CHASE Paymentech™

MERCHANT OPERATING GUIDE

TO THE EXTENT THAT THIS OPERATING GUIDE IS INCONSISTENT WITH THE PAYMENT BRAND RULES, THE PAYMENT BRAND RULES SHALL PREVAIL.

GENERAL RULES APPLICABLE TO ALL TRANSACTIONS

1. PRESENTATION OF PAYMENT INSTRUMENTS

1.1 You or your employee must examine each Payment Instrument presented to determine that the Payment Instrument presented is valid and has not expired by the terms on its face. 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, when applicable. You must not honour 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. PAYMENTECH IN ITS SOLE DISCRETION MAY DECLINE AT ANY TIME OR FROM TIME TO TIME TO PROCESS ANY TRANSACTION DATA THAT DOES NOT INCLUDE THE ACTUAL SIGNATURE OF A CUSTOMER, EVEN IF THE CUSTOMER'S CONSENT OR INSTRUCTIONS HAVE BEEN OBTAINED BY TELEPHONE OR BY MAIL.

1.2 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 provincial law, such as a passport or driver's license, to confirm that the user is the Customer, require the Customer to sign the signature panel of the Payment Instrument prior to completing the Payment Transaction.

1.3 In order to protect yourself, you must never complete a Payment Transaction if the Customer does not present his or her Payment Instrument or if you cannot obtain an electronic record or physical imprint of the Payment Instrument (this includes mail, telephone and internet orders). If you elect to do so, 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 remedy the Chargeback.

2. PROCESSING OF PAYMENT INSTRUMENTS

General Authorization Rules

AUTHORIZATION/APPROVAL CODES

2.1 All Payment Transactions and Conveyed Transactions require an authorization/approval code.

2.2 An authorization/approval code indicates the availability of credit for the Payment Transaction or Conveyed Transaction at the time of inquiry. It is not a promise or a guarantee that you will receive payment for the related Payment Transaction or Conveyed Transaction. It does not warrant that the person presenting the Payment Instrument is the rightful Customer.

A Merchant must:

- Request authorization prior to completing a Transaction;
- Not split a sale;
- Ensure the authorization code appears on the Transaction Data record;
- Obtain authorization on the Transaction date, excluding special conditions such as hotel, car rental company, cruise line, delayed delivery.
- Request authorization, regardless of the Transaction amount;
- For an aggregated Transaction an electronic commerce Merchant, obtain authorization for the full, final aggregated Transaction amount; and
- Request authorization for a mail/telephone order Transaction; e-commerce Transaction.

3. TRANSACTION DATA RECORD REQUIREMENTS

3.1 You must use a suitable imprinter to legibly imprint Payment Instruments on a Transaction Data record or, capture the information from the Payment Instrument by electronic data capture.

•NOTE: A photocopy of the Payment Instrument is not an acceptable substitute for an imprint.

3.2 If the account number is manually keyed into the terminal, you must imprint the Payment Instrument and include the information set out below in this section on the Transaction Data record.

3.3 Your name, location, city and province must match the Merchant plate on the imprinter.

3.4 You must notify us of any changes to the information on the Merchant plate. You must use one Transaction Data record for all goods and services sold in the same Payment Transaction.

3.5 With respect to Payment Transactions, all Transaction Data must be imprinted (or printed from electronic draft capture equipment) with the Customer's account number and Merchant name. For mail, telephone, and pre-authorized orders, all information that would normally be imprinted from a Payment Instrument must be clearly written in the appropriate areas on the order or Transaction Data record. "Mail Order" or "Phone Order" should be written on the signature line of the Transaction Data record.

3.6 If a Customer presents an unenbossed card, you must record the Payment Instrument information electronically.

3.7 Authorization/approval code numbers shall be clearly recorded in the appropriate place on the Transaction Data record. Never circle or underline any information on the Transaction Data record.

3.8 You will require the Customer to sign the Transaction Data record in your presence. You will give the Customer a true and completed copy of the Transaction Data record or appropriate facsimile.

3.9 You shall not require Customers to provide any Personal Information as a condition for honouring Payment Instruments unless otherwise required by the Payment Brand Rules or applicable law. Personal information includes but is not limited to a home or business telephone number, a home or business address, a social insurance number, or a photocopy of a driver's license.

3.10 You shall not retain or store magnetic-stripe data after the authorization of a Transaction, except as required to complete the transmission of such Transaction Data to us.

3.11 You must not reflect the Personal Identification Number (PIN), or any part of the PIN, or any fill characters representing the PIN; and/or the card validation code 2 (CVC 2, CVV2), which is indent-printed on the signature panel of the card.

3.12 Customer receipts generated electronically (attended or unattended) must include only the last four digits of the Customer's account number, replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as "x", "*", or "#", and must exclude the card expiration date.

3.13 The Merchant copy of the Transaction Data record must exclude the card expiration date. It is strongly recommended that the Merchant copy of Transaction Data record reflect only the last four digits of the Customer's account number.

4. PROCESSING OF PAYMENT TRANSACTIONS

4.1 You must submit Transaction Data (including credit vouchers) to us on or before the next business day after the date of the Payment Transaction. Late submission of Transaction Data may result in higher Payment Brand fees and/or a Chargeback to you.

4.2 You must not submit Transaction Data for payment until the goods are delivered, shipped, or the services are performed (except as otherwise provided in the Agreement, and only if you have notified us that you are doing so on your application or otherwise in advance). 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 Transaction Data has been submitted.

4.3 You shall not present for processing any Payment Transaction that was not originated as a result of an act directly between the Customer and you. You shall not present for processing any Transaction you know or should have known to be (i) fraudulent or (ii) not authorized by the Customer. You shall be responsible for the actions of your employees, agents, and representatives while acting in your employ.

4.4 The collection and payment of all federal, provincial, and local taxes is your responsibility. Taxes collected shall be included in the total Transaction amount and not collected separately as cash.

4.5 If you process recurring Payment Transactions, you shall obtain Customer written permission to periodically charge for recurring services and retain a copy of this permission for the duration of the recurring services. You shall include the words "Recurring Transaction" on the Transaction Data. You will not complete any recurring Payment Transaction after receiving: (i) a cancellation notice from the Customer (ii) notice from Paymentech or a Payment Brand; or (iii) an authorization/approval code that the Payment Instrument is not to be honoured.

