

**MERCHANT OPERATING GUIDE**  
**GENERAL RULES APPLICABLE TO ALL TRANSACTIONS**

**1 Acceptance Of Certain Payment Instruments**

In offering Visa and MasterCard payment options to your Customers, you may elect any one of the following options: (i) accept all types of Visa and MasterCard Payment Instruments - including consumer credit and debit/check cards, and commercial credit and debit/check cards; (ii) accept only Visa and MasterCard credit cards and commercial cards (if you choose this option you must accept all consumer credit cards (but not consumer debit/check cards) and all commercial card products, including business debit/check cards; or (iii) accept only Visa and MasterCard consumer debit/check cards (if you choose this option you must accept all consumer debit/check card products (but not business debit/check cards) and will not accept any kind of credit cards). The acceptance options above apply only to U.S. domestic Visa and MasterCard Payment Transactions and, as such, they do not apply to Visa or MasterCard Payment Instruments issued by non-U.S. banks. In other words, if your Customer presents a Visa or MasterCard Payment Instrument issued from a European or Asian bank, for example, you must accept that card just as you would any other card (provided you receive a valid authorization and confirm the identity of the Customer, etc.), regardless of the acceptance option choice you have made and even if you have elected not to accept that type of Payment Instrument from U.S. issuers. If you choose to limit the types of Visa and MasterCard Payment Instruments you accept, the following rules apply to you: (i) you must display appropriate signage to indicate acceptance of the limited acceptance category you have selected (that is, accept only debit/check card products or only credit and commercial products; (ii) if you elect limited acceptance, any Transaction Data submitted into interchange outside of the selected product category will be assessed the standard interchange fee applicable to that card product and may also have additional fees/surcharges assessed; and (iii) additional Visa and MasterCard Rules that may be applicable to you may be viewed on their respective websites.

**2 Authorization/Approval Codes**

All Payment Transactions and Conveyed Transactions require authorization/approval codes. You must request and receive an authorization/approval code for the total amount of the Transaction. An authorization/approval code indicates (i) the availability of credit on the Payment Instrument at the time of inquiry, and (ii) that the Payment Instrument account number is valid. It is not a promise or a guarantee that you will receive payment for that transaction. It does not warrant that the person presenting the Payment Instrument has the authority to do so.

**3 Refunds/Credits**

You must disclose your return/refund policy to your Customers. You must complete a credit for the total amount of the refund and identify the merchandise being returned and any shipping and handling charges being returned. You must imprint or record the credit voucher with the same Payment Instrument used to make the original purchase. For retail Payment Transactions and Conveyed Transactions, the credit voucher must be dated and signed by the Customer and the appropriate copy provided to the Customer. Cash refunds should never be issued for Payment Transactions or Conveyed Transactions, unless required by law. If you fail to follow these procedures, you may be unable to rebut a Chargeback from the Customer for failure to issue a refund (even if you actually gave the refund by cash or check). Paperwork is not necessary for an even exchange. For an uneven exchange, complete a credit for the total amount of the merchandise being returned and complete a new Transaction receipt for any new merchandise purchased. You cannot process a credit or refund without having completed a previous purchase Transaction with the same Customer.

**4 Processing Of Transaction Data**

You must submit Transaction Data (including credit vouchers) to us on or before the next business day after the date of the Transaction. Late submission of Transaction Data may result in higher Payment Brand fees and interchange rates, Chargebacks and other negative consequences. You must not submit Payment Transactions or Conveyed Transactions for payment until the goods are delivered, shipped, or the services are performed (except as otherwise provided in the Merchant Agreement, and only if you have notified us that you are doing so on your application or otherwise in writing). If the Customer disputes being charged for merchandise or services before receiving them, the result will be a Chargeback to you. We may from time to time contact Customers to verify that they have received goods or services for which Transactions have been submitted. You cannot present for processing any Transaction Data that was not originated as a result of an act directly between the Customer and you. You cannot present for processing any Transaction Data you know or should have known to be (i) fraudulent or (ii) not authorized by the Customer. You will be responsible for the actions of your employees while acting in your employ. The collection and payment of all federal, state and local taxes is your responsibility. Taxes collected must be included in the total transaction amount and not collected separately by another form of payment. You must submit one Transaction Data record for all goods and services sold in the same transaction. All available information about the sale, including any handling and shipping charges, must be accurately recorded. You must provide to the Customer a true and completed record of the Transaction.

