permanent, as these addresses can be harder to trace later.
- Pay extra attention to orders that are larger than usual orders, as well as international orders, especially if express shipping is requested.
- Note the customer's email address.
- Be sure that each transaction is authorized correctly and that proper procedures are followed.
- Do not accept other merchants' requests to deposit their receipts through the company's account. If any items are charged back, the merchant who deposits them is responsible for them.
- When skeptical about an order, call the customer to confirm.

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 strip of a credit or debit 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 the loss of millions of dollars.

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

Don't Be Intimidated

Be aware of the customer who attempts to distract the cashier by causing a fuss at the register so that the purchase is rushed, which may lead to an improper or incomplete check out process. The customer may say that the card can't be read by the POS device, insisting that the sales associate key the cardholder information manually. In such instances, customers have also been known to complain about the service, length of the line or may even demand to see a manager. This type of fraudster will do anything to keep the cashier's attention off the authorization of the credit card.

In such a tense atmosphere, the cashier is 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 Global Payments. Never call a telephone number given by the cardholder for authorization.

Don't be intimidated by these customers. Follow standard procedures to authorize the card. In such instances, the merchant may not be losing a sale by making the impatient customer wait, but saving the 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 a thief damages the card on purpose so merchants are forced to manually enter the number in the POS device. Fraudulent cards are often damaged in order to bypass the antifraud features that are placed on them – the magnetic strip cannot be swiped and transmitted for verification and authorization.

For merchants with a POS device, swipe every card – no matter how damaged or worn. Be wary of customers who say that their card can't be read. If the card is damaged and the merchant has to key the cardholder data, make an imprint of the card. If the card is severely damaged, simply ask for another form of payment.

Borrowed Cards

Beware of people using letters of authorization for use of a credit card. Under no circumstances are these letters an acceptable form of verification or authorization. Friends, co-workers and spouses are not permitted to borrow each other's cards. Children cannot borrow their parents' cards. The only person who should present a card 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.

Disposal of Important Information

Thieves look in 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.

Recognize materials that may contain private information and dispose of them properly. Destroy any documents that have any personal information with a paper shredder before declaring them trash. Protecting customers and the merchant's own business is worth a few extra seconds.

The POS Device Repair Scam

One of the most popular and most effective ways for thieves to lift confidential information is to inform the merchant that the POS terminal needs to be repaired – offsite. The thieves then replace the broken POS device with a functioning loaner. Once the loaner is in place, all of the information scanned through this loaner device is recorded and now available to the crooks. These criminals often pretend to work for POS companies or say that they are attending to other official business. Any attempt to repair a POS device should be reported immediately by calling the Global Payments' Help Desk. The Help Desk will check to see if there is a replacement request on file.

Fraudulent Returns

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 employees take the necessary steps to ensure this doesn't happen. Global Payments' POS devices can limit access to returns by requiring the use of passwords. (See the appropriate POS device documentation.)

- Keep POS device passwords confidential and stored in a safe place.
- Change passwords often to protect the business in the event someone does get into the system.
- Don't share POS devices.
- Make sure to follow proper shut-down procedures.
- Keep a daily record of balances to identify a problem as soon as it occurs.

International Credit Cards

As with all cards, 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 POS device 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.

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 utmost attention.

Counterfeit Cards

Stolen and counterfeit cards are a huge problem for merchants and credit card issuers alike. With technology available to them, counterfeiters are able to reproduce false cards that are high quality, even without the original. All they 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. The card association rules prohibit retention of magnetic-stripe or card authentication numbers (CVV2/CVC2/CID) by merchants or their third-party terminal providers because this information could be used to counterfeit cards. Merchants must protect their business by teaching their staff to recognize the signs of a false card.

Don't Hesitate! Call In a Code 10

If a merchant ever has doubts about something – a fraudulent card, a signature or even a customer's behavior – call in a Code 10. With a Code 10, merchants can call for an authorization without the customer becoming suspicious.

After dialing the Voice Authorization Center, inform the operator of a Code 10. The operator will put the merchant through to the correct person, who will ask 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 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 a merchant feels a transaction may not be legitimate, even if the transaction is approved or if the customer had already left the premises.

When to Call in a Code 10:

- ▶ When embossing on the card is illegible.
- ▶ When 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 POS device.
- ▶ When there is no Bank Identification Number (BIN) above or below the first four digits.
- ▶ When the name on the card does not match the signature or there is a misspelling.
- ▶ When holograms are not clear or the picture in the hologram does not move.
- ▶ When the card does not have an expiration date.
- ▶ When the card does not start with the correct numeric digit – all Visa cards should start with the number four, all MasterCard cards with the number five, all Discover cards with the number six, and American Express cards with the number three.
- ▶ 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 POS device match.
- ▶ If the message is other than "approved" or "declined."

Defeating Fraud Helps Merchants and Their Customers

Whether it's a different twist on an old scam or a new scam, there will always be a threat of fraud. If merchants and staff are well prepared with the skills to recognize suspicious transactions and know how to correct the situation, everyone will be more aware of fraud and prepared for it.

Take the extra steps to stop fraud before it starts. After all, it's the merchant – not the consumer – that stands to lose the most from credit card fraud. The most important thing merchants can do is stay educated on how fraud occurs, and then follow standard procedures and processes in a suspicious situation. By following the information in this guide and working together, we increase the chances of successfully protecting businesses against fraud!

Payment Card Industry Security Standards Council (PCI SSC)

The PCI SSC is the membership organization responsible for three important security standards related to safeguarding payment transaction data.

- PCI DSS – Payment Card Industry Data Security Standard
- PA DSS – Payment Application Data Security Standard
- POS PED – Point of Sale PIN Entry Device Standard

All parties involved in payment card acceptance must safeguard payment transaction data and comply with the applicable standard(s). If a system with payment card information is hacked or stolen, then the compromised party must take steps to report the data security breach and work with forensics investigators, law enforcement, merchant acquiring staff and others to report findings. The best defense is to implement data security operating policies, limit stored payment card data, and safeguard data that is necessary.

PCI DSS Program for Level 4 Merchants

To demonstrate our level of commitment, Global Payments has engaged SecurityMetrics, a Qualified Security Assessor (QSA) to help Level 4 Merchants determine their risk and provide direction to solutions. Merchants that have not validated PCI Compliance within 60 days from the date of their merchant agreement may be assessed monthly non-compliance fees of \$50.00 until validation is complete. For further information regarding the program, please visit us at http://www.globalpaymentsinc.com/USA/customerSupport/industryInit/PCI_DSS_Program.html

The Digital Dozen

The Cardholder Information Security Program (CISP) from Visa and site data protection from MasterCard (also known as Payment Card Industry Security Standards Council – PCI SSC) provide a list of best practices and other tips. Called the Digital Dozen, these twelve controls help merchants remain in compliance with card acceptance agreements when accepting payments over the Internet.

5: Preventing Fraud

Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a working network firewall.2. Keep security patches current.
Protect Cardholder Data	<ol style="list-style-type: none">3. Encrypt stored data.4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Always use updated anti-virus software.6. Restrict access to data to a “need to know” basis.
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Assign a unique ID to each user.8. Track access to the data by the unique ID.9. Never use vendor-supplied defaults as passwords or other security features.
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Test the security system and processes regularly.11. Maintain a security policy for employees and contractors.
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Restrict physical access to cardholder information.

6: Spotting Counterfeit/Altered Cards

Knowing the distinctive qualities of MasterCard, Visa, American Express and Discover credit cards can help detect counterfeit or altered cards.

Color

Check the card for discoloration or an uneven feel. Edges should be smooth.

Embossing

Confirm that the embossing of the account number and the name is even in size and spacing and that the card has not been ironed and re-embossed. Check the valid dates to see that they have not been altered to extend the term of an expired card.

The main card association embossing numbering is as follows:

American Express: Starts with 3

Visa: Starts with 4

MasterCard: Starts with 5

Discover: Starts with 6

For MasterCard, Visa and Discover, the first four digits of the card number correspond to a small number printed on the card face just above/below the account number.

Signature Panel

The signature panel is printed with a colored MasterCard, Visa or Discover background pattern. It should be smooth to the touch and should not show evidence of tampering. The panel should be signed and the signature should correspond to the signature on the sales draft. All or a portion (last four digits) of the account number and card authentication (CVC2 or CVV2) are printed. Only the person whose name is embossed on a MasterCard, Visa, Discover or American Express credit card is entitled to use it.

Hologram

The hologram is a three-dimensional foil image put on the card that helps deter counterfeiting. The foil material can be gold or silver and the image should reflect light and change as the card rotates.

The Visa hologram appears to be a dove in flight.

MasterCard's newest hologram is called the MC Micro Globes. It shows two-dimensional rings made up of repeated MC. The three-dimensional globes consist of high-resolution texture mapping of continents onto black spheres. The word MasterCard is distinguishably micro-printed in the background of the hologram in two alternating colors. A hidden image is placed at a specific angle in the hologram during the manufacturing process.