5. MAGNETIC STRIPE PAYMENT INSTRUMENTS

5.1 You must swipe the Payment Instrument into Equipment that electronically reads the magnetic stripe; enter the amount and wait for an approval code.

5.2 If it is declined, advise the Customer and request another form of payment.

5.3 If the magnetic stripe is not functioning when swiped, ensure the swipe reader is clean. Attempt once again to swipe the Payment Instrument. Try to avoid manually key entering the Payment Instrument as this carries more risk.

6. CHIP PAYMENT INSTRUMENTS

6.1 As of the date specified by any Payment Brand, you are required to use Equipment which electronically reads Chip Payment Instruments, and is compliant with all Payment Brand Rules. If you do not implement such Equipment, your Payment Transactions will be subject to Chargebacks as set forth in the Agreement and this Operating Guide.

6.2 If a Chip Payment Instrument is presented by a Customer, you will process the Customer's Payment Transaction as a Chip initiated Payment Transaction, as the only method of initiating and processing the Payment Transaction.

6.3 You shall direct the Customer to insert the Chip Payment Instrument into Chip-reading Equipment instead of being swiped by the Merchant, and to leave the Chip Payment Instrument in the Equipment throughout the transaction. The Customer will enter his/her PIN on a keypad in or connected to the Equipment.

6.4 Certain Chip Payment Instruments will be set up to require a signature. The Equipment will determine whether the Chip Payment Instrument requires PIN or signature and you are required to follow the prompts displayed on the Equipment.

6.5 If a Chip initiated Payment Transaction is declined, the Payment Transaction should not be processed by any other means. The Merchant should advise the Customer to utilize an alternative Payment Instrument for the Payment Transaction.

6.6 For a recovered Chip Payment Instrument, the Merchant must cut away the corner of the Chip Payment Instrument at the opposite end of the chip. A corner must be cut at a 45 degree angle and extend approximately 25 mm from the corner of the Chip Payment Instrument. You shall immediately deliver such recovered Chip Payment Instrument to us.

7. KEY ENTERED TRANSACTIONS

7.1 NOTE: The magnetic stripe or Chip card contains security authentication data that helps to identify the cardholder when swiping or inserting the card into electronically read Equipment. When a manually key entered transaction occurs those security features are no longer available and as a result may carry a higher risk of counterfeit fraud.

For tips on identifying counterfeit cards visit the following websites below, which may be revised from time to time:

- www.chasepaymentech.ca
- www.visa.ca
- www.mastercard.ca

7.2 You must ensure, the date, imprint of the card, details of the transaction, total dollar value of transaction, including taxes and other charges, cardholder signature, authorization number, and your Merchant number are all present.

8. GENERAL REFUND/CREDIT RULES

8.1 You may limit your acceptance of returned merchandise or establish a policy to make price adjustments for any Transactions provided that proper disclosure is made and purchased goods or services are delivered to the Customer at the time the Transaction takes place. Proper disclosure by you shall be determined to have been given at the time of the original purchase Transaction if the following words or similar wording reflecting your policy is legibly printed on all copies of the Transaction Data, in letters approximately .25 inch high and in close proximity to the space provided for the Customer's signature: "NO REFUND," or "EXCHANGE ONLY," or "IN-STORE CREDIT ONLY."

8.2 The Merchant must not provide refund or adjustment by any other means other than by a credit to the card account used to purchase the merchandise or service unless required by applicable law.

8.3 The Customer must be provided a copy of the credit receipt.

8.4 For retail Payment Transactions, the credit receipt must be dated and signed by the Merchant and the appropriate copy provided to the Customer.

8.5 You shall not process a credit without having completed a previous purchase Payment Transaction with the same Customer.

8.6 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 new Transaction Data for any new merchandise purchased.

9. GENERAL DOWNTIME PROCEDURES

9.1 In the event your electronic service is unavailable for any reason or if the information encoded on a Payment Instrument cannot be read by an electronic card reader, you shall manually process the Transaction in accordance with these procedures and all Payment Brand Rules (including, without limitation, imprinting a manual Transaction Data record and obtaining the Customer's signature and all information set out with respect to manual Transaction Data records in section 7. Once your electronic service is available, you shall electronically process the Transaction and attach your manually generated Transaction Data record to the electronically generated Transaction Data record and retain copies of these materials.

10. CHARGEBACKS

10.1 After a Transaction has been settled and funded to you, there may be instances where the cardholder or the issuing bank may determine that, for a given reason specified, a transaction may be invalid. The issuer may then return the transaction as a Chargeback for possible remedy. These reasons are outlined in the Payment Brand Dispute Resolution and/or Chargeback guides. For a listing of Chargeback Reason Codes, please refer to the following websites, which may be revised from time to time:

- www.visa.ca
- www.mastercard.ca

For best practices and tips regarding Chargebacks please visit the Paymentech website at www.chasepaymentech.ca.

11. DISPUTING CHARGEBACKS

11.1 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:

- Date of debit/credit advice;
- Company case number;
- Total amount of Chargeback;
- Date and dollar amount in which the sale/credit was originally submitted;
- If known, the date and authorization/approval code;
- Merchant number;
- If a 3-D Secure transaction (Verified by Visa/SecureCode), specific transaction values, and
- Any supporting documentation to substantiate claim. You should include a dated cover letter detailing reasons for requesting a review of the Chargeback.

11.2 You should retain a copy of the correspondence and all documentation for your files.

11.3 You should also retain proof that we received your response.

Retrieval Request Or Request For Copy

11.4 The three most common reasons for a cardholder's issuing bank to initiate a Retrieval Request or request for Transaction record copy are to:

- Satisfy a cardholder inquiry;
- Substantiate a chargeback; and/or
- Support a legal or fraud investigation.

11.5 You have an obligation to provide a legible Transaction record copy or substitute if requested by us.

11.6 You must provide the Transaction record within the applicable time frames even though there may not be a Chargeback right.

OTHER SERVICES

12. QUICK SERVICE PROGRAMS

12.1 A Merchant may qualify for the Quick Service Programs (QSP) offered by the Payment Brands. Quick Service Program Transactions occur in a face-to-face environment in which Payment Instrument Data is read electronically from the Payment Instrument.

