

**ELECTRONIC PAYMENT  
CARD ACCEPTANCE  
GUIDE**

**032111**

**CARD  
ACCEPTANCE  
GUIDE**

**Released August 2007**

032111-0807 Revision 07

IRN Payment Systems  
800 Shames Drive  
Westbury, NY 11590

**Please Note: This guide is part of your IRN Payment Systems (herein after referred to as IRN Payment or IRN) merchant agreement and you must follow the procedures in this guide to comply with your agreement.**

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 IRN Payment.

The information contained in this guide is proprietary and confidential to IRN Payment and merchants who have executed an agreement with IRN Payment for card payment services.

IRN Payment 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.

© 2007 IRN Payment Systems  
ALL RIGHTS RESERVED, Printed in the USA  
800 Shames Drive, Westbury, NY 11590

IRN Payment and IRN are trademarks of IRN Payment Systems and may not be copied, imitated, or used, in whole or in part, without its prior permission. All other trademarks, registered trademarks, product names, and logos identified or mentioned herein are the property of their respective owners



Determining Card Validity	22
<i>Visa Cards</i>	22
<i>MasterCard Cards</i>	23
<i>American Express Cards</i>	24
<i>Discover Cards</i>	24
Swiping the Card	24
Compare Account Numbers	24
Available Fraud Controls	25
Request Authorization	25
Print the Sales Draft	26
Obtain and Compare Signatures	28
<b>Accepting Debit and EBT Cards</b>	<b>30</b>
EBT Processing	31
<b>Returns and Exchanges</b>	<b>33</b>
Credit Card Refunds	33
Debit Card Refunds	34
<b>Card Not Present Transactions</b>	<b>35</b>
Completing Electronic Commerce Transactions	37
<i>Merchant Website and Electronic Transactions</i>	
<i>Requirements</i>	38
<i>Transaction Receipt Requirements</i>	38
Completing Mail and Telephone Order Transactions	39
Completing Recurring Bill Payment Transactions	40
<i>What is a “Recurring Payment”?</i>	40
<i>How is a “Recurring Payment” different from other forms of payment?</i>	41
<i>What should be on an Order Form?</i>	41
<i>Other Requirements and Prohibitions for Recurring Transactions</i>	42
Best Practices for Merchant Use of Convenience Fees	43
<b>Draft Retrieval Requests</b>	<b>45</b>
Sample Sales Draft Retrieval Request	46
<b>Merchant Deposits</b>	<b>47</b>
<b>Lodging Merchants Best Practices</b>	<b>48</b>
Key Dates for Lodging Merchants:	48
Data Accuracy	49

Authorizations	49
<i>Card Present</i>	49
<i>Estimated Transaction Authorization</i>	49
<i>Incremental Authorization</i>	50
<i>Total Authorized Amount</i>	50
<i>Request for Copy/Travel &amp; Entertainment (T&amp;E) Original</i>	50
Advance Deposit Service for Pre-payment of Resort Lodging	
Accommodations - Sales Draft Checklist	51
<i>Reservation Clerk Procedures</i>	51
<i>Reservation Clerk requests from Cardholder</i>	51
<i>Reservation Clerk provides to Cardholder during call</i>	52
<i>Reservation Clerk provides transaction information to Cardholder on Sales Draft</i>	52
<i>Credit Voucher Checklist</i>	52
Priority Check-Out Service	52
<i>To process Priority Check-Out Service.</i>	53
<b>Sample Forms and Letters</b>	<b>54</b>
Guaranteed Reservations	54
Priority/Express Check-out Sample Form	55
No Show Charge - Sample Letter	56
Processing a "No Show" Reservation	57
<b>Chargebacks</b>	<b>58</b>
Some Do's and Don'ts of Chargebacks	58
<b>Your Right to a Rebuttal</b>	<b>60</b>
<b>Understanding Your Statement</b>	<b>61</b>
Questions About Your Statement	61
Sample Statement	62
<b>Working Together to Prevent Fraud</b>	<b>63</b>
Prohibited Transactions	63
<i>Take Charge of Chargebacks</i>	65
<i>Processing Transactions Manually with an Imprinter</i>	65
<i>Processing Transactions through an Electronic Point-of-Sale Terminal</i>	66
<i>Mail and Telephone Orders</i>	66
<i>Protecting your eBusiness</i>	67
<i>Factoring or Draft Laundering</i>	68
<i>Card Not Present Scams</i>	68

<i>Skimming</i>	69
<i>Don't Be Bullied</i>	69
<i>Deceptive Deliveries</i>	70
<i>The Manual Key-In</i>	70
<i>Borrowed Cards</i>	70
<i>One Person's Trash Is Another's Gold Mine</i>	71
<i>The Terminal Repair Scam</i>	71
<i>Fraudulent Returns</i>	71
<i>International Credit Cards</i>	72
<i>Office Products Scams</i>	72
<i>Phone Fraud</i>	73
<i>Point of Sale Protection</i>	74
<i>The Last Minute Shopper</i>	74
<i>Counterfeit Cards</i>	74
<i>Don't Hesitate! Call In a Code 10</i>	75
<i>Defeating Fraud Helps You and Your Customers</i>	76
<b>Spotting Counterfeit/Altered Cards</b>	<b>77</b>
Color	77
Embossing	77
Signature Panel	77
Hologram	77
MasterCard Formats	78
<i>Security Features</i>	78
Visa Card Formats	78
<i>Security Features</i>	79
Discover Card Formats	82
<i>Security Features</i>	82
JCB Card Formats	83
<i>Security Features</i>	83
<b>Pick Up Card Procedures</b>	<b>86</b>
<b>Limited Acceptance Merchants</b>	<b>87</b>
<b>Exhibits</b>	<b>88</b>
EBT Card Services Agreement	88
E-Commerce/Internet Services Addendum	100
Telephone And Mail Order Services Addendum	106
Visa/MasterCard Reservation Service Addendum	109
Special Authorization Procedures For Lodging Merchants	112

Advance Lodging/ Resort Deposit Service Addendum	114
Priority/Express Check-Out Service Addendum	117
<b>Sponsoring Institutions</b>	<b>119</b>
<b>Glossary</b>	<b>120</b>

## Welcome

Welcome and congratulations on obtaining your new merchant bankcard processing account. Your credit card processing services will be provided by the Independent Sales Organization (ISO) indicated on the first page of this guide and by IRN Payment Systems (“IRN Payment”), as further described herein.

Together, our goal is to ensure that you have the information, card payment options and flexibility you need to help your business grow.

## Our Roles

### ***Independent Sales Organization - ISO***

An ISO is registered with MasterCard and Visa as a sales and service agent of the member financial institution that is a party to the merchant agreement you signed when you applied for service. The services provided by an ISO can vary, but generally ISOs can be involved in providing the following services to merchants:

- Sales
- Customer Service
- Terminal/POS Equipment Sales, Deployment and Support
- Risk and Fraud Management
- POS Supply Fulfillment

### ***IRN Payment***

IRN Payment provides the core processing services in connection with your merchant account. IRN Payment has four decades of expertise in payment processing and is a full service provider of these services for all major credit, debit, EBT, commercial and gift cards in the retail, restaurant, hospitality and travel, direct marketing, health care, supermarket and many other industries.

IRN Payment provides a full range of merchant processing services in both traditional transaction processing and emerging payment technologies including:

- Card Authorization
- Draft Capture
- Merchant Accounting
- Chargeback Handling
- Electronic Benefits Transfer Processing
- Reconciliation
- Settlement

## Your Role

As a merchant it is important that you:

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

## Introduction

Congratulations! Your decision to accept credit, debit, EBT, gift or commercial cards as a valid form of payment offers a valued service to your customers.

Bankcards (MasterCard or Visa) are the most popular type of payment cards - 79% of U. S. households\* have one and find them convenient, fast and flexible. It is also a good business decision, since studies indicate that people who use credit and debit cards can be among your best customers.

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

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

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

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

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

---

\* Source: *The Nilson Report: March 2000*

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

## Parties Involved in the Transaction

### ***Customer/Cardholder***

The process that begins when a customer presents a credit or debit card to pay for goods and services actually starts some time earlier, when the customer submits an application to a bank that issues Visa or MasterCard cards. The cardholder is an authorized user of Visa and/or MasterCard payment products.

### ***Bankcards and Issuers***

MasterCard, Visa, and Discover cards are sometimes known as *bankcards* because individual financial institutions issue them, banks for example, instead of the credit card company itself, such as American Express®.