6: Spotting Counterfeit/Altered Cards

MasterCard Formats

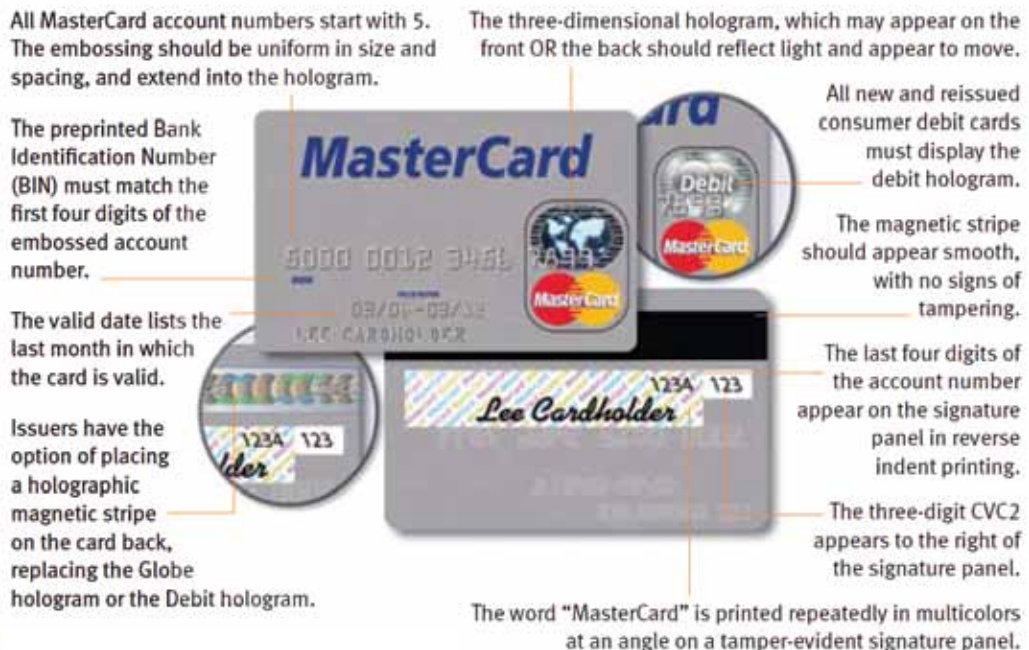
The same basic design is used for all MasterCard cards. Until all cards are replaced by the new format, merchants may see the two previous MasterCard card formats. Cards may be any color or even feature a background pattern or a photograph. Regardless of the card design presented, check the signature and other card features for validity.

Security Features

The following features appear on MasterCard cards:

- The unique security character, embossed on the lower right portion of the card front, is the signal that the following two security features should be present on the card:
 - A small account number (last four digits or all 16 digits) with a three-digit card authentication code (CVC2) printed on the signature panel in reverse italic, slightly indented characters.
 - An encoded account verification number (CVC1) programmed into the magnetic stripe, which will correspond to and verify the number, which is indent-printed on the signature panel.

MasterCard® Card Identification Features



Visa Card Formats

Every Visa card is designed with special security elements to deter counterfeiting and alteration. When presented with a Visa Classic, Visa Gold (Premier) or Visa Business Card, look for the security features below.

Security Features

The following features are required for all Visa cards and must appear on all cards:

- An embossed, stylized V beside the “good thru” date
- Micro-printing around the Visa logo
- The issuing bank identification number embossed in the first four card numbers. This bank ID number is also printed directly below the first four card numbers.

Visa® Card Identification Features

The **Signature Panel** should be white with the word “VISA” repeated in a diagonal pattern in blue and gold print. The card account number should be printed in the panel.

The words “Authorized Signature” and “Not Valid Unless Signed” must appear above, below, or beside the signature panel.

If someone has tried to erase the signature panel, the word “VOID” will be displayed.

The **magnetic stripe** is encoded with the card’s account number, expiration date, and other identifying information.

Card Verification Value (CVV2) is a three-digit code that appears on the signature panel. Portions of the account number may also be present on the signature panel. CVV2 is used primarily in card-absent transactions to verify that the customer is in possession of a valid Visa card at the time of the sale.

Embossed/Printed Account Number begins with 4. All digits must be clear, even, and the same size/shape. If a card has been re-embossed, the numbers may appear fuzzy. As a general rule of thumb, always check the hologram. It is easier to spot a re-embossed number there.

Flying Dove Hologram should appear to be three-dimensional and appear to move when the card is tilted back and forth.

Visa Logo should have micro-printing around the border. The fine print is barely readable without magnification.

Four-Digit Number must be printed directly below the embossed account number. This printed number must match exactly with the first four digits of the account number.

“Good Thru” (or “Valid Thru”) Date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the “Good Thru” date, the card has expired.

Ultraviolet-Sensitive Dove is visible in the face of the card when the card is placed under an ultraviolet light.

Flying “V” is an embossed security character beside the “Good Thru” date. This character is not a required security feature and may or may not appear on the card.

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

6: Spotting Counterfeit/Altered Cards

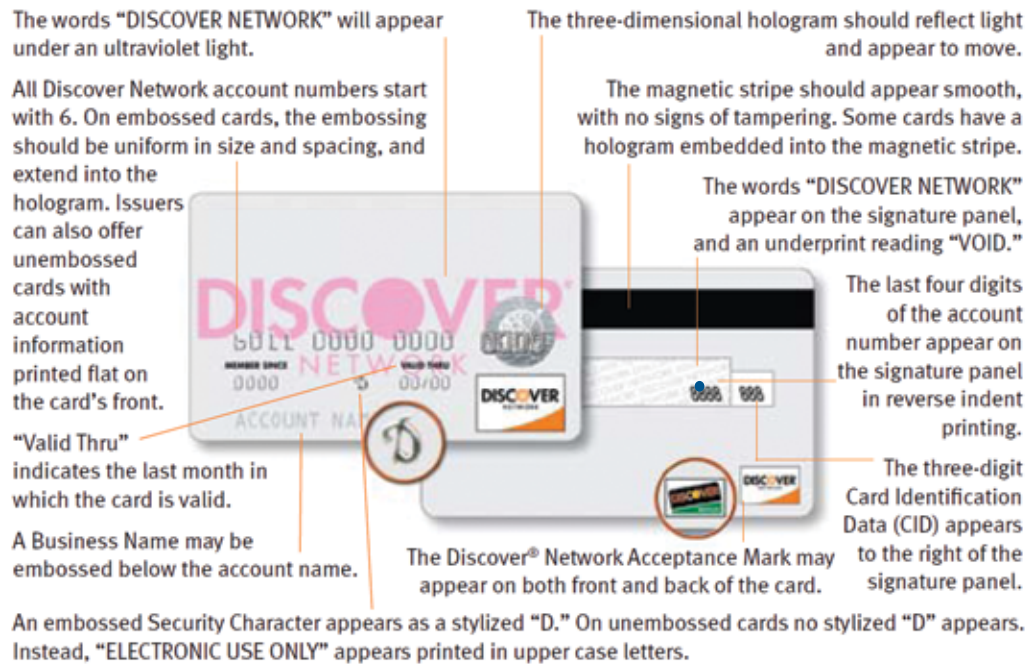
Discover Card Formats

All valid standard rectangular plastic cards bearing the Discover Network acceptance mark or the Discover/NOVUS acceptance mark include the following common characteristics and distinctive features; however, please note that valid cards may not always be rectangular in shape (e.g., Discover 2GO® Card). Additional cards on the Discover Network include JCB and China Unionpay. These cards do not contain the Discover Network acceptance mark.

Security Features

- Card numbers consist of at least 16 digits embossed on the front of the card.
- The embossed numbers in the card number should be clear and uniform in size and spacing within groupings.
- The embossed expiration date, if present, appears in a mm/yy format and indicates the last month in which the card is valid.
- The card contains a magnetic stripe.
- Depending on the issuance date of the card, the word DISCOVER or DISCOVER NETWORK will appear in ultraviolet ink on the front of the card when it is held under an ultraviolet light (Discover Cards only; this does not include JCB or China Unionpay).
- An underprint of “void” on the signature panel becomes visible if erasure of the signature is attempted.
- The card number or the portion of the card number displayed on the signature panel on the back of the card should match the number embossed on the front of the card and appear in reverse indent printing.
- The card number on the back of the card is followed by the card identification data (“CID”).
- An overprint on the signature panel reads Discover Network. On some cards, the overprint may display the name of the card (i.e., Discover, Discover 2GO, Discover Platinum).
- A contactless icon may appear on the back of a standard rectangular plastic card indicating the card can be used to conduct contactless card transactions.

Discover® Network Card Identification Features



JCB Card Formats

All Cards bearing the JCB mark include common characteristics and distinctive features listed below.

Security Features

- Card Numbers are made up of 16 digits, starting with '35,' embossed or printed on the front of the card.
- Embossed digits on the card should be clear and uniform in size and spacing within groupings.
- The cardholder name and, if applicable, business name, are embossed on the front of the card.
- The JCB Mark appears on the front of the card.
- A three-dimensional hologram image of a rising sun, rainbow and 'JCB' in micro-lettering appears on either the front or the back of the card. The hologram reflects light as it is rotated.
- The embossed expiration date appears in mm/yy, mm/yyyy or mm/dd/yy format on the front of the card and indicates the last month in which the card is valid.
- The card contains a magnetic stripe on the back of the card.
- The word 'JCB' appears in ultraviolet ink on the left bottom of the front of the card when held under an ultraviolet light.

6: Spotting Counterfeit/Altered Cards

- The first four digits of the card number match the four-digit number pre-printed just below the embossed card number on the front of the card.
- The first four digits of the card number displayed on the signature panel on the back of the card match the last four digits of the card number that appears on the front of the card.
- The last four digits of the card number on the back of the card are followed by the three-digit CID.
- An overprint on the signature panel reads 'JCB' in two colors, blue and green.
- Some cards have an embedded integrated circuit chip on the front of the card.



Some valid cards bearing the JCB mark have a printed, unembossed card number on the card. If a card sale involving a valid JCB card with an unembossed card number cannot be completed by swiping the card through the POS device, the card should not be accepted for the sale.

If the Merchant accepts a card that displays a printed, rather than embossed card number, the card number and the Merchant ID number are required to obtain a card imprint. The sale may be subject to dispute or a dispute may be resolved against the merchant for failure to obtain an imprint of security features required to be embossed on the card.

American Express Card Formats

American Express has rectangular plastic cards bearing the American Express name. All cards include some basic features that are outlined below.

Security Features

- The letters "AMEX" and a phosphorescent logo in the Centurion portrait are visible under an ultraviolet light.
- Preprinted (non-embossed) card identification number (CID) should always appear above the account number.
- Expiration date.
- All American Express account numbers start with 3.
- Embossing should be clear and uniform in size and spacing. The number on the front and back of the card, plus the one printed on the sales receipt, should all match.
- With this statement on the card, American Express reserves the right to "pick up" the card at any time.

- Some cards have a hologram of the American Express image embedded into the magnetic stripe.
- The signature on the back of the card should match the customer's signature on the receipt.
- The signature panel is tamper-evident.