12.2 You agree to follow the Payment Brand Rules related to the Quick Service Programs offered, including, but not limited to the following:

• Authorization is mandatory for all electronically card-read Transactions equal to or less than the applicable Chargeback protection amount which varies for each Payment Brand.

• You may choose not to obtain the cardholder's signature for properly identified QSP Transactions equal to or less than the applicable Chargeback protection amount. The personal identification number (PIN) requirements remain unchanged

• Providing a receipt to the Customer is optional for properly identified QSP Transactions equal to or less than the applicable Chargeback protection amount. However, all merchants must be able to provide a receipt upon the cardholder's request.

For further qualification criteria, please visit the following websites below, which may be revised from time to time:

• www.mastercard.ca
• www.visa.ca

13. CONTACTLESS/PROXIMITY PAYMENTS

13.1 Contactless functionality can be used at any Merchant location that has a contactless/proximity device installed at the point of sale.

13.2 You must have a contactless/proximity payment device in order to process a contactless/proximity Transaction.

13.3 To process a contactless/proximity transaction, you will: enter transaction amount; the Customer will "tap" a contactless Payment Instrument once; and, you will continue to follow the prompts.

13.4 Transaction receipts do not have to be issued to the Customer for a contactless/proximity Transaction except if requested by the Customer. A Transaction receipt must be provided if a Customer so requests, but a PIN or a signature, is not required.

14. DYNAMIC CURRENCY CONVERSION SERVICES

14.1 If you offer and provide Dynamic Currency Conversion or any other currency conversion services to Visa Customers, you must:

• Notify Paymentech and your bank prior to offering Dynamic Currency Conversion to Visa Customers;

• Inform Visa Customers that Dynamic Currency conversion is optional;

• Not impose any additional requirements on the Customer to have the Transaction processed in the local currency;

• Not use any language or procedures that cause the Customer to choose Dynamic Currency Conversion by default;

• Not misrepresent, either explicitly or implicitly, that the Dynamic Currency Conversion service offered by you is a Visa service;

• Comply with all of the Transaction receipt requirements required by your financial institution from time to time;

• Comply with any other requirements regarding Dynamic Currency Conversion that your financial institution may notify you of from time to time.

PROCESSING DEBIT PAYMENT INSTRUMENTS

15. INTERAC-DIRECT PAYMENT

15.1 You may accept valid and unexpired debit payment cards issued by any institution participating in the Interac Direct Payment program. You shall never request, or obtain, the Customer's personal identification number (PIN) from the Customer. You shall situate the PIN keypad in a way that minimizes the risk of disclosure when the PIN is entered into the point-of-sale device. You shall not permanently fix or attach a PIN keypad to a counter or other object.

15.2 If a Interac Direct Payment card is left at your premises, you agree to promptly return it to the Customer, subject to satisfactory identification of the Customer, or, if you are unable to return it or if the Interac Direct Payment card is not claimed within twenty-four (24) hours, you shall deliver it to us at your first available opportunity.

15.3 The use of a Interac Direct Payment card creates an on-line direct debit to the Customer's account at his/her card issuing institution and a return or void creates a credit to the Customer's account with that card issuing institution.

15.4 You shall not manually key direct payment card information into a point-of-sale terminal in order to complete a transaction. You shall give the Customer a Transaction receipt regardless of whether a Payment Transaction is approved, declined or not completed.

15.5 If your printer is not operational and your Equipment has processed the Payment Transaction, you shall (i) provide an alternate Transaction Data receipt (such as a completed and dated sales slip or manually created facsimile showing the account number on the card to indicate that payment was made with that card or (ii) reverse the Payment Transaction on the day of the request or the next business day if the Customer requests that you do so.

15.6 You shall maintain accurate logs of employee shifts and provide these logs to us, within twenty-four (24) hours of our request, in order that any debit payment card fraud skimming incident can be investigated.

15.7 You shall otherwise comply with all requirements of Interac Direct Payment ("Interac") applicable as specified in the Interac rules. You acknowledge that the Interac rules are confidential information of Interac and you shall maintain such confidential information in confidence and shall not disclose such confidential information to any person without the prior written consent of Interac. You will take care to protect such confidential information using a degree of care at least equal to that used to protect your own confidential information and will not use the confidential information for your own benefit or the benefit of any third person without the consent of Interac. For further information, please visit the following websites, which may be revised from time to time:

• www.chasepaymentech.ca
• www.interac.ca

SPECIALIZED RULES FOR MAIL ORDER, TELEPHONE ORDER, AND INTERNET TRANSACTIONS

16. GENERAL RESPONSIBILITIES

16.1 You agree that the services provided by us pursuant to this Agreement may contain third party services and online links for which you acknowledge that we have no responsibility nor liability whatsoever and you shall not seek any remedy or relief from us. Any use by you of any third party product, service or website is subject to your agreement with the third party's policies and agreements.

16.2 In addition to your obligations set out in the Agreement or the Operating Guide, you agree to comply with all applicable codes, guidelines, principles or laws related to consumer protection for electronic commerce activities which may be issued by any authority.

16.3 You shall not use, or allow a third party to use, the products, services or software provided to you under this Agreement to sell, receive, display or link to: (i) any activity associated with a game of chance or mixed

chance or skill or any other form of gambling (including virtual casinos, funding an account, as well as the purchase of value for proprietary payment mechanisms (including electronic gaming chips); (ii) any communications or material which depicts or describes any obscene materials, pornography or other sexual communication; (iii) any software or other material that contains viruses, corrupted files or is intended to damage the operation of any software application or personal computer; (iv) any unsolicited or unauthorized advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes" or any other form of solicitation; (v) any direct or indirect criminal or quasi-criminal activities or any violation of any applicable laws or government regulations; (vi) any material in any form whatsoever that violates any applicable intellectual property rights; or (vii) any collection of Personal Information about third parties without the consent of such third parties.