If the financial institution (or issuer) accepts the customer's application, it issues the Visa, MasterCard, and Discover card. The card may be a credit card, which means that the bank has authorized a line of credit from which the customer may draw; or a debit card, which is tied to the amount of money actually on deposit for the customer, or a commercial card, which is used for business credit charges.

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

### ***Merchant***

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

## 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), or via telephone, mail, fax or over the Internet.



## Authorization and Electronic Data Capture

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

IRN then electronically routes the electronic data from the card to the card issuer.

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

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

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

## Funding

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

## Settlement

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

Remember that your deposit account is not just for deposits! IRN Payment will subtract each month's accumulated discount fees from your deposit account. The settlement charges will also be subtracted.

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

## **Retention of Sales Drafts**

In order to properly address chargeback issues, merchants must retain signed copies of sales drafts bearing cardholder signature to address cardholder inquiries and requests for copies. IRN Payment requires retention for 18 months of your MasterCard, Visa, and Discover transactions. Retention of the original draft, or a legible copy can be stored for 18 months from the date you were paid for the transaction.

Stored sales drafts and other transaction data should be safeguarded with limited access. Merchant must keep all systems and media containing cardholder, account or transaction information (whether physical or electronic) in a restricted, secure manner so as to prevent access by or disclosure to any unauthorized party. At the end of the 18 month retention period, transaction data such as sales drafts, reports, and other media with cardholder account data must be rendered unreadable prior to being discarded. If you have PC access to transaction information, then you must not dispose of the PC until information has been rendered unreadable or has been shredded.

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

## Best Practices in Accepting Bankcards for Payment

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

To follow best practices:

### Do

- Use a terminal or third party terminal provider service that truncates the card expiration date and all but the last 4 digits of the card number on the cardholder copy of the receipt. (Note: Merchant copy of receipt bearing signature may display full account number and expiration date)
- Store all materials containing cardholder account information in a restricted/secure area
- Limit access to sales drafts, reports, or other sources of cardholder data to your employees on a need to know basis
- Render materials containing cardholder account information unreadable prior to discarding
- Retain legal control over cardholder transaction data and personal cardholder information if you use a third-party
- Limit access to IRN Payment's systems requiring unique operator log-in and notify IRN immediately of staff terminations or changes
- Immediately notify IRN Risk Management of any suspected or confirmed loss or theft of materials or records that contain account information retained by merchant or its third party
- Immediately notify IRN Payment of the use of an agent or third party provider not identified on the Merchant Application
- Communicate these requirements to your third party provider and/or third party terminal provider and

direct them to card association information, publications, and or Web sites regarding safeguarding cardholder transaction data

- Require your third party provider to adhere to PCI DSS, AIS, and MasterCard data security requirements (available on PCI website)
- If merchant internal systems receive, pass, or store cardholder and transaction data, ensure that:
  - 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
  - you are in compliance with PCI Co. requirements
  - you validate data security compliance, if requested by IRN or member,
- Retain sales drafts for 18 months
- Display proper signage

### Don't

- Process cash advance transactions unless you are a financial institution approved to do so through your merchant account
- Assign a minimum or maximum purchase amount
- Add a surcharge or fee
- Restrict bankcard use (for a sale or discounted item)
- Use a bankcard to guarantee a check
- List a cardholder's personal information on a bankcard sales slip (unless the authorization operator requests it)
- Record CVV2/CVC2/CID on sales draft (only the one-digit result code can be recorded or retained)
- Retain sensitive cardholder data if expressly prohibited, including complete contents of a card's magnetic stripe (subsequent to the authorization)
- Sell, transfer, or disclose cardholder account information or personal information (This

information should be released only to IRN or Member, or as specifically required by law. If you want to participate in a loyalty program, the loyalty vendor must be compliant with PCI requirements, PCI DSS certified by Visa and implemented in accordance with processes and procedures.)

- Deny a purchase because a cardholder refuses to provide additional identification such as telephone number, address, social security number, or driver's license
- Use any other telephone number other than the official number provided for authorization of a transaction

### ***You May Ask for Personal Information When...***

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

### ***Never Honor a Card When...***

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

## **Operating Guidelines**

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

### **Month-End Settlement Adjustments**

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

### **Draft Laundering or Factoring**

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

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

## Charge Restrictions

Please realize that MasterCard, Visa, and Discover regulations prohibit assigning a minimum or a maximum purchase amount or adding a surcharge to credit card transactions. Regulations also prohibit the use of credit cards for cash advances, collection of bad debt (e.g., returned checks), or damages, theft, etc.

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

**Adding a surcharge to credit transactions is against the law in many states and violates Visa and MasterCard rules and could result in fines.**

## 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. New MasterCard, Visa, 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.

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

You must not request or use account number information for any purpose the cardholder did not authorize or that may be

fraudulent. If you accept other card types (American Express, Diners, Discover, JCB, etc.) you may release transaction information to them 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 IRN or provide acceptable proof of destruction of this information to IRN.

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

### ***Never retain or store the:***

- Complete contents of a card's magnetic stripe (subsequent to the authorization)
- CVV2, CVC2, or CID (American Express and Discover) 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 you are suspicious that the transaction is not valid, do not hesitate to ask for additional identification -- preferably a photo ID. If you must list the identifying data, write it elsewhere (such as your copy of the sales receipt) rather than on the 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 your customers will appreciate.

### **Proper Display of Signage**

When you agree to accept Visa or MasterCard at your place of business or Web site, you should display the proper signage to indicate that service is available. Visa, MasterCard, and Discover require that you clearly display signs at the point of sale. Use the sign and decals included in your merchant welcome kit. (See "Supplies" section for information on ordering additional signs and window decals.)

### **Electronic Data Capture Merchants**

Electronic Data Capture (EDC) merchants use a terminal or other electronic device (e.g., cash register or PC) to authorize and settle their transactions. Using EDC is preferable to using paper drafts since an electronic record of your credit and debit card transactions is maintained throughout the business day. The terminal can be used to validate your totals before settling with IRN Payment at the end of the day.

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

### **Completing an Electronic Transaction**

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

There are six steps to complete an electronic transaction:

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

### **Determining Card Validity**

Follow these steps to make sure the card is valid:

#### ***Visa Cards***

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

The flying “V” is an embossed security character beside the “Good Through” date. If the V is not italicized or it 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, the three-digit card authentication value printed on the signature panel after the full or truncated account number helps mail order, telephone, and Internet order merchants validate that the customer has a Visa card and that the card account is legitimate.

### **MasterCard Cards**

All MasterCard account numbers begin with a 5. The embossing should be clear and uniform in size and spacing. The MasterCard logo may appear on the front or the back of the card along with a hologram. Whether on the front or back of the card, a hologram with interlocking globes showing the continents should appear three-dimensional and move when the card is tilted. The word “MasterCard” will appear in the background of the hologram. The letters “MC” are micro-engraved around the two rings.

A four-digit number may be pre-printed on the card. It must match the first four digits of the embossed account number. MasterCard cards have a stylized “MC” embossed on the line next to the valid dates.

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

The card is not physically altered in any way.

The transaction falls between the effective date and the card's expiration date. If the current date is not within the specified range, do not accept the card. Follow the terminal authorization procedures as described in your IRN Payment's Quick Reference Guide.

### **American Express Cards**

Please email American Express Fraud Prevention if you have questions on fraud prevention and safeguarding cardholder data by sending email to: [es.fraud.prevention@aexp.com](mailto:es.fraud.prevention@aexp.com). In addition, an American Express Card Acceptance Procedures Guide is available online at: <http://home5.americanexpress.com/merchant/resources/welcomekit/welcomekit.asp>.

### **Discover Cards**

Please refer to your Discover Business Services “Merchant Operating Regulations.” Card bearing the Discover Network Acceptance Mark or the Discover/Novus acceptance Mark. 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. Card number on the back of the card is followed by the card identification data “CID”

### **Swiping the Card**

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

### **Compare Account Numbers**

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

Compare account numbers displayed on the terminal or printed on the sales draft to the embossed number on the

customer's card. If the numbers match, enter the amount of the transaction into the terminal and request authorization. If the numbers do not match, call the authorization center and say, "Code 10." Follow the instructions the operator gives over the telephone.

## Available Fraud Controls

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

## Request Authorization

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

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

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

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

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

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



**Note** *Obtaining an authorization does not guarantee against chargebacks.*


## Print the Sales Draft

Follow these steps if you are using a printer.