American Express® Card Identification Features

The letters "AMEX" and a phosphorescence in the Centurion portrait are visible under an ultraviolet light.

Preprinted (non-embossed) Card Identification Number (CID) should always appear above the account number.

Do not accept a card after the expiration date.

Only the person whose name is embossed on an American Express Card is entitled to use it.

All American Express account numbers start with 3. Embossing should be clear and uniform in size and spacing. The number on the front and back of the card, plus the one printed on the sales receipt should all match.

With this statement on the card, American Express reserves the right to "pick up" the card at any time.

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

The signature on the back of the card should match the customer's signature on the receipt. The signature panel is tamper-evident.



PayPal In-Store Checkout Payment Card Formats

PayPal has introduced the PayPal In-Store Checkout Payment Cards. These PayPal Payment Cards will create a similar safe PayPal environment that allows consumers to pay without sharing financial information, with the ability to pay using a number of options. These cards are unembossed with two-color marks or a grayscale mark when necessary and a PayPal-provided acceptance mark.

Security Features

- Verify PayPal Payment Card characteristics and PayPal Marks for Transactions
- Verify the signature on the back of the PayPal Payment Card
- If the PayPal Payment Card is unsigned, the Merchant may request a government-issued photo ID and request the PayPal Account Holder to add his/her signature to the signature panel located on the back of the PayPal Payment Card.

6: Spotting Counterfeit/Altered Cards

- PayPal Account Holder name
- Last 4 digits of the Account Number printed on the PayPal Payment Card
- Valid thru mm/yy date
- Tamper proof signature panel



Pick Up Card Procedures

If a merchant receives a pick up card response, the merchant is eligible for a cash reward from Global Payments. Simply cut the card in half directly through the entire account number, place the card in an envelope along with the name of the person who retained the card, merchant number, date of pick up and address and mail it to:

Global Payments Inc.
Settlements
10705 Red Run Blvd.
Owings Mills, MD 21117



Exhibits and Addendums

Exhibit A: EBT Card Services Agreement

1. Agreement to Issue Benefits

Global Payments Inc. (“Global Payments”) offers electronic interfaces to Electronic Benefits Transfer (“EBT”) networks for the processing of cash payments or credits to or for the benefit of benefit recipients (“Recipients”). EBT Card services may be added to the Merchant Service Agreement, provided that MERCHANT agrees to comply with the Merchant Service Agreement as amended by the terms and conditions of this Exhibit, and further provided that MERCHANT has been authorized by Global to issue EBT benefits to Recipients in one of the following categories:

- Cash Benefits Only
 - Food Stamp Benefits Only
 - Food Stamp and Cash Benefits
- a. Global Payments will provide settlement and switching services for various Point-of-Sale transactions initiated through MERCHANT (the “Services”) for the authorization of the issuance of the United States Department of Agriculture, Food and Nutrition Services (“FNS”) food stamp benefits (“FS Benefits”) and/or government delivered cash assistance benefits (“Cash Benefits;” and with FS Benefits, “Benefits”) to Recipients through the use of a state-issued card (“EBT Card”). The Services shall be priced at Global Payments’ then-current charge for debit transactions.
 - b. MERCHANT agrees to issue Benefits during MERCHANT’s normal business hours at each of its retail locations identified to Global Payments in writing, subject to the terms and conditions hereof.
 - c. If MERCHANT has agreed to issue Cash Benefits and will provide cash back, MERCHANT agrees to maintain adequate cash on hand to issue confirmed Cash Benefits and will issue Cash Benefits to Recipients in the same manner and to the same extent cash is provided to other customers of MERCHANT. MERCHANT will not require, and will not in its advertising suggest, that any Recipient must purchase goods or services at MERCHANT’s facilities as a condition to a Cash Only from Cash Account Transaction for such Recipient, unless such condition applies to other commercial customers as well. MERCHANT will not designate special checkout lanes restricted for use by Recipients, provided that if MERCHANT designates special checkout lanes for electronic debit or credit card and/or other payment methods such as checks or other than cash, Recipients may be directed to such lanes so long as other customers are directed there as well.
 - d. MERCHANT agrees to give prompt notice to Global Payments of any planned cessation of services, or inability to comply with the terms of this Exhibit.

2. Issuance of Benefits

- a. MERCHANT agrees to issue Benefits to Recipients in accordance with the procedures specified herein and in all documentation, card acceptance guides and user guides provided to MERCHANT by Global Payments, as amended from time-to-time (the “User Guides”) and pursuant to applicable law otherwise governing the issuance of Benefits. MERCHANT will provide each recipient a receipt for each Benefit issuance. MERCHANT will be solely responsible for MERCHANT’s issuance of Benefits other than in accordance with authorizations timely received from Global Payments.
- b. MERCHANT will issue FS and/or Cash Benefits to Recipients, in accordance with the procedures set forth in the User Guides, in the amount authorized through its point-of-sale (“POS”) device, with personal identification number (“PIN”) pad and printer (“Equipment”), upon presentation by Recipient of an EBT Card and Recipient entry of a valid PIN. MERCHANT agrees that in the event of the failure of the Equipment to print Benefit issuance information as approved and validated as a legitimate transaction, MERCHANT will comply with the procedures set forth in the User Guides for authorization of Benefits in such instance.
- c. MERCHANT may elect to support the manual issuance of FS Benefits through manual benefit issuance procedures implemented during the period of time when normal benefit issuance is not possible, as described in the User Guides. MERCHANT will manually issue Benefits, in accordance with the policies set forth in the User Guides and in the amount authorized through Global, to Recipients at no cost to the Recipients upon presentation by Recipient of his/her EBT Card. The following limitations will apply to manual issuance of FS Benefits by MERCHANT:
 - (i) An authorization number for the amount of the purchase must be received from the EBT Service Provider via telephone by MERCHANT within twenty-four hours of the transaction.
 - (ii) Specified Recipient, clerk and sales information, including the telephone authorization number, must be entered properly and legibly on the manual sales draft.
 - (iii) The manual sales draft must be submitted to Global Payments for processing within ten (10) calendar days following the date of authorization. The manual sales draft must be cleared by an electronic transaction initiated through Global Payments.
 - (iv) In the event that, due to EBT host failure (a declared “emergency”), Benefit availability for a Recipient cannot be determined at the time MERCHANT requests authorization, the maximum authorized manual transaction and benefit encumbrance will be \$40.00 or such lesser amount as permitted by the State.

- (v) Except as specifically provided in the User Guides, MERCHANT will not be reimbursed and will be solely responsible for all manual transactions when MERCHANT fails to obtain an authorization number from the EBT Service Provider within twenty-four (24) hours of the transaction and prior to the submission of the manual sales draft, or otherwise fails to process the manual transaction in accordance with the User Guides.
 - (vi) If MERCHANT has not received an authorization number in accordance with paragraph 2(c)(i) above, MERCHANT may not “re-submit” a manual sales draft for payment if insufficient funds exist at the time that the manual sales draft is presented for processing and payment.
- d. MERCHANT agrees to make available such informational materials, as provided by the EBT Service Provider, as may be required by the State and by any applicable regulations pertaining to the issuance of Benefits.
 - e. MERCHANT agrees to comply with all applicable laws, rules and regulations in the performance of its obligations under this Exhibit, including without limitation, laws pertaining to delivery of services to benefit recipients and benefit recipient confidentiality, and the federal Civil Rights Act of 1964, Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, Clean Air Act, Clean Water Act, Energy Policy and Conservation Act, Immigration Reform and Control Act of 1986, and regulations issued by the Department of Agriculture pertaining to Food Stamp Program.
 - f. MERCHANT agrees to comply with the procedures set forth in the User Guides as well as the rules and regulations of all applicable EBT networks as amended from time-to-time as necessary (collectively, the “Rules”), including but not limited to the Quest Operating Rules issued by the National Automated Clearing House Association as approved by the Financial Management Service of the U.S. Treasury Department, and other such rules and regulations as may be applicable to the issuance of Benefits by MERCHANT hereunder. Unless otherwise defined herein, all capitalized terms shall have the meanings ascribed them in the Rules. MERCHANT agrees to comply with all additional procedures specified by the State, as defined in paragraph 11(c) hereto, regarding lost EBT Cards, forgotten PINs, discrepancies in benefits authorized and similar matters by providing Recipients with information such as telephone numbers and addresses of the State or other appropriate agencies.
 - g. MERCHANT will not accept any EBT Card for any purpose other than the issuance of Benefits, including without limitation acceptance of any EBT Card as security for repayment of any Recipient obligation to MERCHANT. In the event of any violation of this provision, MERCHANT will be obligated to reimburse the State for any Benefits unlawfully received by either Recipient or MERCHANT to the extent permitted by law.

3. Issuance Records

- a. MERCHANT will be furnished instructions concerning EBT-related records to be made and kept. Such records shall be of a type kept by a merchant in the normal course of its business. MERCHANT shall maintain manual sales drafts for a period not less than that set forth in paragraph 3(d) hereof.
- b. MERCHANT agrees to separately maintain such EBT-related records as may be reasonably requested or required by the State or its EBT Service Provider and to promptly make such records available for audit upon request to representatives of the State, its EBT Service Provider, or other authorized State or Federal government agency during normal business hours.
- c. To assure compliance with this Exhibit, the State, its EBT Service Provider, or other authorized State or Federal government agency will at all times, upon advance notice except in the case of suspected fraud or other similar activity, have the right to enter MERCHANT's premises, during normal business hours, to inspect or evaluate MERCHANT's performance under this Exhibit, or to obtain any other information required to be provided by MERCHANT or otherwise related to this Exhibit.
- d. MERCHANT agrees to maintain and preserve such records at all times while this Exhibit remains in effect and for a period of three (3) years following Benefit issuance, or for such additional period as applicable regulations may require. Records involving matters in litigation will be kept for a period of not less than three (3) years following the termination of the litigation. Copies of any documents in media other than paper (e.g., microfilm, etc.) related to this Exhibit may be substituted for the originals to the extent permitted under applicable law, and provided that legible paper copies can be reproduced within a reasonable time following written notice to MERCHANT.