16.4 Website Requirements

You will display, at a minimum, all of the following information on your website in connection with any and all of your Internet Transactions:

• your business trade name and its corresponding website;

• proof of your website(s) registration, ownership or lease;

• a complete description of the goods or services available through your website(s);

• your return/refund policies;

• all customer service contact information; including mailing address, electronic mail address and telephone numbers;

• your Internet Transaction currency, whether Canadian or US Dollars, or otherwise;

• all taxes, tariffs and restrictions applicable to your Internet Transactions;

• your delivery policy; for example, if restricted to Canada or another country or any division or area within a country, etc.;

• the country in which you are officially registered and located;

• an appropriate Payment Brand mark unless prohibited by your trade association;

• your consumer data privacy policy;

• your security capabilities and policy for transmission of Payment Instrument details;

• export restrictions (if known).

17. COMPLETION OF PAYMENT TRANSACTION

17.1 If you are authorized by us to accept Payment Instruments for mail, telephone and pre-authorized orders, all available information about the Payment Transaction, including handling and shipping charges, must be accurately recorded.

17.2 For goods to be shipped, a mail/telephone order or an electronic commerce Merchant may obtain authorization on any day up to seven (7) calendar days prior to the Transaction Date. The Transaction Date is the date the merchandise is shipped. The Authorization is valid if the Transaction amount is within 15% of the authorized amount, provided that the additional amount represents shipping costs.

17.3 You will provide to the Customer a true and completed record of the Payment Transaction.

17.4 Any Transaction Data record shall include the following information:

• the date that you obtained the Transaction Data;

• your merchant number applicable to the Payment Transaction;

• your business trade name and web site address;

• the Payment Instrument type used;

• the amount and type (purchase or credit) of the Payment Transaction;

• the currency in which the Payment Transaction was processed;

• the authorization number;

• the unique transaction order number assigned to you;

• a detailed description of the goods and services purchased;

• the contact name, mailing address, electronic mail address; telephone and fax number of the person responsible for handling customer disputes;

• any applicable taxation or export information;

• the name of the purchaser; and

• your return/refund policy.

• Except for the last four digits, the account number and expiry date must be suppressed from the Transaction Data record.

18. RECURRING PAYMENT TRANSACTIONS

18.1 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 must include in your Transaction Data the electronic indicator that the Transaction is a recurring transaction.

19. REFUNDS AND EXCHANGES (CREDITS) - CARD-NOT-PRESENT TRANSACTIONS ONLY.

19.1 You may limit your acceptance of returned merchandise or establish a policy to make price adjustments for any Transactions. If your refund policy prohibits returns under certain circumstances, you may still receive a Chargeback relating to such Payment Transactions pursuant to the Payment Brand Rules.

20. INTERAC ONLINE

20.1 Merchant Responsibilities. You will comply with all applicable federal and provincial laws relating to all activities you carry out pertaining to Interac Online. You are responsible for ensuring that all Merchant information relating to your registration with the Acxsys Payment Brand ("Acxsys") is correct, complete and current.

20.2 Compliance; Fraud. You agree that (i) we may share with Acxsys, and Acxsys may use, any information, including Personal Information we have collected from you, and (ii) we have the right to share with other participants in the Interac Online system and Acxsys, information pertaining to any termination, suspension or other action taken against you for reasons of non-compliance with the Acxsys bylaws, rules, and regulations ("Acxsys Rules") or applicable law. You agree that you will, upon and in accordance with our request, assist us, our business partners and Acxsys with the investigation of a fraud.

20.3 Authorization. You are required to display the issuer confirmation number generated by the issuer on the confirmation screen to the Customer ("Issuer Confirmation Number"). You acknowledge that the Issuer Confirmation Number does not constitute a representation from us, the issuer or Acxsys that a particular Payment Transaction is in fact a valid or undisputed transaction, and that all Payment Transactions are subject to the Acxsys Rules.

20.4 Merchant Web site. You are required to include the following on your website:

• Timeout Message: Where you allow less than thirty (30 minutes for a Customer to complete a Payment Transaction through the issuer's website, you shall disclose to the Customer the amount of time allotted to complete the Payment Transaction.

• Trade-mark: You shall display the Interac Online trade-mark to indicate acceptance of Interac Online in accordance with the Acxsys Rules. You acknowledge that you can view the Acxsys Rules pertaining to display of the trade-mark at the Paymentech internet website (www.chasepaymentech.ca).

• Currency: You shall disclose to the Customer the amount that will be debited from the Customer's account in Canadian funds.

• A Customer must not be able to initiate a payment using Interac Online without having been given the opportunity to follow this link and view this page.

• In addition, you are required to comply with the Canadian Code of Practice for Consumer Protection in Electronic Commerce, published by Industry Canada on January 16, 2004, or such other e-commerce code of practice prescribed by Acxsys from time to time.

20.5 Payment Instrument Acceptance. You will honour a Customer's request to pay by Interac Online. You are not allowed to require a Customer to pay a surcharge for the use of Interac Online where the result would be that the Customer would pay more using Interac Online than if a Customer used other online payment options.

20.6 Confidentiality; Privacy; Security.

(i) You acknowledge that the Interac Online Payment Brand Rules are confidential information of Acxsys and you shall maintain such confidential information in confidence and shall not disclose such confidential information to any person, other than to your agents and contractors for the purpose of assisting you in completing a Payment Transaction, or Acxsys, without the prior written consent of Acxsys. You shall use such confidential information only for the purpose of fulfilling your rights and obligations in connection with Interac Online and under the Payment Brand Rules. You will, and will cause your agents and

contractors to, take care to protect such confidential information using a degree of care at least equal to that used to protect your own confidential information, and will not, except as may be required by law, use the confidential information for your own benefit or for the benefit of any third party without the prior written consent of Acxsys.

(ii) You are required to have appropriate processes and procedures in place to protect all information relating to a Customer, including the Customers name, address, email address, telephone number, login ID, password or any other personal or demographic information relating to such Customer and such Customer's use of Interac Online ("Cardholder Information"), in accordance with all applicable federal and provincial privacy legislation. You are responsible for obtaining the appropriate consent, sufficient to meet all obligations under all applicable laws, from Customers to share Payment Instrument Information through the network for the purpose of Interac Online.

21. TRAVEL AND ENTERTAINMENT SERVICES

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

21.2 A Merchant must participate in the Hotel Reservation Services if it accepts Visa cards to guarantee hotel reservations as described in the Visa rules.