1. Have the cardholder sign the printer-generated sales draft.
2. Compare the signature on the sales draft with the signature on the back of the card. Make sure that the signatures match.
3. If the signatures match, hand the cardholder the customer copy of the sales draft and return the card. Your sale is now complete.
4. If the signature looks suspicious, or if you are suspicious about the card, call your voice authorization center at 1-800-944-1111 and request a

Code 10 authorization. You must also take a manual imprint of the sale.

5. If the display on the terminal is CALL, call the voice authorization center number at 1-800-944-1111. When the authorization operator answers, give the following information:
  - Bank Identification Number
  - Your Merchant Identification Number
  - Cardholder Account Number
  - Amount of Sale (dollars and cents)
  - Expiration date on the card
6. Write the authorization code on the provided space on the sales draft.

 **Note** *All transactions authorized by phone need to be re-entered into your terminal in order to be electronically deposited. Follow the instructions in your terminal procedures for Force Transactions, located in your IRN Payment's Quick Reference Processing Guide. Remember to imprint and fully complete a sales slip for all sales that are forced into the terminal. If the terminal is out of order, contact the Terminal Help Desk.*

*To reduce your risk of incurring a chargeback on a fraudulent card, when receiving a referral response, the issuing bank requests an authorization through a voice operator. Contact our voice authorization center and speak directly to an operator. Do not use the Automated Response Unit (ARU) on these voice referral transactions.*

 **Note** *If a terminal swipe is unsuccessful, you must obtain an imprint of the card on a standard sales draft. Complete the sales draft including a signature and attach a copy to the printer-generated draft for your records.*

Follow these steps if your terminal is **not** connected to a printer:

1. Place the card on the imprinter face up. Make sure the card is properly positioned so that all information

embossed on the card and your merchant identification plate is legible on the sales draft.

2. Place the sales draft face up over the card in the imprinter, making sure that the imprinter's guides hold the draft properly.
3. Move the imprinter handle completely across the draft with a quick, firm motion, and return the handle to its original position.
4. Be sure that the imprinted information is legible on ALL copies of the draft. If not, print the complete information above (not over) the imprinted information.  
Note: Truncation mandates do not apply to manual card imprints, only electronically printed cardholder receipts.
5. Use a ball point pen (not a soft felt tip), to enter the date, description of merchandise or services, sales amount, approval code, tax, total and clerk's initials on the draft.
6. Have the cardholder sign the sales draft.
7. Compare the signature on the sales draft with the signature on the back of the card. They must match.
8. Hand the cardholder the customer copy of the sales draft and return the card. Your sale is now complete.

All transactions authorized by phone need to be re-entered into your terminal in order to be electronically deposited. Follow the instructions in your terminal procedures for Force Transactions, located in your IRN Payment Quick Reference Processing Guide. Remember to imprint and fully complete a sales slip for all sales that are forced into the terminal. If the terminal is out of order, contact the Terminal Help Desk.


## 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 don't match ask for additional information, such as a driver's license or another credit card and call voice authorization center for instructions.

If there is no signature on the signature panel on the card, ask for additional information. 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 your records and for protection against possible disputes.

## Accepting Debit and EBT Cards

 **Note** *In order to accept debit and/or EBT cards, you must first sign an agreement with IRN Payment and abide by the policies and regulations in the agreement. See the EBT amendment in the Exhibit Section of this guide for complete details.*

There are two types of debit transactions – online and offline. Online debit or (PIN-Secured) transactions require customers to enter a secret PIN at the point-of-sale terminal and the amount of the transaction is debited from the customers' checking account.

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

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

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

- The merchant is required to honor all valid debit network cards with terms no less favorable than the terms under which the merchant accepts other card types.
- The merchant may not impose a separate fee as a condition for accepting the debit card
- The merchant must not set minimum or maximum transaction amount for debit card transactions, or a minimum amount as a condition for accepting the card

- For PIN-based transactions, the payment terminal shall be equipped with a Personal Identification Number (PIN) entry device for use by the cardholders to enter their PINs. The PIN entry device must be at or in close proximity to the Point of Sale device
- The Point of Sale device must be capable of reading the entire Track II from the cardholder's card
- The merchant may not require or request a cardholder signature. The cardholder's PIN is their electronic signature
- The merchant may not ask the cardholder to disclose their Personal Identification Number
- The receipt for debit transactions are to be produced by 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

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

An EBT card is a magnetic striped plastic card that electronically delivers Federal and State funded Food Stamps and Cash Benefits to qualified EBT recipients.

An EBT card electronically replaces paper food stamps and unemployment insurance checks, as well as other cash benefits; so it eliminates paper processing of food stamps, making it more efficient. It is of similar size and appearance as

other types of payment cards, so that the user does not feel awkward using it.

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.

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

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

### Credit Card Refunds

1. Ask the cardholder for the card used in the original transaction, and compare the account number on that card with the account number on the copy of original sales draft. They must be identical.
2. If the cardholder does not have the card used for the original purchase, use the information on the original sales draft to record the card number, customer name, and expiration date on the credit draft.
3. If you are using a printer, follow terminal procedures for processing a credit, located in your IRN Payment's Quick Reference Processing Guide.
4. If you are 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.

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

### Debit Card Refunds

1. Ask the cardholder for the card used in the original transaction, and compare the account number on that card with the account number on the copy of the original sales draft. They must be identical.
2. Follow terminal procedures for processing a credit, located in your POS user documentation.


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

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

## Card Not Present Transactions

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

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

 **Note** *You cannot accept Card Not Present transactions unless IRN Payment has agreed to process these for you and such provision is contained in your IRN Payment merchant agreement.*

Take precautions to guard against data compromise when taking orders over the Internet, by telephone, mail, or fax. Since a visual identification cannot be made for cardholders requesting fax, mail, phone or Internet card transactions, some personal information must be obtained in order to receive authorization from IRN Payment.

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

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

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

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

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


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

Also, the Cardholder Information Security Program (CISP) from Visa and site data protection from MasterCard (Also known as Payment Card Industry Data Security Standards - PCIDSS) provides a list of Best Practices and other tips. Called the “Digital Dozen,” these twelve controls help you to remain in compliance with your card acceptance agreements when accepting payments over the Internet.

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

Follow these guidelines and the E-Commerce/Internet Services addendum section in the back of this Guide.

1. Install and maintain a working network firewall
2. Keep security patches current
3. Encrypt stored data
4. Encrypt data sent via open networks
5. Always use updated anti-virus software
6. Restrict access to data to a “need to know” basis
7. Assign a unique ID to each user
8. Track access to the data by that unique ID
9. Never use vendor-supplied defaults as passwords or other security features
10. Test the security system and processes regularly
11. Maintain a security policy for employees and contractors
12. Restrict physical access to cardholder information

 **Note** You may access the Visa Cardholder Information Security Program at [www.usa.visa.com/business/merchants/](http://www.usa.visa.com/business/merchants/) section on *Fraud Prevention*

## 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, your customers want to feel safe and secure while conducting Internet transactions. We are aware of the growing popularity of Web-based business and have developed flexible, secure Internet payment processing options that help you and your customers feel at ease.

MasterCard, Visa, 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 terminal. This definition relates to the interaction between the cardholder and the merchant. It is not concerned with how the merchant processes the transaction after the account information is received.

IRN requires that a merchant identify their electronic commerce transactions under a separate merchant number to ensure compliance with Visa, MasterCard, and Discover Operating Regulations. American Express and Discover also have directed us 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 Website and Electronic Transactions Requirements

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

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

## Transaction Receipt Requirements

- Merchant name most recognizable to consumers
  - “doing business as” name (DBA) as used on your website;
  - Merchant “universal resource locator” (URL); or
  - Merchant name used in the Clearing Record
- Customer Service contact, including telephone number (If you deliver goods internationally, include both local and internationally accessible numbers)
- Properly disclosed terms and conditions of the sale, if restricted
- Exact date that free trial period ends, if offered
- Properly disclosed cancellation policies

- A complete and accurate description of the goods or services offered
- Merchant online address
- Description of merchandise/services
- Transaction amount
- Transaction date
- Transaction type (purchase or credit)
- Purchaser name
- Authorization code
- Unique transaction identification number
- Terms and conditions of sale, if restricted
- Return/refund policy (if restricted)

## Completing Mail and Telephone Order Transactions

1. Obtain the cardholder's name, card account number and expiration date and record these on your sales draft. You must also obtain the cardholder's billing address and zip code. (You may need to provide this information when you request Authorization.)
2. Request the three-digit card authentication number (CVV2/CVC2/CID) from the signature panel. (or the four-digit number if approved for American Express CID participation) Note: Merchant retention of this authentication number is strictly prohibited. However, you may record and retain the one-character result code.
3. Fill in a brief description of the goods sold and show the amount of the sale in the space marked "Total."
4. Write TO (telephone order) or MO (mail order) on the signature line of the sales draft.
5. Enter transaction information into terminal or PC. Refer to your IRN Payment's Quick Reference Guide for instructions on manually entering sales transactions.