**5 Chargebacks**

Chargebacks of Payment Transactions and Conveyed Transactions may occur under a variety of circumstances, as dictated by the Payment Brand Rules, which are subject to modification from time to time. Consequently, the following is only a partial list of circumstances that might give rise to Chargebacks: (i) a Customer account number is incorrect or otherwise invalid; (ii) an authorization/approval code was not received or other required authorization was not obtained; (iii) an authorization/approval code was obtained for the wrong amount or wrong date; (iv) the Customer never received the merchandise/service requested; (v) a Customer's refund/credit was processed as a sale; (vi) the Transaction Data is for the wrong amount; (vii) a Customer was never credited for returned merchandise or a canceled order; (viii) the Payment Instrument was expired, counterfeit, altered, or invalid at time of sale; (ix) a Payment Transaction or Conveyed Transaction was deposited more than once; (x) the Customer did not authorize or consent to the Transaction; (xi) the signature on the Transaction receipt does not match the signature on the Payment Instrument (if required); (xii) the Payment Instrument was not imprinted or its magnetic strip was not electronically recorded (for example, "swiping" or "tapping" a Payment Instrument) through a terminal; (xiii) the Customer asserts any disputes, claim, counterclaim, defense or offset against you; (xiv) the Transaction Data or any material information thereon is illegible, incomplete, inaccurate or unsigned, or is not delivered to us within the required time limits; (xv) the Transaction Data is fraudulent or does not represent a bona fide transaction in the ordinary course of your business, or is subject to any claim of illegality, negligence, dishonesty or offset; and (xvi) you have failed to provide copies of Transaction Data requested by us (retrieval request) within the prescribed time period.

**6 Disputing Chargebacks**

If you have reason to dispute or respond to a Chargeback, then you must do so by the date provided by us on our report to you. We are not required to investigate, reverse or make any adjustment to any Chargeback when thirty (30) calendar days have elapsed from the date of the Chargeback. All responses to Chargebacks must be in writing, and must contain the following information: (i) date of debit/credit advice; (ii) company case number; (iii) total amount of Chargeback; (iv) date and dollar amount for which the Transaction Data was originally submitted (v) if known, the date and authorization approval code; and (vi) any supporting documentation to substantiate your claim. You should include a dated cover letter detailing

reasons for requesting a review of the Chargeback. You should retain a copy of the correspondence and all documentation for your files. You should also retain proof that we received your response.

## **7 Data Security And Privacy**

You agree to post and maintain on all your Web sites both your consumer data privacy policy (which must comply with all Payment Brand Rules, regulations and guidelines) and your method of transaction security. You may not retain or store CVV2/CVC2 data or PIN data subsequent to the authorization. You must comply with all Security Standards published by the Payment Brands and the PCISSC including, but not limited to, Visa's Customer Information Security Program ("CISP"), MasterCard's Security Data Program (MSDP) and the Payment Card Industry Data Security Standard (PCIDSS). Pursuant to the Security Standards, you must, among other things: (i) install and maintain a working network firewall to protect data accessible via the Internet; (ii) keep security patches up-to-date; (iii) encrypt stored data and data sent over open networks; (iv) use and update anti-virus software; (v) restrict access to data by employees who are on a "need-to-know" basis; (vi) assign a unique ID to each person with computer access to data; (vii) not use vendor-supplied defaults for system passwords and other security parameters; (viii) track access to data by unique ID; (ix) regularly test security systems and processes; (x) maintain a policy that addresses information security for employees and contractors; (xi) restrict physical access to Customer information; (xii) when outsourcing administration of information assets, networks, or data you must retain legal control of proprietary information and use limited "need-to-know" access to such assets, networks or data; and (xiii) reference the protection of Customer information and compliance with the Security Standards in contracts with other service providers. You must notify Paymentech of any third party vendor with access to Customer information, and you are responsible for ensuring that all third party vendors are compliant with the Security Standards, to the extent applicable. The Security Standards may require that you engage an approved third party vendor to conduct quarterly perimeter scans and/or an on-site security review of your systems in order to be compliant. Visa and MasterCard's individual requirements for such scans or security reviews can be accessed through the Visa and MasterCard websites at [www.Visa.com](http://www.Visa.com) and [www.MasterCard.com](http://www.MasterCard.com). The Payment Brand rules provide that Customer information and Transaction Data is owned by the Payment Brand and the Customer. Paymentech also asserts some ownership rights in the Transaction Data to the extent it belongs to the Payment Brand system. You are responsible for securing Customer information. You will not use any Payment Instrument or Customer information other than for the sole purpose of completing the transaction authorized by the Customer for which the information was provided to you, or as specifically allowed by the Payment Brand Rules, or required by law. Paymentech or any Payment Brand may inspect Merchant's premises and computers, and the premises and computers of any company the Merchant has contracted with, for the purposes of verifying that Customer information is securely stored and processed, and is not used for any purpose other than processing the transactions to which it relates.