22. DATA SECURITY AND PRIVACY

22.1 You agree to post and maintain on all your websites both your consumer data privacy policy (which must comply with all Payment Brand Rules and guidelines) and your method of Transaction security.

22.2 You may not retain or store sensitive CVV2/CVC2 data, PIN data, and any magnetic stripe data subsequent to the authorization.

22.3. You must comply with the PCI Data Security Standards as set out by the PCI Security Standards Council. You must comply with, the Visa Canada Account Information Security Program ("AIS") and MasterCard's Security Data Program (SDP) monitoring programs. Pursuant to these programs, you must, among other things:

- restrict access to data by business "need-to-know";
- assign a unique ID to each person with computer access to data;
- not use vendor-supplied defaults for system passwords and other security parameters;
- track access to data by unique ID;
- regularly test security systems and processes;
- install and maintain a working network firewall to protect data accessible via the Internet;
- keep security patches up-to-date;
- encrypt stored data and data sent over open networks
- use and update anti-virus software;
- maintain a policy that addresses information security for employees and contractors; and
- restrict physical access to Payment Instrument Information.
- 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.
- Reference the protection of Payment Instrument Information and compliance with the Visa AIS and MasterCard SDP Rules in contracts with other Service Providers.

22.4 You must notify Paymentech of any third party vendor with Payment Instrument Information. You are responsible for the AIS and SDP compliance of that third party. AIS and SDP 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.

22.5 The Visa and MasterCard rules provide that Payment Instrument Information and Transaction Data is owned by the Payment Brands, and the Customer. Paymentech also asserts some ownership rights in the data to the extent it belongs to the MasterCard or Visa system.

22.6 You are responsible for securing Payment Instrument Information. You will not use any Payment Instrument or Payment Instrument 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 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 Payment Instrument Information is securely stored and processed and is not used for any purpose other than processing the Transaction to which it relates. Details about PCI, AIS or SDP can be found at the following website which may be revised from time to time:

- www.pcisecuritystandards.org/
- www.mastercard.com/sdp
- www.visa.ca/ais

FRAUD PREVENTION AND SECURITY

23. Protecting Your Business Against Card Present Fraud

23.1 You should examine all notices received from us or from Visa or MasterCard or other Payment Brands to help you determine whether a Payment Instrument presented is counterfeit.

23.2 You should attempt to retain the Payment Instrument while making an authorization request and when applicable, then match the signature on the Payment Instrument with the one on the Transaction Data record.

25.3 You should compare the embossed account number on the Payment Instrument to the account number printed on the receipt or displayed on the Equipment.

23.4 You should examine each Payment Instrument to see if it looks genuine.

23.5 You should use reasonable, peaceful efforts to recover any Payment Instrument if (i) the printed four digits above the embossed account number do not match the account number, if applicable, (ii) you are advised by us or authorization centre to retain it, or (iii) you have reasonable grounds to believe such Payment Instrument is counterfeit, fraudulent or stolen.

23.6 If you are suspicious of the Transaction for any reason at all, you should contact the voice authorization center, state to the authorization clerk "This is Code Ten" and await instructions.

23.7 You shall be solely responsible for your actions in recovering/retaining Payment Instruments.

24. Protect Your Business Against Card Not Present Fraud

24.1 Leverage Payment Brand tools in a "Layered Approach". Although optional, it is strongly recommended that as a Card Not Present merchant, you protect your business against Card Not Present Fraud with the following tools:

- **Card Verification Value (CVV2/CVC2)**. A 3 digit code found on the back of a Payment Instrument primarily used for telephone and e-commerce Transactions.
- **Address Verification System (AVS)**.This service verifies a cardholder's card billing address information and provides a response code to the Merchant that is separate from the authorization response code. A Merchant can then use this response code along with other risk mitigation intelligence to make an informed "risk assessment" decision as to whether to continue with the card absent transaction.
- **MasterCard Securecode & Verified by Visa**. A MasterCard and/or Visa-approved authentication method based on 3–D Secure.

24.2 Where applicable, perform negative file check, including listing prior "friendly" fraud attempts.

24.3 Implement customized Transaction risk filters, and process high risk Transactions through additional risk mitigation steps.

24.4 Prioritize Transactions that have been flagged for offline/manual review.

24.5 Provide clear customer return/cancellation/refund policies.

24.6 By implementing one or all of the above mentioned tools, you assist in lowering the risk of Card Not Present fraud and you assist in lowering your risk of receiving fraud Chargebacks.

25. Specialized Rules for STORED VALUE AND LOYALTY TRANSACTIONS

25.1 **Services**. The Merchant's Customers are given a magnetic stripe card by the Merchant in exchange for money received, merchandise returned or other consideration. The Stored Value (SV) Payment Instrument represents a dollar value that the Merchant's Customer can either use or give to another individual. There is no security associated with the SV Payment Instrument itself. The actual record of the balance on the SV Payment Instrument is maintained on Paymentech's Stored Value card database. The SV Payment Instrument, the design and use of which is proprietary to the Merchant, is designed to be swiped or manually entered through a POS terminal during each Stored Value Transaction at Merchant's location. When the Customer gives the SV Payment Instrument to the cashier, the cashier will press the appropriate keys dependent upon the Stored Value Transaction type, swipe the SV Payment Instrument into the terminal, and key in the amount to be applied against the SV Payment Instrument's balance. This information will be transmitted to Paymentech, and the appropriate approval response will be routed to the Merchant. Associated with the program is a standard online reporting package detailing the Merchant's Stored Value Transactions and the outstanding balances on the individual SV Payment Instruments. The Merchant will have access to help desk support through Paymentech for their Stored Value Transactions. Customers will have access to an interactive voice response system ("IVR"), via a toll free number, through which they may receive some basic account information. Merchant's SV Program will be configured in the manner specified by Merchant to Paymentech during enrollment, which will represent binding program rules relating to Merchant's SV Program. Changes to such SV Program requested by Merchant subsequent to setup will be made at Paymentech's sole discretion and in the time and manner which Paymentech shall determine. We will supply a detailed statement reflecting your SV Program activity. We will not be responsible for any error that you do not bring to our attention within ninety (90) days from date of such statement.