6. Provide a copy of the sales draft to the cardholder, either with the cardholder order (if being shipped to the cardholder) or separately (i.e. if purchase is a gift). The transaction date is the date goods were shipped to the cardholder. Electronically printed sales receipts provided to cardholder should truncate or mask the account number and the expiration date.



**Note** *An authorization for a phone order, mail order, fax, or Internet transaction does not guarantee against chargebacks. Please ship only to the address verified as the cardholder's. Shipment to a different address jeopardizes your protection from chargebacks. You may verify the billing address of the cardholder with the Authorization Center or the cardholder's bank. The Customer Service Department can provide you with the number of the cardholder's bank if necessary.*

## Completing Recurring Bill Payment Transactions

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

### ***What is a "Recurring Payment"?***

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

utility bills). Other recurring payments may occur for newspaper subscriptions, cable TV service, cleaning service, lawn service, etc.

### ***How is a “Recurring Payment” different from other forms of payment?***

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

A recurring services merchant must obtain a completed “Order Form” from the cardholder containing a written request for the goods or services to be charged to the cardholder's account. An Order Form is a document bearing the cardholder's signature, either written or electronic, authorizing goods or services to be periodically charged to his/her account for recurring services. An Order Form may be any of the following:

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

### ***What should be on an Order Form?***

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

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


Retain the Order Form for the duration of the recurring services (plus an additional 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.

### ***Other Requirements and Prohibitions for Recurring Transactions***

- Partial payment for goods or services purchased in a single transaction is NOT allowed.
- Finance Charges are not permitted on a recurring transaction.
- A recurring transaction can NOT be deposited if the Cardholder has cancelled the payment arrangement.
- A recurring transaction 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, as such a new authorization is required for each recurring charge.
- The floor limit for recurring bill payments is \$0. You must always obtain an authorization and identify recurring bill payments in the authorization request as required by MasterCard, Visa, and Discover.
- Only deposit authorized recurring bill payment transactions.
- Identify recurring bill payment transactions in authorization and clearing record as required by MasterCard, Visa, and Discover.
- Clearing record for recurring transaction 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.

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

## Best Practices for Merchant Use of Convenience Fees

Merchants are prohibited by card association rules 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 a situation in which particular business cases (i.e. government or schools) may warrant imposition of a convenience fee for utilization of specific alternative payment modes, such as Internet and telephone.

The card associations have found that convenience fees are a barrier to card acceptance and various requirements have been established by the card associations. The requirements vary by card association and these 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 payment accepted in the alternative payment channel
- 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

Imposing a convenience fee has been found by the card associations to impede consumer credit card payments, so be aware of the potential for changes to current policy and procedures. Effective April 2005, a special Visa program has been launched for registered Utility MCC 4900 merchants who affirm they will abstain from charging convenience fees associated with bill payments.

A percentage-based fee is permitted ONLY for consumer tax payments. This is a pilot program available at this time for registered merchants only if the merchant or their third party servicer has demonstrated compliance with Payment Card Industry Data Security Standards (PCI DSS).

In the normal course of business, the card associations do not monitor other merchant fees that are uniformly applied to all payment types, such as shipping and handling fees or student registration fees, since they do not discriminate or limit card acceptance. Some merchants, such as ticket sellers and travel agents, may charge consumers for costs associated with the value-added services they provide and the merchant name and other transaction data must indicate the merchant of record. Businesses that facilitate credit card payments for other merchants are subject to additional requirements and require registration and interaction between IRN Payment and the Card Association.

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

## Draft Retrieval Requests


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

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

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

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

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

 **Note** *Contact Customer Service if you would like to receive the retrieval requests via fax rather than U.S. Mail.*

## Sample Sales Draft Retrieval Request

A sample retrieval request letter is shown below.

SAMPLE LETTER				
RETRIEVAL SALES DRAFT REQUEST				
Date				
Merchant Name 1234 Any Street Anytown, State Zip			Global Payments Department CBR 10705 Red Run Blvd. Owings Mills, MD 21117	
<b>Sales Draft Request</b>				
This is a request for copies of sales drafts. To preserve your reversal rights please respond by 00-00-00. 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. Be sure to list case number (given below) for each sales draft. The following items <b>MUST</b> be legible: cardholder account number, transaction amount, transaction date, merchant name/location, expiration date, and cardholder signature.				
<b>ATTENTION: Mail Order/Telephone Order and eCommerce merchants - Please be advised that cardholder signature is not required; however, a substitute sales draft and/or order form must be supplied.</b>				
<u>Merchant Reference</u>	<u>Transaction Date</u>	<u>Transaction Amount</u>	<u>Batch Amount</u>	<u>Cardholder Number</u>
00000000	00-00-00	40.94	0.00	1234567812345687
<u>Processing Reference</u>	<u>Posting Date</u>	<u>BIN/ICA</u>	<u>Case Number</u>	<u>Request ID</u>
1233456789123456	00-00-00	0000	111122223	
<b>Retrieval Reason</b>				
Cardholder does not recognize transaction.				

## Merchant Deposits

If you are using Electronic Data Capture (EDC) to process your credit card transactions, DO NOT submit paper sales drafts for deposit into your bank deposit account. Transaction information should be transmitted to IRN Payment using terminal settlement at the end of each business day. Refer to your IRN Payment's Quick Reference Guide for information on completing terminal settlement procedures. If you are unable to complete a terminal settlement, please contact the Terminal Help Desk for further instructions.

## Lodging Merchants Best Practices

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

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

## Key Dates for Lodging Merchants:

### Check-In Date

Initial Authorization date

Must be after "valid from" date on card

Must be prior to "expiration date" on card

### Check-Out Date

Transaction Date on the transaction receipt and other documents.

### Prepayment Date (Visa)

Transaction Date on the transaction receipt and other documents for an ADVANCE DEPOSIT.

### Delayed or Amended Charges

If the Cardholder has consented to be liable for delayed or amended charges (i.e. costs for room, food or beverage charges), they must be processed to the Cardholder's account within 90 calendar days of Check-out date. This must not include charges for loss, theft, or damage. Complete the transaction and include the words "Signature on File" on the signature line. Send the Cardholder a copy of any amended or additional charges added to a Transaction Receipt within 5 days of entering the charge. Send to the address shown on the folio.

## Data Accuracy

### Name and Location

The business establishment where the transaction took place.

### Transactions Date

Lodging check-out date or prepayment date for a Visa Advance Deposit.

### Merchant Category Code

Generic MCC 7011 (lodging), or merchant specific 3501-3799

### Cardholder Signature

Merchant may deposit the Transaction Receipt without a Cardholder signature if Merchant has the signature on file and cardholder has consented to be liable for charges.

Merchant must write the following words on the signature line of the Transaction Receipt:

<u>Transaction Type</u>	<u>Signature Line Printing</u>
No Show	NO SHOW
T&E Advance Deposit	ADVANCE DEPOSIT
Express Check-Out	SIGNATURE ON FILE
Delayed Charges	SIGNATURE ON FILE

## Authorizations

### Card Present

The full magnetic stripe must be read and transmitted with the initial authorization request. Additional/incremental authorizations do NOT alter the original “card present” indicator.

### Estimated Transaction Authorization

A lodging establishment must estimate transaction amounts for Authorization based on the following:

- Cardholder's intended length of stay

- Room rate
- Applicable tax
- Other allowed charges

### Incremental Authorization

Visa allows incremental authorizations. Data from original authorization must be retained and returned with incremental authorizations.

### Total Authorized Amount

Visa allows the sum of the initial and incremental authorizations, less a MAXIMUM of one reversal per transaction, to be used to adjust the Total Authorized Amount to be equal to the settled amount. If sum of initial and incremental authorizations is within 15% of the settled amount, an authorization reversal is not required. Understand and promote the recording of all authorization amounts, approval codes, and authorization dates on the folio.