4. Training

MERCHANT will be furnished necessary and reasonable training in policies and procedures. MERCHANT agrees to cooperate and to permit its employees to receive such training at such times as is reasonably mutually convenient to the parties.

5. Reimbursement of Merchant for Issuances

- a. Settlement for MERCHANT Benefits disbursements in the form of credit for food purchases or cash, for Benefit issuances to Recipients pursuant to this Exhibit, and settlement for other transactions as permitted in accordance with the Rules will be made by credit or debit of funds to MERCHANT's designated account, in accordance with the terms of the Agreement, including but not limited to any transfers to or from such account as may be required to correct any erroneous or unauthorized transfers or issuances. MERCHANT hereby acknowledges and agrees that its authorization of such transfers in accordance with the terms of the Agreement likewise extends to the EBT services provided under this Exhibit. Such authorization shall remain in effect until

withdrawn by MERCHANT upon written notice to the State or its EBT Service Provider and the State and its financial service provider will have had a reasonable time to act upon such written notice.

- b. Credit or debit to MERCHANT's designated account will be made the next business day, but no later than two (2) business days, following receipt by the State's EBT Service Provider of MERCHANT's end-of-day POS settlement information. Settlement information received after the State's EBT Service Provider's processing deadline, as stated in the User Guides, will be processed for credit or debit the following business day (credit or debit to be made no later than two (2) business days after processing). Such credit or debit will be by Automated Clearing House credit or debit.
- c. In the event that the credit received by MERCHANT for issuances is less than MERCHANT believes is otherwise due, MERCHANT shall promptly notify Global Payments and the State's EBT Service Provider of the discrepancy; the State's EBT Service Provider and MERCHANT and/or Global Payments shall compare records to determine the source of such discrepancy. The State's EBT Service Provider and MERCHANT and/or Global Payments will negotiate in good faith to resolve any discrepancies in accordance with the Rules.

6. Required Licenses

If MERCHANT issues FS Benefits under this Exhibit, MERCHANT represents and warrants to Global that MERCHANT is an FNS authorized merchant and is not currently suspended, disqualified or withdrawn by FNS. MERCHANT agrees to secure and maintain at its own expense all necessary licenses, permits, franchises, or other authorities required to lawfully effect the issuance and distribution of Benefits under this Exhibit, including without limitation, any applicable franchise tax certificate and non-governmental contractor's certificate, and covenants that MERCHANT will not issue Benefits at any time during which MERCHANT is not in compliance with the requirements of any applicable law.

7. Term and Termination

- a. If MERCHANT is disqualified or withdrawn from the FS Program, MERCHANT's authority to issue FS Benefits will be terminated contemporaneously therewith. Such disqualification or withdrawal will be deemed a breach of this Exhibit with respect to MERCHANT's authority to issue Cash Benefits and Global shall have the right to immediately terminate its provision of Services hereunder.
- b. With respect to the issuance of Cash Benefits only, MERCHANT's authority to issue Cash Benefits may be suspended or terminated immediately by Global, the State or its EBT Service Provider, in its sole discretion, effective upon delivery of a notice of suspension or termination specifying the reasons for such suspension or termination if there shall be (i) any suspension, injunction, cessation, or termination of the EBT Service Provider's authority to provide EBT Services to the State; (ii) failure by MERCHANT, upon not less

than thirty (30) days prior written notice, to cure any breach by MERCHANT of the provisions of these terms and conditions, including without limitation, MERCHANT's failure to support the issuance of Benefits during MERCHANT's normal business hours consistent with MERCHANT's normal business practices, MERCHANT's failure to comply with issuance procedures, MERCHANT's impermissible acceptance of an EBT Card, or MERCHANT's disqualification or withdrawal from the FS Program; or (iii) based on Global Payments', the State's or its EBT Service Provider's investigation of the relevant facts, evidence that MERCHANT or any of its agents or employees is committing, participating in, or has knowledge of fraud or theft in connection with the dispensing of Benefits. In the event that MERCHANT fails to cure any breach as set forth above, MERCHANT may appeal such suspension or termination to the State for determination in its sole discretion.

- c. MERCHANT may, in its sole discretion, suspend or terminate this Exhibit and its authority to issue Benefits, effective upon delivery of a notice of suspension or termination specifying the reasons for such suspension or termination, for any breach of this Exhibit.
- d. With respect to the issuance of Cash Benefits only, this Exhibit may also be suspended or terminated by Global Payments, the MERCHANT, the State or its EBT Service Provider, in their sole discretion, effective upon delivery of a notice of suspension or termination specifying the reasons therefore if (i) any of them shall have commenced, or shall have commenced against it without dismissal within ninety (90) days, any case or proceeding relating to bankruptcy, insolvency or relief of debtors or seeking the appointment of a receiver, trustee or similar official, or (ii) if any of them shall make a general assignment for the benefit of creditors, or (iii) if any of them shall admit its inability to generally pay its debts as they become due.
- e. MERCHANT acknowledges that the State has the right to terminate its agreement with its EBT Service Provider at will.
- f. In the event that MERCHANT's authority to issue Benefits is suspended or terminated by the State or its EBT Service Provider, and MERCHANT successfully appeals such suspension or termination to the State or its EBT Service Provider, Global Payments shall be under no obligation to MERCHANT to reinstate this Exhibit.
- g. This Exhibit will terminate immediately in the event MERCHANT's Service Agreement with Global Payments terminates for whatever reason.
- h. All payments, accounts, documents, reports, or other matters remaining due at the suspension or termination of MERCHANT's authority to issue Benefits will be completed and delivered as though its authority were still in effect, and the obligations under paragraphs 3, 5, 7, 9 and 10 of these terms and conditions shall survive any suspension or termination.

8. Force Majeure

Neither Global Payments, the MERCHANT, the State nor the State's EBT Service Provider will be responsible under this Exhibit for errors, delays or nonperformance due to events beyond their reasonable control, including but not limited to acts of God; interruption, fluctuation or non-availability of power or communications; changes in law or regulation or other acts, orders or omissions of governmental authority compliance therewith; acts of sabotage; strikes; weather conditions; fires; floods; or explosions.

9. Confidentiality of EBT System Information

- a. All information obtained by MERCHANT through its performance under this Exhibit shall be considered confidential information. MERCHANT, its directors, officers, employees and agents will treat all such information, with particular emphasis on information relating to Recipients and applicants for Benefits, as confidential information to the extent required by the laws of the State wherein MERCHANT issues Benefits pursuant hereto, by the laws of the United States and by any regulations promulgated there under.
- b. Individually identifiable information relating to any Recipient or applicant for Benefits will be held confidential and will not be disclosed by MERCHANT, its directors, officers, employees or agents, without prior written approval of the State.
- c. The use of information obtained by MERCHANT in the performance of its duties under this Exhibit will be limited to purposes directly connected with such duties.
- d. Except as otherwise required by law, MERCHANT will promptly advise the State or its EBT Service Provider of all requests made to MERCHANT for information described in this paragraph 9.
- e. MERCHANT will be responsible for assuring that any agreement between MERCHANT, any of its directors, officers, employees or agents contains a provision which appropriately addresses the confidentiality of the class of information covered by this paragraph 9.
- f. If MERCHANT issues Benefits in more than one State pursuant to this Exhibit, the law of the State in which the Benefits were issued will apply to information arising out of that transaction. In all other instances, the laws of the State where MERCHANT's principal corporate offices are located will apply.

10. EBT Service Marks

MERCHANT will adequately display the State's service marks or other licensed marks of the applicable EBT networks (including but not limited to the Quest mark), and other materials supplied by Global Payments or the State's EBT Service Provider (collectively the "Protected Marks"), in accordance with the standards set by the State. MERCHANT will use the Protected Marks only to indicate that Benefits are issued at MERCHANT's location(s) and will not indicate that Global Payments, the State or its EBT Service Provider endorses MERCHANT's goods or services. MERCHANT's right to use such Protected Marks pursuant to this Exhibit will continue only so long as this Exhibit remains in effect or until MERCHANT is notified by Global Payments, the State or its EBT Service Provider to cease their use or display.

11. Miscellaneous

- a. **Modifications to Exhibit.** This Exhibit may be modified by Global Payments at any time upon notice to MERCHANT to comply with directions of any EBT network. In addition, if any of the terms and conditions of this Exhibit are found to conflict with Federal or State law, regulation or policy, or the Rules, such terms and conditions are subject to reasonable modification by Global Payments, the State or its EBT Service Provider to address such conflict upon ninety (90) days written notice to MERCHANT, provided that MERCHANT may, upon written notice to Global Payments, terminate this Exhibit upon receipt of notice of such modification.
- b. **Assignment.** MERCHANT agrees not to convey, assign, delegate, subcontract, novate, or otherwise transfer in any manner whatsoever any of MERCHANT's rights or obligations under this Exhibit without prior written approval of the State or its EBT Service Provider.
- c. **No Third Party Beneficiaries.** These terms and conditions do not create, and will not be construed as creating, any rights enforceable by any person not having any rights directly hereunder, except that the State and its Issuer (as defined in the Rules) will be deemed third party beneficiaries of the representations, warranties, covenants and agreements of MERCHANT hereunder.
- d. **State Action.** Nothing contained herein shall preclude the State from commencing appropriate administrative or legal action against MERCHANT or for making any referral for such action to any appropriate Federal, State, or local agency.
- e. **Reference to State.** Any references to State herein shall mean the State in which MERCHANT issues Benefits pursuant hereto. If MERCHANT issues Benefits in more than one State pursuant hereto, then the reference shall mean each such State severally, not jointly.
- f. **Order of Priority.** If any term of condition of the Agreement conflicts with or is inconsistent with any term or condition of this Exhibit, such terms and conditions of this Exhibit shall be controlling.