25.2 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 SV Payment Instruments and the loss of sensitive SV Payment Instrument Information that might result in unauthorized transactions and, 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 Stored Value Transactions (i.e. those involving the activation or reloading of SV 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 Stored Value 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 SV Payment Instruments, or in otherwise identifying the source of any fraud.

26. DEFINITIONS

26.1 For the purposes of this Operating Guide, the following definitions shall have the meaning described below:

"Chargeback" is a reversal of a Transaction you previously presented to Paymentech pursuant to Payment Brand Rules.

"Conveyed Transaction" is any Transaction conveyed to a Payment Brand for settlement by such Payment Brand directly to Merchant. .

"Customer" is the person or entity to whom a Payment Instrument is issued or who is otherwise entitled to use a Payment Instrument.

"Equipment" is a point-of-sale terminal or other software, hardware or other Payment Instrument processing equipment used by you to obtain Payment Instrument information and transmit Transaction Data to us.

"Payment Brand" is any payment method provider whose payment method is accepted by Paymentech for processing, including, but not limited to, MasterCard International Inc., Visa International, Inc., Visa Canada, Interac, Acxsys Corporation, other credit and debit card providers, debit network providers, Chase Paymentech Gift Card and other stored value, loyalty program providers and Payment Card Industry Security Standards Council.

"Payment Brand Rules" are the bylaws, rules, and regulations, as they exist from time to time, of the Payment Brands.

"Payment Instrument" is an account, or evidence of an account authorized and established between a Customer and a Payment Brand, or representatives or members of a Payment Brand that you accept from Customers as payment. Payment Instruments include, but are not limited to, credit cards, debit cards, stored value cards, loyalty cards, electronic gift cards, authorized account or access numbers, paper certificates, credit accounts and the like.

"Payment Instrument Information" is information related to a Customer or the Customer's Payment Instrument, that is obtained by Merchant from the Customer's Payment Instrument, or from the Customer in connection with his or her use of a Payment Instrument (for example a security code, a PIN number, or the Customer's postal code when provided as part of an address verification system). Without limiting the foregoing, such information may include a the Payment Instrument account number and expiration date, the Customer's name or date of birth, PIN data, security code data (such as CVV2 and CVC2) and any data read, scanned, imprinted, or otherwise obtained from the Payment Instrument, whether printed thereon, or magnetically, electronically or otherwise stored thereon.

"Payment Transaction" is a Transaction other than a Stored Value Transaction or a Conveyed Transaction.

"Personal Information" is information which relates to an individual and allows that individual to be identified.

"Retrieval Request" is a request for information by a Customer or Payment Brand relating to a claim or complaint concerning a Transaction.

"Security Standards" are all rules, regulations, standards or guidelines adopted or required by the Payment Brands or the Payment Card Industry Security Standards Council relating to privacy, data security and the safeguarding, disclosure and handling of Payment Instrument Information, including but not limited to the Payment Card Industry Data Security Standards ("PCI DSS"), Visa's Cardholder Information Security Program ("CISP"), Discover's Information Security & Compliance Program, American Express's Data Security Operating Policy, MasterCard's Site Data Protection Program ("SDP"), Visa's Payment Application Best Practices ("PABP"), the Payment Card Industry's Payment Application Data Security Standard ("PA DSS"), MasterCard's POS Terminal Security program and the Payment Card Industry PIN Entry Device Standard, in each case as they may be amended from time to time.

"Stored Value Transaction" is a Transaction utilizing a Payment Instrument issued by or on behalf of a Merchant in respect of which a Customer receives value from the Merchant in exchange for consideration from the Customer.

"Transaction" is a transaction conducted between a Customer and Merchant utilizing a Payment Instrument in respect of which consideration is exchanged between the Customer and Merchant.

"Transaction Data" is the written or electronic evidence of a Transaction.

WIRELESS SERVICES

THIS SECTION APPLIES TO MERCHANTS THAT ARE SUPPLIED WIRELESS EQUIPMENT THROUGH PAYMENTECH.

1) Wireless Services:

Merchant will subscribe to, and Paymentech will provide to Merchant, network and connectivity via the underlying carrier's facilities to Paymentech's systems for card processing (the "Wireless Services"). Merchant agrees that the Wireless Services are being provided solely for the purposes of connecting to Paymentech's systems to facilitate Merchant's processing of credit card, debit card and gift card transactions as applicable. Except as otherwise defined herein, capitalized terms used herein shall have the meaning assigned to them in the Merchant Agreement. Any express conflict between the terms and conditions of the Operating Guide and the Merchant Agreement shall be resolved in favour of the Operating Guide with respect to the provision of the Wireless Services. Except as altered hereby, the provision of the Operating Guide shall be governed by the Merchant Agreement. Paymentech may change any aspect of the Wireless Services, including without limitation features and functionality if any such aspect is changed by the underlying carrier of the Wireless Services.

2) Merchant Obligations:

a) Merchant agrees not to tamper with, alter or otherwise rearrange the Wireless Services nor will it permit or assist others to abuse or fraudulently use the Wireless Services, including but not limited to using the Wireless Services.

i. In any manner which interferes unreasonably with the Wireless Services of the underlying carrier's network, or access thereto by other persons; or

ii. for any purpose or in any manner directly or indirectly in violation of applicable laws or in violation of third party rights. Merchant will be responsible for use of the Wireless Services by any of its employees, officers, directors, agents or subcontractors. Merchant agrees to comply with any third party software license terms and conditions in respect of software used by the Merchant in connection with the use of the Wireless Services.

b) Merchant will not resell or share the Wireless Services; use the Wireless Services to operate an e-mail, web, news or other similar service; use the Wireless Services to transmit or send any annoying, inappropriate, improper, excessive, threatening or obscene material or to otherwise harass, offend, threaten, embarrass, distress or invade the privacy of any person; engage in any activity that could compromise the security of or disrupt or interfere with the Wireless Services or any network or computers on the Internet or disrupt or interfere with the Wireless Services of any Internet access provider; use unauthorized equipment with the Wireless Services; reproduce, alter, adjust, repair or tamper with any signalling, identification (including the MIN, ESN, IMEI, IMSI, and other numbers) or transmission function or component of any device used with the Wireless Services, and will not permit anyone other than the underlying carrier, Paymentech or an authorized person as determined by Paymentech to do so.