### Request for Copy/Travel & Entertainment (T&E) Original

1. Fulfill requests for copy (RFC) or T&E document(s) in a timely manner
2. Fulfill request with substitute draft rather than risk loss
3. Substitute Transaction Receipt Requirements For Lodging Transactions:
  - Cardholder account number
  - Card expiration date (if available)
  - Cardholder name
  - Guest name
  - Transaction amount
  - Itemized charges
  - Room rate
  - Tax
  - Food, beverage
  - Incidental charges
  - Authorization code(s)


- Guest folio number
- Dates of stay
- Check-in date
- Check-out date
- Merchant name
- Property location

## **Advance Deposit Service for Pre-payment of Resort Lodging Accommodations - Sales Draft Checklist**

### **Reservation Clerk Procedures**

To accept an Advance Deposit reservation, the reservation clerk must explain the terms of the reservation, cancellation, and refund policy procedure to the cardholder or travel agent or must display on internet site with “I agree button”

To process an Advance Deposit reservation, the reservation clerk or travel agent completes a sales draft filling in the merchant identification and cardholder information as listed below. Send the cardholder a written reservation confirmation, a copy of the sales draft, and your cancellation and refund policy.

 **Note** *It is recommended that the merchant note on the sales ticket any special terms and conditions regarding its refund policy. Merchants must properly identify the prepayment date as the transaction date when submitting Advance Deposit transactions. The merchant mails to the cardholder a copy of the draft, and letter of confirmation if requested.*

### **Reservation Clerk requests from Cardholder**

- Cardholder name
- Cardholder account number
- Card expiration date
- Cardholder phone number
- Cardholder billing address

### **Reservation Clerk provides to Cardholder during call**

- Confirmation code
- Total amount of advance deposit

### **Reservation Clerk provides transaction information to Cardholder on Sales Draft**

- Transaction date (date of pre-payment)
- Authorization code (NOTE: Zero floor limit; application must provide all required data to qualify for Lodging CNP rate)
- “ADVANCE DEPOSIT” on signature line
- Hotel merchant name and location
- Scheduled arrival date
- Cancellation deadline (date and time)
- Written cancellation policy
- Mail copy to guest

### **Credit Voucher Checklist**

To process an Advance Deposit Cancellation, use a credit voucher (or your terminal and printer) and Reservation Form. Mail a copy of the credit voucher reflecting the cancellation to the cardholder.

- Cardholder name
- Cardholder account number
- Card expiration date
- Advance deposit cancellations code
- Total amount of credit
- Write “DEPOSIT CANCELLATION” on signature line
- Mail copy to guest

### **Priority Check-Out Service**

**Priority Check-Out Service** allows lodging merchants to complete the final check-out transaction without requiring the cardholder presence. This offers your guests the

convenience of a Priority / Express Check-Out. The cardholder/guest signs a Priority / Express Check-Out Service agreement authorizing a charge to the specified account for the final amount of the bill without requiring the cardholder's signature at checkout. At time of check-in, imprint a sales ticket with the cardholder's account number, and follow its normal authorization procedures. The cardholder is provided with the itemized bill (within specified timeframe).

Retain all pertinent records relating to the itemized bill and authorization requests in the event of a dispute.

- Name, address, and telephone number of the hotel, motel, or resort
- Cardholder account number
- Cardholder billing/ mailing address
- Applicable charges posted after check-out
- Cardholder's signature
- Cardholder's room number
- Provide itemized bill and copy of completed sales draft to guest within 3 days after checkout.
- If requested, provide copy of Express Check-Out Agreement  
Sales Draft Checklist

**To process Priority Check-Out Service.**

If requested by the cardholder, send them copies of the completed sales draft, the itemized hotel bill, and the Priority / Express Check Out Agreement (if requested).

- Cardholder name
- Cardholder account number
- Card expiration date
- Total charges incurred during the stay
- Delayed charges (posted after check-out)
- Authorization code
- "SIGNATURE ON FILE-EXPRESS CHECKOUT"  
printed legibly on the signature line
- Mail copy to guest, if requested

**Sample Forms and Letters**

**Guaranteed Reservations**

Guaranteed Reservations –  
Confirmation / Cancellation / Check-In Form

*Obtain the following from cardholder (in addition to reservation information):*  
Cardholder name:  
Cardholder address:  
Cardholder account number:  
Card expiration date:

*Reservation information:*  
Arrival date:  
Number of nights:

*Advise the guest of the following:*  
Room rate and applicable taxes:  
Accommodation request (such as non-smoking room, king size bed)  
Confirmation code for guaranteed reservation:  
Importance of keeping confirmation code for future reference:  
Deadline for cancellation without penalty before 6 pm on scheduled arrival date:  
Hotel name and location:  
Written confirmation notice requested / sent:

*Cancellation information:*  
Cancellation code:

*Advise guest to retain*  
Written cancellation notice requested / sent:  
Pre-Registration information:  
Registration card prepared:  
Room number assigned:

*If No Show, retain reservation form, pre-registration card, etc. for six months. Note: See Retention section for important information on safeguarding data*

## Priority/Express Check-out Sample Form

[MERCHANT NAME]  
[MERCHANT LOCATION]  
[MERCHANT TELEPHONE NUMBER]

---

PRIORITY/EXPRESS CHECK-OUT  
CASHIER, PLEASE CHECK ME OUT OF:

Room # \_\_\_\_\_ on \_\_\_\_\_  
Departure Date

---

Guest Name (please print)

I authorize a charge to my Visa or MasterCard Card account number imprinted on my Sales Draft for the amount of all costs incurred during my stay.

Cardholder Signature \_\_\_\_\_  
(NOTE: *must contain full account number*)  
\_\_\_\_\_

Visa or MasterCard Card Account Number \_\_\_\_\_

Please send a copy of my lodging receipt and my Sales Draft to the address listed below.

I also want you to send a copy of this agreement.

---

Name (please print) \_\_\_\_\_

---

Company \_\_\_\_\_

---

Street \_\_\_\_\_

---

City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

## No Show Charge - Sample Letter

**Send to Guest upon Billing of "No Show"**

[MERCHANT NAME]  
[MERCHANT LOCATION]  
[MERCHANT TELEPHONE NUMBER]

Dear \_\_\_\_\_

We missed you! We held a room/suite at the (name of hotel) for your arrival the evening of (date), and were sorry to discover that you didn't arrive as planned.

Our records show that the room was held in the name of \_\_\_\_\_, and was guaranteed with a (name of credit card), number \_\_\_\_\_.


Because your room was guaranteed, and we don't have a record of your canceling your reservation, we have charged the credit card you guaranteed the room with for the amount of one night's rate. If we've overlooked any pertinent information or you have a cancellation number, please contact me at the hotel during daytime business hours.

We're sorry you weren't able to stay with us this time, and we hope we'll have another opportunity to serve you.

Sincerely,

General Manager  
Hotel Name and Phone Number

Enclosure (facsimile or credit card charge receipt)

 **Note** Check to ensure that the guest's name is spelled correctly and that this really is a No Show and not a reservation with an incorrect date of arrival.

## Processing a "No Show" Reservation

If accommodations reserved under the Visa/MasterCard/Discover Reservation Service have not been claimed or cancelled 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 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 of transaction record.

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

## Chargebacks


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

## Some Do's and Don'ts of Chargebacks

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

- Do not charge a cardholder before shipping the merchandise
- Do not accept sales that are declined, and if a sale is declined, do not attempt authorization a second time on a declined sale. *The cardholder bank may collect a \$50.00 fee if you fail to follow card acceptance and authorization procedures.*
- Do not accept sales that are not authorized for the exact amount
- Do not accept an expired card
- Do not accept a card before the effective date on a dual dated card
- Do not process a credit as a sale
- Do not deposit the sales draft more than once
- Do not deposit an incomplete sales draft
- Do not accept a sales draft without a cardholder signature
- Do not participate in a suspicious transaction
- Do not obtain an authorization by using multiple transaction/split sales drafts

- Do not accept a card where the account number obtained off the magnetic stripe does not match the account number on the draft
- Do understand that you assume all responsibility for the identity of the cardholder for all fax, Internet, mail order and telephone order sales
- Do prepare and submit a written rebuttal within the time specified on the chargeback notification
- Do accept cards where the cardholder account number is valid
- Do authorize all sales
- Do verify arithmetic on sales drafts
- Do charge the cardholder for the correct amount
- Do deposit the sales draft before the contractual time limit
- Do credit the cardholder for the returned merchandise
- Do credit the cardholder for a canceled order
- Do verify that the signature on the sales draft matches the signature on the card
- Do verify the authorization code
- Do obtain a manual imprint, if unable to capture from magnetic stripe

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

## Your Right to a Rebuttal

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

## Understanding Your Statement

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

## Questions About Your Statement

If you think your statement is incorrect, or if you need more information about a transaction on your statement, please contact us via letter. We must hear from you no later than 60 days after the first bill, on which the error or problem appeared, was sent. You can phone us; but doing so will not preserve your rights.