Exhibit B: eCommerce/Internet Services Addendum

1. You agree that all eCommerce/Internet transactions will be treated as telephone and mail order transactions as described in this Agreement and that, as the customer's card is not physically present for eCommerce/Internet transactions, you may incur a chargeback on all eCommerce/Internet transactions, in accordance with the appropriate MasterCard, Visa, American Express and Discover operating rules. You also agree to abide by the terms and conditions relating to telephone and mail order services set out in the exhibit for Telephone and Mail Order Services.

2. You agree that your Web site will contain all the following information presented in a clear manner:
 - your country of domicile, provided immediately prior to the cardholder accessing payment instructions
 - merchant outlet address
 - merchant outlet country (must be presented at time of presenting payment options to consumer)
 - a complete and accurate description of the goods or services offered
 - your return/refund policy displayed on the checkout screen
 - your consumer data privacy policy and the method of transaction security used to secure cardholder account data during the ordering and payment process
 - security capabilities and policy for transmission of payment card details
 - a customer service contact, including electronic mail address or telephone number
 - transaction currency (e.g. US dollars, Canadian dollars)
 - export restrictions (if known)
 - your delivery/fulfillment policy
 - the card acceptance brand marks in full color

3. You agree to only use an electronic commerce solution for processing eCommerce/Internet transactions that is capable of providing the required information set out by Global Payments from time to time in accordance with MasterCard, Visa, American Express and Discover regulations:
 - an electronic commerce transaction must be identified in both the authorization request and the clearing record.
 - electronic commerce merchant must offer cardholder a Data Protection Method such as Secure Socket Layer (SSL) or secure cardholder authentication such as 3-D Secure (Verified by Visa) and MasterCard SecureCode.

4. You agree to include the following data on a transaction receipt completed for an eCommerce/Internet transaction:
 - Merchant name most recognizable to consumers
 - Doing Business As (DBA) name as used on website;
 - Merchant Universal Resource Locator (URL); or
 - Merchant name used in the Clearing Record
 - Customer Service contact, including telephone number (If merchant delivers 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
 - 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)
5. You agree to provide a completed copy of the transaction record to the cardholder at the time the purchased goods are delivered or services performed. You may deliver the transaction receipt in either of the following formats:
 - Electronic (e.g., e-mail or fax)
 - Paper (e.g., hand-written or terminal-generated)
6. You agree to not transmit the account number to the cardholder over the Internet or on the transaction receipt.
7. You agree not to hold Global or Member liable for any service option deficiency, delay, interruption, or cessation of service caused by any event that is beyond its reasonable control or for any disclosure of confidential information except where caused by its gross negligence. This clause survives termination of this Agreement.

8. You agree to take all appropriate steps to minimize cardholder disputes and chargebacks. You agree that if you exceed MasterCard International's or Visa International's threshold for chargebacks, as set from time to time, you will be subject to the appropriate MasterCard and/or Visa charges levied for non-compliance.
9. You agree not to engage in the sale of prohibited products and services or conduct business in the following areas without the specific written consent of Global:
 - Online gambling and online gambling transactions (including, but not limited to, any of the following: pyramid schemes, betting, lotteries, casino-style games, funding an account established by the merchant on behalf of the cardholder, purchase of value for proprietary payment mechanisms, such as electronic gaming chips)
 - Sale of pornographic or illicit material of any type
 - Escort services
 - Goods and/or services prohibited by applicable law or under the rules, regulations or directives of any card association.
10. You agree that you will not retain or use any cardholder data without the express consent of the cardholder. You also agree that, prior to discarding, you will destroy this information in a manner rendering it unreadable.
11. You agree that any cardholder information, stored or otherwise, must be appropriately managed, controlled and protected and held in a secure manner to prevent access by unauthorized parties and prevent unauthorized use. This includes:
 - a. You will provide multiple security measures to protect cardholder databases, so that if any one security control fails, it will not result in unauthorized disclosure of account and transaction information.
 - b. You must implement controls so that the cardholder Internet sessions cannot be redirected to an unauthorized website. If a cardholder is redirected to an unauthorized Web site, the cardholder may unknowingly disclose confidential information, account, or transaction information using strong cryptography.
 - c. You must secure all communication between the cardholder and yourself including, but not limited to, cardholder identification, authentication information, account, or transaction information, using strong cryptography.
 - d. You must ensure that databases containing cardholder information are only accessible through tested Web interfaces designated for cardholders. Static passwords do not provide adequate security for system, database or application administrative access over the Internet to cardholder databases.

- e. Your application process must never allow the user to enter unrestricted system or database commands. Application programs must never cause the application to fail in a way that allows users to enter unrestricted system or database commands.
 - f. Your customer support functions must only originate from approved networks and computers.
12. You agree that you also have in place, or will implement before commencing accepting transactions, the following additional measures to protect a cardholder database:
- a. You will implement network access controls that prevent the system that hosts the cardholder database from being directly addressed from the Internet;
 - b. You will not open or run e-mail attachments or other unknown files on the Web or database servers from unknown sources. You will not use the Web or database servers as browsers to view other Web sites;
 - c. You will secure the account number by doing the following:
 - Using strong cryptography (preferably hardware which secures the cryptographic keys) if the account number must be decrypted on a computer system that can be addressed from the Internet;
 - Using strong cryptography hardware or software if the account number can only be decrypted on devices not accessible from the Internet;
 - Not storing the account and transaction information on a computer accessible from the Internet.
13. You agree that before implementing any changes on a computer system that contains account and transaction information accessible from the Internet, you will validate that the changes do not adversely affect the following:
- Hardware that implements security controls
 - Software that implements security controls for account and transaction information

You also agree that, after implementation, you will validate that the appropriate security controls remain in effect.



It is the merchant's obligation to comply with all applicable laws, including but not limited to those state laws regarding obtaining personal information from a cardholder in connection with a card transaction.

14. You agree that MasterCard and/or Visa may permanently prohibit you or one of your owners, officers, partners, proprietors, or employees from participating in the MasterCard, Visa or Visa Electron Program, as applicable, for any reasons it deems appropriate, such as:
 - Fraudulent activity
 - Presenting transaction receipts that do not result from an act between you and the cardholder (laundering)
 - Activity that causes Global or Member to repeatedly violate the Visa International Operating Regulations or the MasterCard International Operating Regulations
 - Activity that has resulted in a MasterCard or Visa Regional office prohibiting you from participating in the MasterCard, Visa or Visa Electron Program
 - Any other activity that may result in undue economic hardship or damage to the goodwill of the MasterCard or Visa system.
15. You agree to perform periodic self-assessments regarding website security and data security as may be recommended or required by MasterCard, Visa, American Express and Discover.
16. You agree that Global, Member, MasterCard, Visa, American Express and Discover have the right to perform periodic audits of your Web site to confirm that you are adhering to the policies and procedures laid out in this agreement and any written directions issued by Global.
17. You agree to pay any fees or charges relating to eCommerce/Internet services set by Global from time to time.
18. In the event of an inconsistency between the terms and conditions of this Exhibit and any other terms and conditions of the Merchant Service Agreement, the provisions of this Exhibit shall prevail.

Exhibit C: Telephone and Mail Order Services Addendum


Pursuant to the Merchant Service Agreement (including the Merchant application and Terms and conditions of Merchant Service Agreement), a Merchant who wishes to offer telephone, mail order, Internet sales or any other services where the card is not physically present must (i) obtain Global's prior consent before offering such services, and (ii) comply with the terms herein and any written directions issued by Global relating to such services.

The Merchant shall not submit any such sale for purchase until the goods or services are shipped or performed, as applicable. Unless expressly requested by Merchant and agreed to by Global, Global WILL set up a separate account for telephone/mail order or Internet sales. The Merchant acknowledges that all sales where the card is not physically present will be subject to an increased risk of chargeback. By offering such services, the Merchant assumes responsibility and agrees to pay Global for all chargebacks relating to telephone order/ mail order and /or Internet sales and indemnifies Global for all costs, fees and expenses in connection therewith.

Merchant will not, under any circumstances, process Visa, MasterCard, American Express or Discover sales for another merchant, person, or entity. Any person or entity that wants to accept MasterCard, American Express or Visa for payment must have its own account with a processor. Processing drafts for another party is known as "factoring," and it is against Visa/ MasterCard/Discover regulations and a breach of the Merchant Agreement. If Global discovers any Merchant has been factoring drafts, such Merchant may be terminated and its name will be placed on the terminated merchant file with MasterCard, Visa and Discover, which could make it impossible for such Merchant to ever obtain another merchant account with any other processor.

1. **Prohibitions.** You will not accept telephone and mail order payments:
 - a. without a mail order form signed by the customer or without verbal authorization from the customer (for telephone orders) that authorizes the charge to a specific card;
 - b. if you have received notification that the card has been voided or revoked; or
 - c. if the goods or services for sale are offered in violation of applicable laws, in a fraudulent manner, are contrary to public policy or have not otherwise been authorized under this Agreement.
2. **Processing.** You will not process any telephone or mail order charges or submit any telephone or mail order sale for purchase until the goods or services purchased are shipped or performed, as applicable.
3. **Procedure.** You will complete a sales draft for each mail order or telephone order, including the date of the transaction, in a form supplied or approved by Global, by following these steps:
 - a. write or imprint the following on the sales draft: your name and merchant number and city, the cardholder's name and account number, the valid from date

- and expiration date of the credit card;
 - b. enter the total cash price plus any taxes. Include a short description of the goods or services involved;
 - c. indicate on the signature panel of the sales draft “mail order/MO” or “phone order/PO;”
 - d. the transaction date is the date of shipment;
 - e. provide a copy of the sales draft to the cardholder;
 - f. keep the merchant copy of each completed sales draft or credit voucher and appropriate backup documentation for a minimum of 18 months; and
 - g. issue a credit voucher if the cardholder is entitled to a refund. Do not refund the amount in cash.
4. **Risk Allocation.** You acknowledge and understand that all sales processed where the card is not physically present are subject to an increased risk of chargeback. You hereby assume responsibility and agree to pay Global for all chargebacks relating to telephone order/mail order sales and hereby agree to indemnify Global and Member for all costs, fees and expenses in connection therewith.
5. **Processing for Third Party.** You will not, under any circumstances, process Visa, MasterCard, American Express or Discover sales for another merchant, person or entity. Any person or entity that wants to accept Visa/MasterCard/American Express/Discover for payment must have its own account with a processor. Processing drafts for another party is known as “factoring” or “draft laundering” and it is against Visa/MasterCard/American Express/Discover regulations and constitutes a breach of your obligations under this Agreement. If Global discovers that you have been factoring or laundering sales drafts, Global may terminate this Agreement effective immediately and may place your name on the terminated merchant file with Visa/MasterCard/American Express/Discover, which could make it impossible for you to obtain a merchant bank account with another processor.
6. **Liability.** You acknowledge and understand that you accept full liability for the identification of the cardholder on any telephone, fax, mail order or Internet transactions.
7. **Order of Priority.** In the event of an inconsistency between the terms and conditions of this Exhibit and any other terms and conditions of the Merchant Service Agreement, the provisions of this Exhibit shall prevail.