3) Limitation of Wireless Services:

a) Paymentech and underlying carrier do not guarantee timely, secure, error-free or uninterrupted Wireless Services or receipt of material or messages transmitted over or through underlying carrier network or the networks of other companies or through the Internet. The Wireless Services may fail or be interrupted for reasons beyond Paymentech or underlying carrier's reasonable control, including environmental conditions, technical limitations, defects or failures, limitations of the systems of other telecommunications companies, emergency or public safety requirements.

b) The Merchant acknowledges that the Wireless Services may be available to Merchant only when their Equipment is in operating range of the underlying carrier's facilities. In addition, the Wireless Services may be temporarily refused, interrupted, or limited at any time because of: (i) limitations to the underlying carrier's facilities; (ii) transmission limitations caused by atmospheric, topographical or other factors reasonably outside of underlying carrier's' control; or (iii) equipment modifications, upgrades, relocations, repairs, and other similar activities necessary for the proper or improved operation of the underlying carrier's Wireless Services. Individual data transmissions may be involuntarily delayed for a variety of reasons, including atmospheric conditions, topography, weak batteries, system over-capacity, movement outside a service area and gaps in coverage within a service area.

4) Monitoring:

a) Merchant acknowledges that (i) it is possible for third parties to monitor data traffic over the facilities of the underlying carrier and privacy cannot be guaranteed; and (ii) Merchant assumes full responsibility for the establishment of appropriate security measures to control access to its respective equipment and information.

b) Paymentech and underlying carrier have the right, but not the obligation, to monitor or log any site or use of the Wireless Services. Merchant consents to any such monitoring and logging that is necessary to satisfy any law, regulation or other government request or to enhance operating efficiencies, improve Wireless Service levels, assess customer satisfaction, or protect Paymentech from unwanted use of certain Wireless Services or applications or in accordance with the terms of the Merchant Agreement and the Operating Guide. Paymentech and underlying carrier reserve the right to delete, remove or block access to any Internet capability, content, information or third party products or services available or transmitted through the Wireless Services.

5) Warranties:

EXCEPT AS EXPRESSLY SET FORTH HEREIN, PAYMENTECH AND UNDERLYING CARRIER MAKE NO REPRESENTATIONS, WARRANTIES, CONDITIONS (EXPRESS, IMPLIED OR STATUTORY) WHATSOEVER INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE RELATING TO THE WIRELESS SERVICES AND ANY EQUIPMENT AND SHALL HAVE NO LEGAL, EQUITABLE, OR OTHER LIABILITY OF ANY KIND TO MERCHANT REGARDLESS OF THE FORM OF ACTION, WHETHER FOR BREACH OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE. NEITHER THIS DOCUMENT NOR ANY DOCUMENTATION FURNISHED UNDER IT IS INTENDED TO EXPRESS OR IMPLY ANY WARRANTY BY PAYMENTECH THAT THE WIRELESS SERVICES WILL FUNCTION WITHOUT INTERRUPTION OR ERRORS OR THAT IT WILL OPERATE IN A PARTICULAR TERRITORY OR AREA. ANY SECURITY MECHANISMS INCORPORATED IN THE WIRELESS SERVICES HAVE INHERENT LIMITATIONS, AND MERCHANT MUST INDEPENDENTLY DETERMINE THAT SUCH MECHANISMS ADEQUATELY MEET ITS SECURITY AND RELIABILITY REQUIREMENTS. BY USING THE WIRELESS SERVICES, MERCHANT REPRESENTS THAT IT HAS SO DETERMINED. MERCHANT EXPRESSLY UNDERSTANDS AND AGREES THAT IT HAS NO CONTRACTUAL RELATIONSHIP WHATSOEVER WITH THE UNDERLYING CARRIER AND THAT THE MERCHANT IS NOT A THIRD PARTY BENEFICIARY OF ANY AGREEMENT BETWEEN PAYMENTECH AND THE UNDERLYING CARRIER.

6) Limitation of Liability:

A. PAYMENTECH OR UNDERLYING CARRIER SHALL NOT HAVE ANY LIABILITY TO MERCHANT FOR (A) LIBEL, SLANDER, DEFAMATION, THE INFRINGEMENT OF COPYRIGHT, PRIVACY OR OTHER RIGHTS, ARISING FROM MATERIAL OR MESSAGES TRANSMITTED OVER THE TELECOMMUNICATIONS NETWORK OF UNDERLYING CARRIER OR RECORDED ON THE EQUIPMENT; (B) DAMAGES ARISING OUT OF A MERCHANT'S ACT, DEFAULT, NEGLECT OR OMISSION IN THE USE OR OPERATION OF EQUIPMENT ACTIVATED ON THE TELECOMMUNICATIONS NETWORKS OF UNDERLYING CARRIER; (C) DAMAGES ARISING OUT OF THE TRANSMISSION OF MATERIAL OR MESSAGES OVER THE TELECOMMUNICATIONS NETWORKS OF UNDERLYING CARRIER ON MERCHANT'S BEHALF, WHICH IS IN ANY WAY UNLAWFUL; OR (D) ANY ACT, OMISSION OR NEGLIGENCE OF OTHER COMPANIES OR TELECOMMUNICATIONS SYSTEMS IN RELATION TO THE PROVISION OF THE WIRELESS SERVICES, WHEN THE FACILITIES OF SUCH OTHER COMPANIES OR TELECOMMUNICATIONS SYSTEMS ARE USED IN ESTABLISHING CONNECTIONS TO OR FROM FACILITIES AND EQUIPMENT CONTROLLED BY MERCHANT (D) DAMAGES, INCLUDING LOSS OF EARNINGS OR PROFIT OR HARM TO PERSONS OR PROPERTY, RESULTING FROM MISTAKES, OMISSIONS, INTERRUPTIONS, DELAYS, ERRORS OR OTHER DEFECTS OR FAILURES IN TRANSMISSION, FEATURES OR FUNCTIONS, FROM DEFECTS IN OR

FAILURES OF EQUIPMENT, OR FROM ANY OTHER CAUSE RELATED TO THE PROPER OR IMPROPER USE OF THE WIRELESS SERVICES OR EQUIPMENT BY MERCHANT.