## **8 Certain Merchant Prohibitions**

You may not (i) accept Customer payments for previous Visa or Visa Electron charges; (ii) require a Customer to complete a postcard or similar device that includes the Customer's account number, Payment Instrument expiration date, signature, or any other account data in plain view when mailed; (iii) add any tax to a Transaction unless applicable law expressly requires that you be permitted to impose a tax; (iv) request or use a Payment Instrument account number for any purpose other than as payment for its goods or services, except to support Visa's Health Care Eligibility Service or Prepaid Load Network; (v) disburse funds in the form of travelers cheques, if the sole purpose is to allow the Customer to make a cash purchase of goods or services from you; (vi) accept Visa or Visa Electron for the purchase of scrip; or (vii) accept Visa Electron for a manual cash disbursement. You understand and acknowledge that all Visa BIN information provided by us to you is proprietary and confidential information belonging to Visa. You must not disclose Visa BIN Information to any third party without prior written permission from Visa. You understand and acknowledge that Visa may impose conditions on, or permanently prohibit you from participating in the Visa program for any reasons it deems appropriate, including, but not limited to (i) fraudulent activity; (ii) submitting Transaction Data that does not result from an act between you and the Customer (laundering); (iii) entering into this Agreement under a new name with the intent to circumvent provisions of the Rules; (iv) activity that causes us to repeatedly violate the Rules; any other activity that may result in undue economic hardship or damage to the goodwill of the Visa system.

## **Specialized Rules For Retail Transactions**

### **1 Presentation Of Payment Instruments**

You or your employee must examine each Payment Instrument presented to determine that the Payment Instrument presented is valid and has not expired. You must exercise reasonable diligence to determine that the authorized signature on any Payment Instrument presented corresponds to the Customer's signature on the Transaction Data. You must not honor expired, invalid, altered, counterfeit, or revoked Payment Instruments nor any Payment Instrument presented by any person other than the proper Customer as evidenced by the authorized signature on the Payment Instrument. A Customer may authorize another person to use his or her Payment Instrument for purchases, provided the user's signature appears on the back of the Payment Instrument. The signature on the back must match the one on the Transaction Data. If the Payment Instrument is not signed, in addition to requesting an authorization, you may review positive identification as allowed by local and state law, such as a passport or driver's license, to confirm that the user is the Customer, record the information and require the Customer to sign the signature panel of the Payment Instrument prior to completing the Transaction. You should not complete a Transaction if the Customer does not present his or her Payment Instrument or if you cannot obtain an electronic swipe record or physical imprint of the Payment Instrument (this includes mail, telephone and internet orders). By the submission of any Transaction Data to us, you will be deemed to warrant the identity of the purchaser as the authorized holder of the Payment Instrument, and if the Customer later denies making the purchase, you will not be able to rebut the Chargeback.

### **2 Completion Of Transactions**

You must use a suitable imprinter to legibly imprint Payment Instruments on Transaction Data or, capture the information from the Payment Instrument by electronic data capture. A photocopy of the Payment Instrument is not an acceptable substitute for an imprint. If the account number is manually keyed into the terminal, you must imprint the Payment Instrument. Your name, location, city and state must match the Merchant plate on the imprinter. You must notify us of any changes to the information on the Merchant plate. In addition to having the Customer sign the Transaction receipt, the Transaction date and dollar amounts and other information must be clearly written or printed on the Transaction receipt or captured by an electronic device. A brief description of the goods sold or service rendered must be provided on the Transaction receipt. Authorization/approval code numbers must be clearly recorded in the appropriate place on the Transaction receipt. Never circle or underline any information on the Transaction receipt. Every Transaction Receipt and credit voucher must be imprinted (or printed from electronic draft capture equipment) with the Customer's truncated account number and Merchant name. You will give the Customer a true and completed copy of the Transaction Receipt or appropriate facsimile. If the Customer's copy of the Transaction receipt or credit voucher is printed from electronic draft capture equipment/terminal, it must comply with all applicable Payment Brand Rules and laws. You cannot require Customers to provide any personal information as a condition for honoring Payment Instruments unless otherwise required by the Payment Brand Rules or law. Personal information includes, but is not limited to, a home or business telephone number, a home or business address, a social security number, or a photocopy of a driver's license. You cannot retain or store full magnetic-stripe data, CVV2, CVC2 codes or PIN data after the authorization of a Payment Transaction or Conveyed Transaction, except as required to complete the transmission of such Transaction Data to us.

### **3 Forgeries/Counterfeit Payment Instruments**

You should examine all notices received from us or from a Payment Brand to help you determine whether a Payment Instrument presented is counterfeit. You should attempt to retain the Payment Instrument while making an authorization request and then match any signature on the Payment Instrument with the one on the Transaction receipt. You should compare the account number on the Payment Instrument to the account number printed on the receipt or displayed on the terminal. You should examine each Payment Instrument to see if it looks genuine. You should use reasonable, peaceful efforts to recover any Payment Instrument if you have reasonable grounds to believe such Payment Instrument is counterfeit, fraudulent or stolen. You will be solely responsible for your actions in recovering/retaining Payment Instruments.