Note

It is the merchant's obligation to comply with all applicable laws, including but not limited to those state laws regarding obtaining personal information from a cardholder in connection with a card transaction.

Exhibit D: Lodging Visa/MasterCard Service Addendum

This Addendum supplements the Merchant Agreement and provides the procedures MERCHANT must follow if MERCHANT chooses to use the Visa/MasterCard Reservation Service to accept Visa or MasterCard Cards to guarantee reservations.

Visa/MasterCard Reservation Service for Lodging Accommodations. If MERCHANT is a lodging merchant (hotel, motel, or inn) and MERCHANT uses the Visa/MasterCard Reservation Service, MERCHANT will comply with all of the following procedures:

Reservation Procedures

Accept all MasterCard and Visa cards for reservations requested under the Visa/MasterCard Reservation Service.

Inform the Cardholder that the accommodations will be held until check-out time the following day unless canceled by 6:00 p.m. establishment time on the scheduled arrival date. For resort establishments requiring cancellation prior to 6:00 p.m. establishment time on the scheduled arrival date, the cancellation time and date may vary but must not exceed 72 hours prior to the scheduled arrival date. In these cases, the Cardholder must be provided with the specific written cancellation policy including the date and time the cancellation privileges expire. If a reservation for such an establishment is made less than 72 hours before scheduled arrival, the procedure permitting cancellation by 6:00 p.m. establishment time on the scheduled arrival date must be made available to the Cardholder.

Obtain the Cardholder's account number, expiration date and name embossed on the Visa or MasterCard Card.

Advise the Cardholder that if he has not checked in by check-out time the day after his scheduled arrival date and the reservation was not properly canceled, the Cardholder will be billed for one night's lodging plus the applicable tax.

Quote the rate of the reserved accommodations, the exact physical address of the establishment including name, street address, city and state and provide the Cardholder a confirmation code advising that it be retained. If requested, provide a written confirmation of the reservation including the Visa or MasterCard account number, expiration date and name embossed on the Visa or MasterCard card as provided by the Cardholder, the reservation confirmation code, the exact physical address of the establishment, the provisions of the Visa/MasterCard Reservation Service relating to the Cardholder's obligation, and any other details related to the accommodations reserved.

Cancellation Procedures

Accept all cancellation requests from Cardholders provided the cancellation request is made prior to the specified cancellation time.

Provide the Cardholder a cancellation code and advise the Cardholder that it must be retained to preserve his rights in case of dispute. If requested, provide the Cardholder written confirmation of the cancellation including the Visa or MasterCard account number, expiration date and name embossed on the Visa or MasterCard Card, the cancellation code, and the details related to the accommodations canceled.

Scheduled Arrival Date Procedures

If accommodations reserved under the Visa/MasterCard Reservation Service have not been claimed or canceled prior to the specified cancellation time, the room(s) must be held available in accordance with the reservation.

If the Cardholder does not cancel the reservation or does not check in within the prescribed time, deposit a Sales Draft or transaction record for one night's lodging plus applicable tax indicating the Visa or MasterCard account number, expiration date and name embossed on the Visa or MasterCard card, and the words "Guaranteed Reservation/No Show" on the Cardholder's signature line. If a MasterCard Card was used to guarantee the reservation, the room number assigned to the Cardholder also must be included on the Sales Draft or transaction record.

Obtain an authorization for the "No Show" transaction by following the authorization procedures for lodging transactions.

Alternate Accommodations

If accommodations which were guaranteed under the Visa/MasterCard Reservation Service are unavailable, provide the Cardholder with at least comparable accommodations for one night at another establishment.

Provide transportation for the Cardholder to the location of the alternate establishment.

If requested, provide the Cardholder with a 3-minute telephone call.

If requested, forward all messages and calls for the Cardholder to the location of the alternate establishment.

Provide all services in this section at no charge to the Cardholder.

Special Authorization Procedures For Lodging Merchants

This Addendum supplements the Merchant Agreement and provides the special procedures that may be used in certain circumstances to obtain an authorization for a Visa or MasterCard transaction based on MERCHANT's estimate of the total transaction amount and the additional procedures to be followed if the actual amount of the transaction exceeds, or is likely to exceed, the initial estimate by more than a specified amount. When applicable, the procedures in this Addendum override any conflicting terms set forth in the Merchant Agreement. To use these special authorization procedures, MERCHANT must be engaged in providing lodging accommodations.

Lodging Authorization Procedures

If MERCHANT is engaged in providing lodging accommodations, MERCHANT must estimate the amount of the transaction based on the Cardholder's intended length of stay at check-in, the room rate, applicable tax and/or service charge rates and MERCHANT's procedure for estimating additional ancillary charges.

In all other circumstances, MERCHANT must obtain an authorization approval code for the estimated transaction amount. MERCHANT must record on the guest folio and/or Sales Draft the date, amount and authorization approval code(s) obtained.

If necessary, MERCHANT may obtain additional authorizations for additional amounts (not cumulative of previous amounts) at any time on or between the Cardholder's check-in date and check-out date. MERCHANT must record on the guest folio and/or Sales Draft or transaction record the date, amount and approval code for each additional authorization so obtained.

A final or additional authorization is not necessary to comply with basic authorization requirements if the actual transaction amount does not exceed the sum of the authorized amounts plus 15% of all such authorized amounts. In order for a transaction to qualify for certain incentive rates, however, the floor limit generally must be zero and limits may be imposed on the number and/or dollar amount of any additional authorization requests that may be submitted after the first such request.

Visa Lodging "Status Check" Procedures

This procedure is limited to lodging transactions at hotels permitted by Visa to use the "Status Check" procedure (an authorization request for \$1.00).

If the estimated transaction amount is equal to or below any applicable floor limit and involves a Visa Card for lodging transactions at hotels permitted by Visa to use the "Status Check" procedure (an authorization request for \$1.00), MERCHANT need only request a "Status Check" on the Cardholder's check-in date.

If a hotel permitted to use the "Status Check" procedure uses that procedure without obtaining any other authorization because the initial estimated Visa Card lodging transaction amount was equal to or below the applicable floor limit and MERCHANT subsequently estimates that the transaction amount will exceed that floor limit (based on the Cardholder's actual charges), MERCHANT must obtain an authorization approval code for all of the new estimated transaction amount. MERCHANT must record on the guest folio and/or Sales Draft or transaction record the date, amount and authorization approval code(s) obtained.

A final or additional authorization is not necessary to comply with basic authorization requirements if the actual transaction amount does not exceed the applicable floor limit for a Visa Card lodging transaction for which a permitted Status Check procedure was previously performed.

Delivery of Sales Draft

If MERCHANT alters or prepares an additional Sales Draft in order to add delayed or add-on charges previously consented to by the Cardholder, MERCHANT will mail a copy of the amended Sales Draft to the Cardholder with an explanation of the charges.

Exhibit E: Advance Lodging/Resort Deposit Service Addendum

This Addendum supplements the Merchant Agreement and provides the additional procedures for MERCHANT to follow if MERCHANT chooses to use the Visa Advance Lodging Deposit Service or the MasterCard Advance Resort Deposit service. To use these procedures, MERCHANT must be a lodging merchant (hotel, motel or inn) offering overnight accommodations, or a “Central Reservation Service” merchant (as defined in the Visa U.S.A. Operating Regulations). If MERCHANT uses the Visa Advance Lodging Deposit Service or the MasterCard Advance Resort Deposit service, MERCHANT will comply with all of the following procedures:

Reservation Procedures

Accept all MasterCard, Visa and Discover Cards for advance deposit when the Advance Lodging Resort Deposit Service is agreed to by the Cardholder.

Determine the amount of the Advance Lodging/Resort Deposit Transaction by the intended length of stay, which must not exceed the cost for 14 nights' accommodation for lodging. The amount of the Advance Lodging/Resort Deposit transaction must be applied to the total obligation.

Inform the Cardholder (i) of the advance deposit requirements and (ii) of the cancellation policy requirements and (iii) that, for lodging, the accommodations will be held for the number of nights used to determine the amount of the Advance Lodging/Resort Deposit transaction. Obtain the Cardholder's account number, Card expiration date, the name embossed on the Card, telephone number, mailing address, scheduled date of arrival or embarkation and, for lodging, the intended length of stay.

Inform the Cardholder that if changes in the reservation are requested, written confirmation of such changes will be provided at the Cardholder's request.

Advise the Cardholder that (i) if he/she has not checked in by check-out time the day following the last night of accommodation used to determine the amount of the Advance Lodging/Resort Deposit transaction or (ii) the reservation was not canceled by the specified time and date, the Cardholder will forfeit the entire amount of the Advance Lodging/Resort Deposit transaction or a portion of that amount in accordance with MERCHANT's stated policy. Under no circumstances is an additional deposit of a transaction resulting from the Cardholder's failure to cancel or use the reservation allowed under the Advance Lodging/Resort Deposit Service.

Quote the rate of the reserved accommodations, the amount of the Advance Lodging/Resort Deposit transaction and the exact MERCHANT location. Provide the Cardholder with a confirmation number (advising that it must be retained) and with the actual date and time the cancellation privileges expire.