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

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

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

**Note** All statement related (billing) inquiries should be received by IRN Payment within 60 days of the date of the statement containing the discrepancy.

## Sample Statement

Your monthly account statement.  
It's easy to understand!

**Merchant Statement**

globalpayments<sup>®</sup>

XYZ CORPORATION  
0000 ANY STREET  
CITY, STATE 12345-6789

CREDIT CARD MERCHANT STATEMENT  
DATE: 02 03 1111 PAGE: 1 OF 1  
CODES: N FORM: 9 0 10000048  
MERCHANT: 1234 000 12345  
DBA: XYZ CORPORATION

INFORMATION ONLY

CHARGEBACKS				CREDITS	DISC	AMOUNT
DAY	REF NO.	ITEMS	AMOUNT			
	0	00		.00	.00	.00
CHARGE TOTALS	0					

DEPOSITS				CREDITS	DISC	NET DEPOSIT
DAY	REF NO.	ITEMS	SALES			
16	2532787800	6	84.00	.00	.00	84.00
17	2532787800	8	84.30	.00	.00	84.30
DEPOSIT TOTALS	2	2	168.30			168.30

DEPOSIT ITEM SUMMARY				DISC ADJ.	CR ADJ.	TOTAL
SALES	14		168.30	0	0	0
CREDITS	2		168.30	0	0	0
TOTAL	14		168.30	0	0	0

SETTLEMENT/DISCOUNT				DISC RATE	ITEM RATE	SEE AMOUNT
DESCRIPTION	ITEMS	AMOUNT	AVG TICKET			
VISA	5	60.00	9.22	2.5700	.00	1.18
MC	9	122.22	13.58	2.5750	.00	3.14
TOTAL						4.32

MINIMUM BILLING ADJUSTMENT CREDIT CARD: 20.00

YOUR ACCOUNT HAS BEEN DEBITED.

STATEMENT MESSAGE: WELCOME TO YOUR NEW MONTHLY STATEMENT. IF YOU REQUIRE CUSTOMER SERVICE, PLEASE CALL 1-800-367-2639, 24 HOURS A DAY.

## Working Together to Prevent Fraud

As your merchant advocate, IRN Payment utilizes a sophisticated fraud detection system that monitors all card transactions, 24 hours a day, seven days a week. This fraud detection system is one way of protecting your business. Reading and complying with the standards and the policies in this guide will be your best defense against fraud and help you remain in compliance with your merchant agreement.

A merchant must not, in the event of its failure, including bankruptcy, insolvency, or other suspension of business operations, sell, transfer, or disclose any materials that contain Cardholder Account Numbers, personal information, or credit card transaction information to third parties. The merchant must return this information to IRN or provide acceptable proof of destruction of this information to IRN.

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

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

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

## Prohibited Transactions

Merchants who accept credit cards must be aware of prohibited transactions and the penalties that can be imposed if a prohibited transaction is completed. A prohibited transaction is one that does not comply with the operating regulations of the Visa, MasterCard, and Discover associations, and/or policies and procedures as defined in the IRN Payment merchant agreement. If deposited, sale drafts involving prohibited transactions will be subject to

chargeback and may lead to termination of the IRN Payment merchant agreement, perhaps immediately!

The following are examples of prohibited transactions:

- Processing transactions to cover previously incurred debts (Visa allows if existing debt transactions are identified properly and account is not in collection), or bad debt such as bounced checks, or payment for returned merchandise
- Processing a sale on a previously charged back transaction
- Accepting transactions that are declined by the Authorization Center
- Attempting multiple authorization requests following a decline
- Accepting cards with an invalid effective date
- Accepting expired cards
- Using a split sale to avoid authorization requirements
- Giving cash to the cardholder 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 Visa or MasterCard 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 you may own or purchase, but are not explicitly listed in your current application (or supplements to it) currently on file with us. Laundering of deposit drafts will likely result in the immediate termination of your Merchant Bankcard privileges
- Depositing a sales draft twice
- Depositing a sales draft in one or more financial institution for payment before or after you deposit it with IRN Payment

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

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

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

### ***Take Charge of Chargebacks***

Chargebacks are one of the most common - and costly - ways that fraudsters take advantage of merchants. For example, some fraudsters, appearing to be legitimate customers, will 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. And, since your company has no record of the transaction, the full amount is credited back to the consumer, and you face a loss.

There are steps you 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***

- If you process transactions manually, be sure to take an imprint of the card every time a purchase is made with a credit card
- Be sure to call in for authorization for every credit card transaction
- Make sure you neatly print the sales draft so that it is clear and easy to read
- Don't forget to write your merchant number on the draft

- Have the customer sign the receipt while you watch and verify that this signature matches the one on the back of the card
- Don't divide one purchase on to 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 a transaction has been cancelled by the customer, take the required steps to stop, reverse, or stop the billing immediately
- Be sure to display your return policy at the point of sale and on sales slip - remember, it is your 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 your sales draft in case of future disputes

### ***Processing Transactions through an Electronic Point-of-Sale Terminal***

- Be sure to always swipe the card through an electronic point-of-sale device whenever possible – keying in transactions increases your exposure to chargebacks
- Be certain your return policy is stated clearly on all of your materials or receipts
- Keep your point-of-sale equipment clean and operating efficiently

### ***Mail and Telephone Orders***

- If possible, establish the customer's identity by writing their name, address, credit card number, and expiration date on the sales draft
- Be sure to obtain an authorization for every sales transaction
- If you are taking an order over the phone, fax, Internet, or by mail, only ship items to permanent

addresses – steer clear of post office boxes or 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

### ***Protecting your eBusiness***

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

If you are creating or operating an online store, be sure to learn about security risks by assessing your shopping cart procedures, securing your online transactions, and letting your customers know that your Web site transactions are safe.

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

- Post your purchase policies on your Web site where your 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 your usual orders, as well as international orders, especially if express shipping is requested
- Note the customer’s e-mail 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 your account – if any items are charged back, you will be responsible for them
- If you are skeptical of an order, call the customer to confirm

### ***Factoring or Draft Laundering***

Factoring (or draft laundering) scams occur when another merchant’s sales are processed through your merchant account, or any time receipts are processed outside of the terms of your merchant agreement. Criminals often accomplish this act by asking for a favor from a business owner or bribing someone they know.

Some merchants and employees, however, are not aware that processing another person’s information on the account is illegal. For example, if an individual operates two separate businesses, they cannot process one store’s sales through the other store’s merchant account. Since you are ultimately responsible for all transactions that run through your merchant account, if any items are charged back, you are held responsible, and your account will be debited for these transactions.

The reality is that if fraudulent transactions are processed through your terminal through factoring, you are in violation of your merchant agreement, and as a result, you could be fined and prosecuted.

### ***Card Not Present Scams***

The risk of fraud increases greatly if your customer and their credit card are not present at the time a purchase is made because you don’t have the opportunity to inspect the card. “Card not present” transactions typically occur over the telephone or fax, through the mail or over the Internet.

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

If you are processing card transactions by telephone, mail, fax or Internet, make sure that you have signed the specific merchant agreement required to perform these transactions where the card is not present. Even after you have the proper

agreement in place, it is crucial that you take the precautionary steps to prevent potential chargebacks.

### ***Skimming***

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

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

### ***Don't Be Bullied***

Here, the customer attempts to intimidate the cashier by causing a fuss at the register so that the purchase is rushed, which may lead to improper check out. They may tell you that the card won't read and not to bother running it through – that you'll have to key it in manually. In such instances, customers have also been known to complain about the service or length of the line. They may even demand to see a manager – anything to keep the cashier's attention off the authorization of the credit card.

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

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

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

### ***Deceptive Deliveries***

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

### ***The Manual Key-In***

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

If you have an electronic point-of-sales terminal, swipe every card that you come across – no matter how damaged or worn. And be wary of customers who let you know right away that their card won't read. If the card doesn't work and you end up keying in the number, make sure you take an imprint of the card. If the card is severely damaged, simply ask for another form of payment.

### ***Borrowed Cards***

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

## ***One Person's Trash Is Another's Gold Mine***

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

Your “trash” could be a thief’s treasure, with all of the information a criminal needs to make a false card, as well as information about your company that could hurt you later if it fell into the wrong hands. Recognize materials that may contain private information and dispose of them properly. Destroy any documents that have any personal information on them with a paper shredder before declaring them trash. Protecting your customers and your business is worth a few extra seconds.