### **4 Travel And Entertainment Services**

At your option and as specified in the applicable sections of the Payment Brand Rules, Merchants may participate in one or more specialized travel & entertainment services offered by any of the Payment Brands. Merchants offering travel and entertainment services must institute and comply with the procedures set forth in the Payment Brand Rules.

## **Specialized Rules for Mail Order, Telephone Order, And Internet-Transactions**

### **1 Completion Of Sale**

You are responsible for determining that the purchaser is the person whose name appears as the Customer. If an account number is transposed into an invalid or inaccurate account number, the sale will result in a Chargeback. You must be authorized by us to accept Payment Instruments for mail, telephone, internet and pre-authorized orders, and you must have noted such on your application to us. All information that would normally be imprinted from a Payment Instrument must be clearly written in the appropriate areas on the order or Transaction receipt. "Mail Order" or "Phone Order" should be written on the signature line of the Transaction receipt.

### **2 Recurring Transactions**

For recurring transactions, you must obtain a written request from the Customer for the goods and services to be charged to the Customer's account, specifying the frequency of the recurring charge and the duration of time during which such charges may be made. You will not complete any recurring transaction after receiving: (i) a cancellation notice from the Customer (ii) notice from Paymentech or any Payment Brand that the Payment Instrument is not to be honored; or (iii) an authorization/approval code that the Payment Instrument is not to be honored. You must include in your Transaction Data the electronic indicator that the transaction is a recurring transaction.

## **Specialized Rules for Stored Value Transactions**

### **1 Payment Instruments & Packaging**

You may be obligated to purchase Stored Value Payment Transaction Payment Instruments ("Gift Cards") from us or pay us a data transfer fee in lieu thereof. Please check the pricing schedule of your Merchant Agreement to see if these requirements apply to you. If you are obligated to purchase Gift Cards from us or if you elect to do so, we will arrange for the Gift Card production and may, at our option, invoice you therefore, in lieu of electronically debiting your account. Any such invoice will be payable upon receipt. Gift Cards, Packaging and Point-of-purchase marketing materials are available and priced on a per bundle basis, based on current rates. All production and delivery timeframes and costs provided by us are estimates only and we do not guarantee any specific date of delivery or price for Gift Cards produced by third parties. You are responsible for all production costs and delivery charges for Gift Cards. The form and content of all Gift Cards will be subject to our approval.

### **2 Compliance and Warranties**

You are solely responsible for complying with all applicable laws relating to your Gift Card program and you agree to indemnify and hold us harmless from any loss, damage or claim relating to or arising out of any failure to comply with applicable laws in connection therewith. You are solely responsible for monitoring the legal developments applicable to the operation of your Gift Card program and ensuring that your Gift Card program complies fully with such requirements as in effect from time to time. Merchant acknowledges that Paymentech cannot reasonably be expected to monitor and interpret the laws applicable to its merchants, and has no responsibility to monitor or interpret laws applicable to Merchant's business.

### **3 Fraud**

You hereby agree (i) that you are responsible for ensuring that all Gift Cards require activation at the point of sale; (ii) to provide notification in writing to Paymentech of any fraud losses by type by fifteen days following the end of each calendar quarter; (iii) that you will be solely responsible for any and all value adding and fraud losses and expenses relating to or arising from your Gift Card; (iv) to discourage transportation of groups of sequentially numbered Gift Cards; and (v) to deactivate or otherwise remove all value from Gift Cards that have been compromised. You will be responsible for any fraudulent transactions involving your Gift Cards, including, without limitation, the unauthorized activation of Gift Cards, reloading of existing Gift Cards (whether pursuant to a manual telephone order or otherwise) with additional value, or the unauthorized replication of Gift Cards or Gift Card data for fraudulent transactions. Paymentech provides a number of tools and options to help Merchant reduce Merchant's risk of exposure for fraudulent transactions. We urge you to make use of any and all of such tools as we may offer in order to help reduce the risk of such transactions. In particular, we recommend that you utilize only those vendors that have been certified by Paymentech as having appropriate security measures in place to reduce the risk of counterfeit Gift Cards and the loss of sensitive Gift Card information that might result in unauthorized transactions, and we recommend that you promptly and frequently reconcile the transaction reports we provide to you against your own internal transaction records, and to report any unauthorized transactions to your account representative at Paymentech. Because manual Gift Card transactions (i.e. those involving the activation or reloading of Payment Instruments over the telephone in cases where your terminals may be unavailable) pose a higher risk of potential fraud, we urge you to pay special attention to these transactions and reconcile them on an even more frequent basis. In the event that you do not reconcile your transaction reports and promptly report any suspicious activity to us, Paymentech may not be able to assist you in canceling fraudulently activated or reloaded Gift Cards, or in otherwise identifying the source of any fraud.