Complete a Sales Draft or transaction record for the amount of the advance deposit, indicating the Cardholder account number, Card expiration date, the name embossed on the Card, the

Cardholder's telephone number and mailing address, the words "Advance Deposit" on the signature line, the Cardholder's confirmation number, the scheduled arrival or embarkation date, and the last day and time the cancellation privileges expire without forfeiture of the deposit if the accommodations are not used.

Follow normal authorization procedures for lodging transactions, as applicable; but regardless of any otherwise applicable floor limit, all advance deposits made with MasterCard Cards must be authorized if the amount exceeds \$50.

If the authorization request results in a decline, so advise the Cardholder and do not deposit the Sales Draft.

If authorization is approved:

- Mail the Cardholder copy of the Sales Draft and the written lodging cancellation policy to the address indicated by the Cardholder within three business days from the transaction date.
- Submit the Sales Draft or transaction record in accordance with usual procedures as specified in the Agreement.

Cancellation Procedures

Accept all cancellation requests from Cardholders provided the cancellation request is made prior to the specified cancellation date and time.

Provide a cancellation number and advise the Cardholder that it must be retained to preserve his/her rights in the case of a dispute.

For the cancellation of a lodging reservation, complete a Credit Voucher for the entire amount of the Advance Lodging/Resort Deposit transaction. Include on the Credit Voucher the Cardholder account number, Card expiration date, the name embossed on the Card, mailing address, the cancellation number and the words, "Advance Deposit" (if Visa) or "Deposit Cancellation" (if MasterCard) on the signature line.

Mail the Cardholder a copy of the Credit Voucher to the address indicated by the Cardholder within three business days from the transaction date.

Alternate Accommodations

If accommodations which were reserved under the Advance Lodging Deposit Service are unavailable, complete and deliver to the Cardholder a Credit Voucher for the entire amount of the Advance Lodging Deposit Transaction.

Provide the following services at no charge to the Cardholder:

- At least comparable accommodations at an alternate establishment (i) for the number of nights used to determine the amount of the Advance Lodging Deposit transaction,

- not to exceed 14 nights, or (ii) until the reserved accommodations are made available at the original establishment, whichever occurs first.
- Transportation to the location of the alternate establishment and return transportation to the original establishment. If requested, transportation to and from the alternate establishment must be provided on a daily basis.
 - If requested, two three-minute telephone calls.
 - If requested, forwarding of all messages and calls to the location of the alternate establishment.

Central Reservation Service Responsibilities

Any MERCHANT acting as a “Central Reservation Service” and desiring to accept Cards as payment for such services:

- Must be registered with Visa and, if applicable, other Card Associations, and must have duly executed written contracts with lodging establishments for which it provides reservation services;
- Must follow all procedures for reservations, cancellations, alternate accommodations and chargebacks provided in this Attachment and in the applicable Association Rules; and Shall bear full responsibility for resolving any Cardholder problems related to Advance Lodging Deposit Service.

Exhibit F: Priority/Express Check-Out Service Addendum

This Addendum supplements the Merchant Agreement and provides the procedures for MERCHANT to follow if MERCHANT chooses to use the Visa Priority Check-Out Service or the MasterCard Express Checkout Service. MERCHANT must be a lodging merchant (hotel, motel or inn). If MERCHANT uses the Visa Priority Check-Out Service or the MasterCard Express Checkout Service, MERCHANT will comply with all of the following procedures.

Priority Check-Out Procedures

1. Accept all MasterCard, Visa and Discover Cards when a Cardholder requests the Priority/Express Check-Out Service for lodging.
2. Provide the Cardholder with a Priority/Express Check-Out Agreement.
3. Inform the Cardholder that the Priority/Express Check-Out Agreement must be completed and signed; the mailing address must be included to receive a copy of the hotel bill supporting the final transaction amount.
4. Obtain the completed Priority/Express Check-Out Agreement and ensure the Cardholder account number identified is identical to the account number imprinted on the Sales Draft or transaction record.
5. On the Cardholder's date of departure, complete the Sales Draft indicating the total amount of the Cardholder's obligation and the words "Priority Check-Out" (for Visa) or "Signature on File -- Express Checkout" (for MasterCard) on the signature line.
6. Follow normal authorization procedures for lodging transactions.
7. Mail the Cardholder copy of the Sales Draft, the itemized lodging bill, and, if requested, the signed Priority/Express Check-Out Agreement to the address provided by the Cardholder on the Priority/Express Check-Out Agreement within three business days of the Cardholder's departure.

Record Retention

The itemized lodging bill and the signed Priority/Express Check-Out Agreement supporting a Priority/Express Check-Out transaction must be retained for a minimum of six months from the transaction date.



The merchant is to comply with all the obligations set forth in these exhibits/appendices; and these exhibits/appendices contain all of the verbiage that is mandated by MasterCard, Visa and Discover.



Glossary of Terms

Address Verification Service (AVS): A service through which a merchant may verify a cardholder's billing address against the card issuer's records during the authorization process and prior to completing a sale; helpful in preventing fraud when processing MOTO transactions.

Association Chargeback Fees: The card associations permit the cardholder bank to collect additional fees for items that result in a chargeback. Merchants may be subject to these Association Chargeback Fees if they failed to follow card acceptance and authorization procedures and the card issuer has a valid chargeback.

Authorization: The process of verifying a bankcard transaction by a bankcard-issuing bank, other institution or by an approved independent service provider. Authorization is initiated by accessing (by voice or POS terminal, as appropriate) Global Payments designated Voice Authorization Center(s). Authorization is based on the cardholder account status and available credit.

Authorization Code: A six-digit alphanumeric code assigned by the issuer to identify the approval for a specific authorization request. The authorization code is always included on the merchant sales draft. Also referred to as 'issuer's response code,' 'authorization approval code,' or 'authorization response code.'

Authorization Approval Code: Refer to Authorization Code.

Authorization Response Code: Refer to Authorization Code.

AVS Only Fee: Fee charged for account status check transactions that validate cardholder address (AVS), or c-code on card, or both, and do not place a financial hold on cardholder available funds. This feature may be used by hospitality merchants (restaurant, bar, tavern) that may only perform one authorization for a transaction.

Bankcards or Cards: MasterCard, Visa and Discover credit and/or debit cards issued by a financial institution. Effective November 8, 2004, this also includes Diners International cards that bear the MasterCard brand on back. Discover and JCB cards issued by card association or by a financial institution also fall under the definition of "Cards."

Bankcard 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 Global Payments and merchant, or by an electronic equivalent of a sales draft or credit draft, which is presented to Global Payments by the merchant for processing through the Interchange Systems.

Card Verification Code (CVC/CVC2): A unique three-digit numeric value calculated from the date encoded on the magnetic stripe of a MasterCard, for the purpose of validating card information during the authorization process; used to enhance the authentication of the card. CVC 1 is a three-digit value encoded in the discretionary data on tracks 1 and 2; CVC 2 is indent-printed in the signature panel of the card; printed in the signature area on the back of the card, but not present on the card's magnetic stripe. Typically used for fraud control for card-not-present transactions.

Card Verification Value (CVV/CVV2): A unique three-digit numeric value calculated from the date encoded on the magnetic stripe of a Visa Card, for the purpose of validating card information during the authorization process. The number is printed in the signature area on the back of the card, but not present on the card's magnetic stripe. Typically used for fraud control for card-not-present transactions.

CID: 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 **Section 2: Card-Not-Present Transactions** for more details.

Cardholder: The authorized user to whom a credit or payment card has been issued. The authorized user's name is embossed on a card or appears on a bankcard as an authorized user. A person that uses a credit or payment card to purchase goods or services.

Cardholder and Payment Transaction Information: Any information evidencing either (a) a cardholder's personal data, including without limitation evidence of the cardholder's credit, debit, or other type of card, or (b) transactions consummated with credit, debit or other types of cards, including electronic, written and other forms of data. This definition also incorporates other, similar terms, including "cardholder data" and "cardholder information;" This includes, but is not limited to, card imprints, transaction receipts, carbon copies, mailing lists, tapes or other media obtained as a result of a card transaction.

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

Chargeback: A previous bankcard transaction which is under dispute by the cardholders or their issuing institution. This action is initiated by the card issuing bank to settle a financial claim between the issuer and acquirer resulting from the lack of adherence to the conditions of the sales agreement, association regulations or the operating procedures. This claim may be initiated by the issuing bank directly or by its customer or the cardholder, and can result in the transaction being billed back to the merchant.

Chargeback (continued): When used as a noun, a [chargeback](#) is a bankcard transaction that is debited to the deposit account by Global Payments, set-off against any other account maintained by the merchant with Global Payments or presented directly to the merchant by the bank for repayment when the deposit account does not contain sufficient funds. [Chargeback](#), when used as a verb, is 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 Reason Code: A numerical code, which identifies the specific reason for the chargeback.

Code 10: A universal code that provides merchants with a way to alert the Voice Authorization Center that a suspicious transaction is occurring without alerting the cardholder (or other person presenting the bankcard). 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 to select business staff by their employer for Commercial use, often with a higher discount expense than consumer cards. Transactions originating from these cards have unique qualification requirements and interchange fees depending on the card and merchant type. Non-T&E (Travel & Entertainment) merchants accepting a large volume of commercial cards should use a product that will support entry of sales tax and customer code.

Commercial Rewards Card: A Corporate World Card, Corporate World Elite Card, Business World Card and Business World Elite Card issued for commercial use with additional benefits. These cards may be subject to higher discount expense associated with rewards cards.

Consumer Card: A card issued to a consumer. See Bankcards or Cards definition for details. Consumer Rewards Cards: Visa Infinite Card, Visa Signature Card, Visa Signature Preferred Card, Visa Rewards Card, MasterCard World Cards and MasterCard World Elite Cards issued to consumers have additional benefits. T&E merchants incur additional discount expense for these upscale cards. Effective April 2005, Consumer Rewards Cards used at non-T&E merchants may be subject to higher interchange expenses.