## ***The Terminal Repair Scam***

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

You may not even see it coming, as these criminals often pretend to work for POS companies or say that they are attending to other official business. Any attempt to repair your terminal should be reported to the police, and no replacement terminals should be accepted. The safest thing you can do is to be cautious and report any suspicious happenings immediately by calling the Help Desk number on page 1 of this guide. They will check to see if there is a replacement request noted for your location.

## ***Fraudulent Returns***

Fraudulent returns are a major problem associated with fraud and theft. Staff members have been caught returning items that

were never purchased and pocketing the money. In some cases, merchants don’t even realize they have been victimized until it is too late. Make sure your employees take the necessary steps to ensure this doesn’t happen in your business. IRN Payment’s terminals can also limit access to returns by requiring the use of passwords. (See the terminal documentation)

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

## ***International Credit Cards***

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

Inspect the card thoroughly, checking to make sure the card is valid, and always swipe it. The main elements of the card – logo, hologram, clear embossing and so on – should be the same despite where the card originated. Check to make sure the signature matches the name on the card, and that once swiped, the number on the terminal matches the number on the card. Also, watch out for customers who check out the cashiers first before getting in line – criminals often look for an inexperienced clerk or someone who may be easily intimidated. If anything seems suspicious during the transaction, call in a Code 10.

## ***Office Products Scams***

Watch out for companies trying to sell office products such as copy paper, ink cartridges, stationery and other supplies to

your business. They may try to appear as if they are working for a reputable company. In reality, they will overcharge you for inferior merchandise. Deceptive telemarketing is a violation of the law – report any suspicious persons immediately.

### ***Phone Fraud***

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

These crooks still use the phone to swindle merchandise from the retailer. Most of the time the criminal will phone a store, telling the clerk he has picked out the items he wants but cannot come to pick them up for some reason or another. He will ask the clerk to run his credit card through and assure the clerk that a courier will be by to pick up the merchandise. Once the merchandise has left the store, there is no way of knowing to whom it actually went or where it was going.

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

### ***Point of Sale Protection***

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

### ***The Last Minute Shopper***

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

### ***Counterfeit Cards***

Stolen and counterfeit cards are a huge problem for merchants and credit card issuers alike. Because of the technology available to them, counterfeiters are able to reproduce false cards that are high quality, even without the benefit of the original. All they really need is personal information and technology to produce credit cards, debit cards and smart cards. The result is a huge financial loss to businesses around the globe. The card association rules prohibit retention of magnetic-stripe or card authentication numbers (CVV2/CVC2/CID) by merchants or their third-party terminal providers since this information could be used to counterfeit cards.

Protect your business by teaching your staff to recognize the signs of a false card. When to call in a Code 10:

- If the embossing on the card is illegible

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

### ***Don't Hesitate! Call In a Code 10***

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

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

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

### ***Defeating Fraud Helps You and Your Customers***

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

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

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

## Spotting Counterfeit/Altered Cards

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

### Color

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

### Embossing

Check to see that the account number and name embossing 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.

MasterCard embossing starts with a 5. Visa card embossing starts with a 4 and Discover embossing starts with a 6. The first four digits of the card number correspond to a small number printed on the card face just above the account number.

### Signature Panel

The signature panel is printed with a colored MasterCard or 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 your sales draft. All or a portion (last four digits) of the account number and card authentication (CVC2 or CVV2) are printed.

### 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 you rotate the card.

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.

## MasterCard Formats

The same basic design is used for all MasterCard cards. Until all cards are replaced by the new format, you may see the two previous MasterCard card formats at your place of business. 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 and don't hesitate to call for a Code 10 authorization if you are suspicious.

### Security Features

The following features appear on MasterCard cards:

- The unique security character, embossed on the lower right portion of the card front, is your 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 indented printed on the signature panel.

## Visa Card Formats

Every Visa card is designed with special security elements to deter counterfeiting and alteration. When you are presented

with a Visa Classic, Visa Gold (Premier), or Visa Business Card, look for the following security elements:

### Security Features

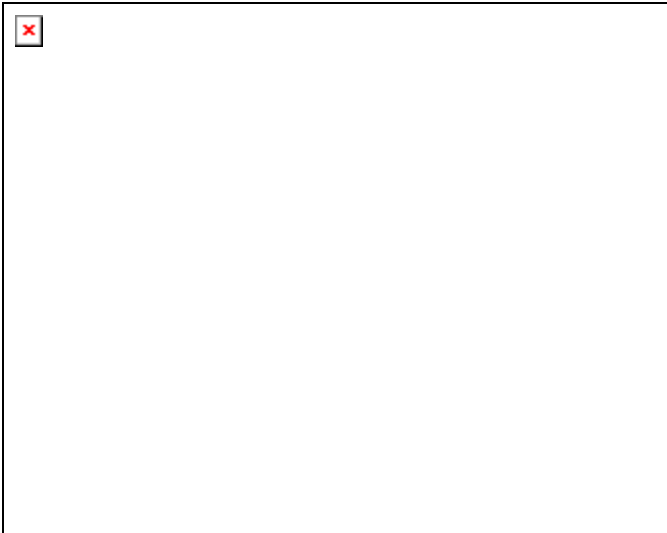
The following features are required for all VISA cards and must appear on all cards:

- 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.

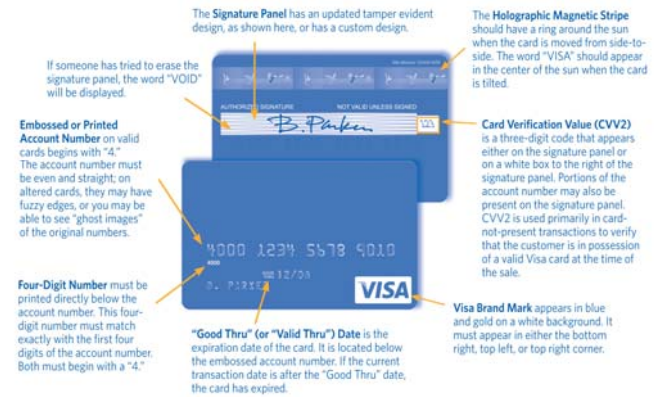


- 1 All MasterCard® account numbers start with 5. The embossing should be clear and uniform in size and spacing and extend into the hologram.
- 2 A three-dimensional hologram with interlocking globes should reflect light and seem to move as you rotate the card. The word "MasterCard" is printed repeatedly in the background of the hologram. The letters "MC" are micro-engraved around the two rings.
- 3 The 16-digit account number embossed on the card must be exactly the same as the account number printed on the sales draft, or displayed on your terminal (if equipment allows).
- 4 The magnetic stripe should appear smooth and straight, with no signs of tampering.
- 5 The word "MasterCard" is printed repeatedly in multicolors at an angle on a tamper-evident signature panel. You may see only the last four digits of the account number, plus the three-digit CVC2 indent-printed on some newer cards. Some cards may contain the full 16-digit account number, followed by the three-digit CVC2, indent-printed on the signature panel.
- 6 The back of the card must be signed and the signature should reasonably compare with the signature on the sales draft.
- 7 MasterCard cards have a stylized "MC" security character embossed to the right of the valid dates.
- 8 The valid date lists the last day on which the card is valid. Some cards may have an effective date as well.
- 9 The pre-printed Bank Identification Number (BIN) must match the first four digits of the embossed account number.

**If you are ever suspicious about the card, call your Voice Authorization Center and request a Code 10.**



### Cards with Visa Holographic Magnetic Stripe on Back of Card



## 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).

### Security Features

- Card Numbers are made up 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;

- 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.

## JCB Card Formats

All Cards bearing the JCB Mark, displayed below, include the following common characteristics and distinctive features:

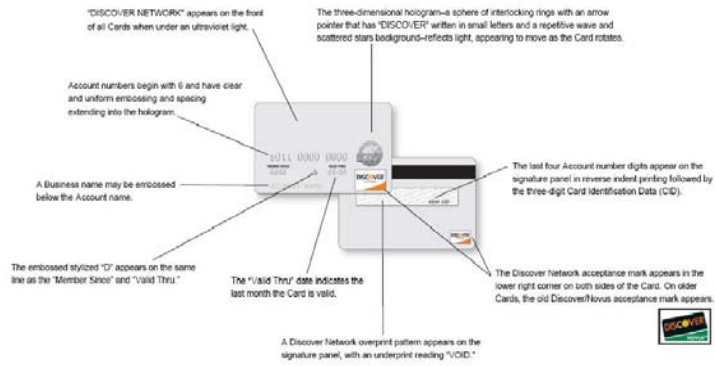
### Security Features

- 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, is embossed on the front of the Card.
- The JCB Mark appears on the front of the Card.
- A three-dimensional hologram image of rising sun, rainbow and 'JCB' in microlettering 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/yy 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.
- The first 4 digits of the Card Number match the 4-digit number pre-printed just below the embossed Card Number on the front of the Card.
- The first 4 digits of the Card Number displayed on the signature panel on the back of the Card match the last 4 digits of the Card Number that appears on the front of the Card.
- The last 4 digits of the Card Number on the back of the Card are followed by the 3-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.