Contactless Reader: A payment card reader that uses Radio Frequency Identification (RFID) technology to read payment information without coming into contact with the payment card.

Credit Draft: A document evidencing the return of merchandise by a card member to a merchant, or other refund made by the merchant to the card member.

Cross Border Fee: A transaction where the merchant country and cardholder country are different and transactions are subject to cross border fees assessed by Discover, MasterCard and Visa. Cross border fees and charges are summarized on merchant statements and may impact the following categories based on the merchant location:

Brand	Statement Description
Discover	DISC INTL PROCESSING FEE
Discover	DISC INTL SERVICE FEE
MasterCard	CROSS BORDER
MasterCard	CROSS BORDER STANDARD
MasterCard	MC ACQ SUPPORT FEE
MasterCard	CROSS BORDER LAC REG
MasterCard	CROSS BORDER LAC REG STD
Visa	VISA INTL SVC ASSESS
Visa	VISA INTL ACQ FEE

Data Capture: At the same time a credit card transaction is authorized, it is also captured for ultimate delivery to the card issuer for merchant reimbursement.

Debit Card or Check Card: A payment card issued by a financial institution that is used to initiate a debit transaction. In general, these transactions are used primarily to pay for goods and services or to obtain cash. In order to obtain cash, the cardholder's checking account is debited by the card-issuing institution. The funds are withdrawn directly from the cardholder's checking account at the time of the sale. For online debit transactions, PIN entry is required. For offline debit transactions, a signature is required.

Deposit Account or Demand Deposit Account (DDA): A business checking account designated by the merchant through which all bankcard transactions and adjustments are processed by Global Payments.

Discount Rate: Comprised of a number of dues, fees, assessments, network charges and mark-ups, merchants are required to pay for accepting credit and debit cards, the largest of which is the Interchange fee. However, some assessments will be billed separately from the Discount Rate, such as:

Brand	Statement Description
Discover	DISC NETWORK ACCESS FEE
MasterCard	MC NETWORK ACCESS FEE
Visa	VISA APF FEE
Visa	VS MISUSE OF AUTH SYSTEM FEE
Visa	VISA NETWORK ACCESS FEE
Visa	VS ZERO FLOOR LIMIT FEE

EMV: Refers to chip standards managed by EMVCo, formed by Europay International, MasterCard International and Visa International. EMVco's primary role is to manage, maintain and enhance the EMV Card Specifications to ensure worldwide interoperability and universal acceptance of chip payment cards.

Factoring or Draft Laundering: A merchant's presentation to Global Payments 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 processing, debiting, negotiating or obtaining payment pursuant to the Global Payments 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 specific dollar amount set by the acquirer in accordance with bankcard association rules and regulations to determine which bankcard transactions must be authorized. For example, if a business has a floor limit of \$25.00, authorization must be obtained for any transaction over that amount.

Force Transactions: Used to enter a sale transaction after the fact. In most cases, the customer has already left the store. A **force transaction** is usually done because the merchant couldn't complete the original authorization: either a referral message response was received from the original transaction or there was a temporary interruption of service and the merchant had to obtain a voice authorization. Following a voice approval, the merchant uses the force to enter the transaction information so it can be settled as part of the settlement batch.

In Flight Terminal: A terminal which is connected to a secure network and capable of processing payment transactions.

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

Issuer's Response Code: Refer to Authorization Code.

Limited Acceptance Merchant: A merchant who elects to accept credit cards or debit/pre-paid cards, or both, by so notifying Global Payments in writing.

Magnetic Stripe: A stripe of magnetic information affixed to the back of a plastic credit or debit card. The magnetic stripe contains encoded cardholder account information.

MasterCard/Visa Interchange Systems or Interchange System: The standardized electronic exchange of financial and non-financial Visa and MasterCard transaction data between acquirers and issuers.

Merchant: A person or entity entering into a Merchant Agreement with Global Payments, as well as all personnel, agents and representatives of the merchant, that accepts credit or debit cards as a form of payment for goods or services.

Merchant Identification Number: A 6- to 16-digit number each merchant is provided under the Global Payments Merchant Agreement.

Misuse of Authorization Fee: Fee per transaction that will be applied to authorization attempts that are not followed by a matching Visa or MasterCard clearing transaction (or, in the case of a cancelled or timed out transaction, are not properly reversed). Also recognized as the fee charged for authorizations that are either not settled or reversed within certain timeframes. For instance, a restaurant should not do an authorization attempt for a patron that has an ongoing tab. The restaurant should use AVS Only, or simply receive one authorization and settle one transaction for the patron's entire bill.

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.

No Signature Required (NSR): With NSR, no customer signature is required and a receipt does not have to be provided to the cardholder unless requested for purchases up to \$25.00.

Offline Debit Card: A bankcard, 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. Offline debit transactions take place using the dual message credit card processing method in which the authorization occurs at the time of the transaction using one message, and the transaction is settled later using another message. These transactions do not require a PIN (Personal Identification Number), but do require the cardholder's signature. This transaction is processed like a credit card with the posting to the cardholder's account within a few days of the transaction occurrence. These are often referred to as 'check card' transactions.

Offline PIN: The PIN stored on the chip card (versus a PIN stored at the host). In a chip transaction using offline PIN, the PIN entered at the terminal is compared with the PIN stored securely on the chip card without going online to the issuer host for the comparison. Only the result of the comparison is passed to the issuer host system.

Online Debit Card: A bankcard 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 online debit cards.

Online PIN: In a chip transaction, the process of comparing the cardholder's entered PIN with the PIN stored on the issuer host system. The PIN is encrypted by the POS terminal PIN pad before being passed to the acquirer system. The PIN is then decrypted and re-encrypted as it passes between each party on its way to the issuer.

Operating Regulations or Regulations: The current operating regulations of both MasterCard, Visa, American Express and Discover, unless specifically referred to as the operating regulations of either Visa or MasterCard.

Participation Fee: A PayPal fee charged as a fixed amount for each Authorization Request, charged on a monthly basis. This fee can be identified on your statement as PPALPRTICP (Short Description) PAYPAL ATH PARTICIPATION FEE.

Participation Rate: A PayPal Rate charged on a monthly basis as a percentage of the Gross Sales Volume. This rate can be identified on your statement as PPAL ASM (Short Description) PAYPAL ASSESSMENTS.

Payment Card Industry Data Security Standards (PCI DSS): Common standards for merchants and third parties resulting from the alignment of MasterCard, Visa and other card associations with the similar goal of protecting payment card account data wherever it is received or stored.

PCI Security Standards Council (PCI Co.): An independent body founded by Visa International, MasterCard Worldwide, American Express, Discover Financial Services and JCB to govern the security standards for the payments industry. PCI Co. owns, develops, maintains and distributes the Payment Card Industry (PCI) Data Security Standard (DSS) which is located on their website at: <https://www.pcisecuritystandards.org/>.

PIN: Personal Identification Number. The confidential individual number or code used by a cardholder to authenticate card ownership for ATM or point-of-sale transactions.

PIN Debit: PIN debit or online debit involves payment processing in which customers are required to swipe their debit card and also enter the PIN or Personal Identification Number. This is possible through the use of POS device or POS software system with an attached PIN Pad.

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 Draft: A paper or electronic record of a sale, rental or service transaction which the merchant presents to Global Payments 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.

Service Fee: A fee assessed by a Government or Higher Education Merchant or its agent to a Cardholder using a Visa Card for payment of goods or services (including tax payments).

Signature Debit: Signature debit (or offline debit) transactions involve payment processing using a debit card the same way a credit card is processed. The only difference is that the cardholder is accessing his/her deposit account rather than a line of credit. The transaction may be carried out on the Internet, or using a POS device. Instead of using a PIN, the cardholder signs a sales receipt to authorize the transaction.

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

Split Tender: A transaction split between a pre-paid card and another card or another form of payment.

Status Check: A test of the cardholder's account to confirm that funds are in the account before authorizing a transaction (usually in the amount of \$1.00).

Surcharge: A fee assessed to a Cardholder by a Merchant in the U.S. Region or in a U.S. Territory that is added to a Credit Card Transaction for the acceptance of a Visa, MasterCard or Discover Credit Card.

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 third party POS device provider) that assists merchants in completing credit card transactions. Third party is not a member of the card associations, is not directly connected to the card associations, is not directly connected to the card associations for authorization or capture of transaction data and provide(s) the following service(s): Authorization and/or transaction processing (including pre-authorization, authorization, AVS CVV2/CVC2/CID, cardholder authentication, Verified by VISA and MasterCard Secure Code).

TIF (Transaction Integrity Fee): A fee assessed to signature debit transactions, including Visa prepaid card purchase transactions that either fail or do not request CPS (Custom Payment Service) qualification.

Touch Tone Capture (TTC): By dialing a toll-free number, merchants are connected to an Interactive Voice Response (IVR) unit. Merchants use their touchtone keypad to enter the authorization request. Once approved, the transaction is automatically captured by the processor's host draft capture system and held for settlement.

Triple DES: Also referred to as 3DES, a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key). This is one of the security standards in the payment industry.

Unlawful Internet Gambling Enforcement Act and Regulation GG: The U.S. Department of the Treasury and the Board of Governors of the Federal Reserve System have issued regulations implementing the Unlawful Internet Gambling Enforcement Act¹ requiring U.S. financial institutions and certain “participants in designated payment systems” to establish and implement policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit unlawful internet gambling transactions covered by this Act. Compliance by these participants is required by June 1, 2010. NOTE: Internet gambling is prohibited under established credit policy.

Voice Authorization: Authorization obtained by telephoning a Global Payments voice operator.

Zero Floor Limit Fee: Fee charged for transactions that are settled without the corresponding authorization code. NOTE: The floor limit for all merchant transactions is \$0.00

Sponsoring Institutions

Global Payments, Inc. is a registered ISO of BMO Harris Bank, N.A

Global Payments, Inc. is a registered ISO of Wells Fargo Bank, N.A., Walnut Creek, CA