**Note** *Some valid Cards bearing the JCB Mark will 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 Card Sale. If the Merchant accepts a Card that displays a printed, rather than embossed, Card Number and the Merchant is required to obtain a Card imprint, the Card 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.*



## Pick Up Card Procedures

If you receive a pick up card response from your terminal or the Authorization Center, you are eligible for a cash reward from IRN Payment. Simply cut the card in half directly through the entire account number.

Place the card in an envelope along with your name, merchant number, date of pick up, and your address and mail it to:

IRN Payment Systems  
 Settlements  
 800 Shames Drive  
 Westbury, NY 11590

## Limited Acceptance Merchants

Legal actions indicate that it is your decision to accept certain types of cards. For more information on card acceptance policies, please see the Industry Initiatives section of our Web site at [www.IRNPayment.com](http://www.IRNPayment.com).

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

## Exhibits



**Note** *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 Visa, MasterCard and Discover.*

## EBT Card Services Agreement

### 1. Agreement to Issue Benefits.

IRN Payment System ("IRN") 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 IRN 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. IRN 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 IRN's 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 IRN 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 IRN 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 IRN, 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 IRN.

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") terminal, 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 IRN, 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 IRN 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 IRN.

(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 IRN and the State's EBT Service Provider of the discrepancy; the State's EBT Service Provider and MERCHANT and/or IRN shall compare records to determine the source of such discrepancy. The State's EBT Service Provider and MERCHANT and/or IRN 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 IRN 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 IRN 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 IRN, 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 IRN's, 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 IRN, 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, IRN 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 IRN 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 IRN, 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 thereunder.

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 IRN 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 IRN, 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 IRN, 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 IRN 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 IRN, 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 IRN, 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.

### **E-Commerce/Internet Services Addendum**

1. You agree that all E-Commerce/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 E-Commerce/Internet transactions, you may incur a chargeback on all E-Commerce/ Internet transactions, in accordance with the appropriate VISA, MasterCard, 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 merchandise return and refund policy clearly displayed on either the checkout screen, or on a separate screen that allows the purchaser to click an acceptance button
  - your consumer data privacy policy and 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 E-Commerce/Internet transactions that is capable of providing the required information set out by IRN Payment from time to time in accordance with VISA, MasterCard, 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 E-Commerce/Internet transaction:
- Merchant name most recognizable to consumers
    - “doing business as” name (DBA) as used on your website;
    - Merchant “universal resource locator” (URL); or
    - Merchant name used in the Clearing Record
  - Customer Service contact information including telephone country code and area code. If you deliver goods or services internationally, you must list both local and internationally accessible telephone numbers

- 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
  - Exact date free trial period ends, if offered
  - Cancellation policies
  - 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 IRN 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 IRN:

- 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 website, 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.

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 IRN 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, and Discover.
16. You agree that IRN, Member, MasterCard, VISA, and Discover have the right to perform periodic audits of your website to confirm that you are adhering to the policies and procedures laid out in this agreement and any written directions issued by IRN.
17. You agree to pay any fees or charges relating to E-Commerce/Internet services set by IRN 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.

## **Telephone And Mail Order Services Addendum**

Pursuant to the Merchant 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 IRN's prior consent before offering such services, and (ii) comply with the terms herein and any written directions issued by IRN 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 IRN, IRN 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 IRN for all chargebacks relating to telephone order/mail order and /or Internet sales and indemnifies IRN for all costs, fees and expenses in connection therewith.

Merchant will not, under any circumstances, process Visa or MasterCard sales for another merchant, person, or entity. Any person or entity that wants to accept MasterCard 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 regulations and a breach of the Merchant Agreement. If IRN discovers any Merchant has been factoring drafts, such Merchant may be terminated and its name will be placed on the terminated merchant file with Visa, MasterCard, 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 IRN, 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 IRN for all chargebacks relating to telephone order/mail order sales and hereby agree to indemnify IRN and Member for all costs, fees and expenses in connection therewith.
5. Processing for Third Parties, you will not, under any circumstances, process VISA or MasterCard sales for another merchant, person or entity. Any person or entity that wants to accept VISA/MasterCard 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 regulations and constitutes a breach of your obligations under this Agreement. If IRN discovers that you have been factoring or laundering sales drafts, IRN may terminate this Agreement effective immediately and may place your name on the terminated merchant file with VISA/MasterCard, 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.

## **Visa/MasterCard Reservation 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 Visa, MasterCard, and Discover 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).

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), 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.

**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 Visa, MasterCard, 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**

Lodging Merchants must comply with the following provisions for Advance Lodging Deposit Service transactions:

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.

**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 Visa, MasterCard, 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, which must contain, but is not limited to, the information required in the attached Sample Form.
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.

## Sponsoring Institutions

For a list of all sponsoring institutions, please visit [www.IRNPayment.com](http://www.IRNPayment.com) and view the Industry Initiatives section.

IRN Payment System is a registered ISO and MSP of Palm Desert National Bank, USA, Palm Desert, CA

## Glossary

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

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

*Authorization:* Verification of a bankcard transaction by a bankcard-issuing bank or other institution, or by an approved independent service provider. Authorization is initiated by accessing (by voice or electronic terminal, as appropriate) IRN Payment designated authorization center(s). Authorization is based on the cardholder account status and available credit.

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

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

*CISP:* Cardholder Information Security Program (CISP) from Visa.

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

*Cardholder 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 both 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.

*Cardholder:* The person or entity whose name is embossed on a card or whose name appears on a bankcard as an authorized user.

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

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

When used as a noun, a bankcard transaction which is debited to the deposit account by IRN Payment, set-off against any other account maintained by the merchant with IRN Payment or presented directly to the merchant by the bank for repayment when the deposit account does not contain sufficient funds. When used as a verb, the act of debiting the deposit account, setting-off against another account or otherwise recovering, or seeking to recover, the value of the transaction.

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

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

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

*Code 10:* A universal code that provides merchants with a way to alert the authorization center that a suspicious transaction is occurring without alerting the cardholder (or other person presenting the 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 for Commercial use, often with a higher discount expense than consumer cards. Non-T&E (Travel & Entertainment) merchants accepting a large volume of Commercial Cards should utilize a product that will support entry of sales tax and customer code.

*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 perks. These cards may be subject to higher discount expense associated with Rewards Cards.

*Consumer Card:* A card issued to a consumer.

*Consumer Rewards Cards:* Visa Infinite Card, Visa Signature Card, Visa Signature Preferred Card, Visa Rewards Card, and MasterCard World Cards, and MasterCard World Elite Cards issued to consumers have additional perks. T&E merchants incur additional discount expense for these upscale cards. Effective April 2005, Consumer Rewards Cards use at non-T&E merchants may be subject to higher interchange expenses.

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

*Cross Border Fee:* A transaction where the merchant country and cardholder country are different. MasterCard cross border transactions subject to cross border fee are summarized on merchant statement.

*Debit Card:* A plastic card used to initiate a debit transaction. In general, these transactions are used primarily for goods and services and to obtain cash, for which the cardholder's checking account is debited by the card-issuing institution.

*Deposit Account:* A business checking account designated by the merchant through which all bankcard transactions and adjustments are processed by IRN Payment.

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

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

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

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

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

*MasterCard/VISA Interchange Systems or Interchange System:* Processing systems, which facilitate the interchange and payment of transactions between cardholders and persons, and entities (including merchant) that accept cards.

*Merchant:* A person or entity entering into merchant agreement with IRN Payment, as well as all personnel, agents and representatives of the merchant.

*Merchant Identification Number:* A 6 to 16-digit number each merchant is provided under the IRN Payment merchant agreement.

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

*Off-Line Debit Card:* A 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.

*On-Line 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 on-line debit cards.

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

*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/>

*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.

*PIN:* Personal Identification Number. The confidential individual number or code used by a cardholder to

authenticate card ownership for ATM or POS terminal transactions.

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

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

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

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

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

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

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

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

*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 terminal provider) that assists merchant 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 association 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, MasterCard Secure Code))
- Data Capture

*Voice Authorization:* Authorization obtained by telephoning a IRN Payment voice operator.

**Notes**

**Notes**