B. PAYMENTECH AND UNDERLYING CARRIER SHALL NOT BE LIABLE TO MERCHANT OR TO ANY OTHER PERSON FOR ANY LOSS OF PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF DATA OR INFORMATION, OR FOR ANY PUNITIVE, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE PROVISION, USE OR FAILURE OF THE WIRELESS SERVICES, OR THE EQUIPMENT OR OTHER DEVICES USED WITH THE WIRELESS SERVICES, WHETHER CLAIMED IN CONTRACT, TORT OR OTHERWISE, EVEN IF PAYMENTECH OR UNDERLYING CARRIER COULD REASONABLY HAVE FORESEEN OR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

C. IN NO EVENT SHALL THE AGGREGATE, TOTAL LIABILITY OF PAYMENTECH OR UNDERLYING CARRIER FOR ANY DAMAGES, LOSSES AND CAUSES OF ACTION (WHETHER CLAIMED IN CONTRACT, TORT OR OTHERWISE) ARISING OUT OF OR IN CONNECTION WITH THE PROVISION, USE OR FAILURE OF THE WIRELESS SERVICES, OR ANY EQUIPMENT OR OTHER DEVICES USED WITH THE WIRELESS SERVICES, INCLUDING DAMAGES FOR PHYSICAL INJURY, DEATH OR DAMAGE TO PROPERTY, EXCEED AN AMOUNT EQUAL TO ONE MONTH OF FEES PAID BY MERCHANT TO PAYMENTECH FOR EQUIPMENT FEES, CALCULATED AS AN AVERAGE OVER THE THREE MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT WHICH GAVE RISE TO THE CLAIMS.

7) Indemnity:

Merchant shall indemnify and hold harmless Paymentech, the underlying carrier supplying Wireless Services to Paymentech, and their respective officers, employees, and agents against damages, losses, expenses, all manner of actions, claims, damages, liabilities and judgments (including reasonable legal fees and court costs) sustained by or made against Paymentech, the underlying carrier supplying Wireless Services to Paymentech, any and all claims, including without limitation claims for libel, slander, infringement of copyright, or personal injury or death, arising in any way directly or indirectly in connection with the Wireless Services provided hereunder or caused by Merchant's non-compliance with the terms of the Merchant Agreement, including the Operating Guide or the use, misuse, failure to use, or inability to use the Wireless Services provided to Merchant or with any data, software or Equipment used by any person with the Wireless Services provided to Merchant, or with any data, software, or Equipment used by any person with the Wireless Services.

8) MERCHANT HEREBY ACKNOLWEDGES THE FOLLOWING:

A. PAYMENTECH IS ACTING AS AGENT TO THE UNDERLYING CARRIER SUPPLYING WIRELESS SERVICES TO PAYMENTECH FOR THE LIMITED PURPOSE OF SECURING PERFORMANCE OF THE FOREGOING PROVISIONS.

B. MERCHANT HAS NO PROPERTY RIGHT IN ANY IDENTIFIER ISSUED TO OR ASSOCIATED WITH MERCHANT OR ANY EQUIPMENT USED BY MERCHANT.

C. THE UNDERLYING CARRIER'S WIRELESS SERVICES DO NOT INCLUDE ANY VOICE WIRELESS SERVICES.

D. THE SIM SUPPLIED WITH THE EQUIPMENT MAY ONLY BE USED BY MERCHANT IN SUCH EQUIPMENT AND IN NO OTHER DEVICE.

E. MERCHANTS MAY ONLY ROAM INCIDENTALLY TO THEIR USE OF THE WIRELESS SERVICES IN CANADA. WHEN ROAMING OUTSIDE OF UNDERLYING CARRIER'S COVERAGE AREA, MERCHANT IS RESPONSIBLE FOR ALL APPLICABLE CHARGES.

9) Confidentiality:

Solely with respect to the Wireless Services provided hereunder, unless Merchant provides express consent or disclosure is pursuant to a legal power, all information kept by Paymentech or underlying carrier regarding the Wireless Services hereunder, other than the Merchant's name, address and listed telephone number, is confidential and may not be disclosed by Paymentech or underlying carrier to anyone other than:

a) the Merchant;

b) a person who, in the reasonable judgment of Paymentech or underlying carrier, is seeking the information as an agent of the Merchant;

c) another telephone company, provided the information is required for the efficient and cost-effective provision of telephone service and disclosure is made on a confidential basis with the information to be used only for that purpose;

d) a company involved in supplying Paymentech or underlying carrier with telephone or telephone directory related Wireless Services, provided the information is required for that purpose and disclosure is made on a confidential basis with the information to be used only for that purpose; or

e) an agent retained by Paymentech or underlying carrier in the collection of Merchant's account, provided the information is required for and is to be used only for that purpose.

Express consent may be taken to be given by Paymentech or underlying carrier where the Merchant provides:

i. written consent;

ii. oral confirmation verified by an independent third party;

iii. electronic confirmation through the use of a toll-free number;

iv. electronic confirmation via the Internet;

v. oral consent, where an audio recording of the consent is retained by Paymentech; or

vi. consent through other methods, as long as an objective documented record of Merchant's consent is created by the Merchant or by an independent third party.

10) Limits on Liability for Emergency Wireless Services Provided on a Mandatory Basis:

This section 10 applies only to the provision of emergency Wireless Services on a mandatory basis. In respect of the provision of emergency Wireless Services on a mandatory basis, Paymentech and underlying carrier are not liable for:

1. libel, slander, defamation or the infringement of copyright arising from material or messages transmitted over Paymentech or underlying carrier's network from Merchant's property or premises or recorded by the equipment;

a. damages arising out of Merchant's act, default, neglect or omission in the use or operation of equipment provided by Paymentech;

b. damages arising out of the transmission of material or messages over Paymentech or underlying carrier's network on Merchant's behalf which is in any way unlawful; or

c. any act, omission or negligence of other companies or telecommunications systems when their facilities are used in establishing connections to or from Merchant's facilities and equipment.

2. Furthermore, except in cases where negligence on Paymentech's or underlying carrier's part results in physical injury, death or damage to Merchant's property or premises, Paymentech's or underlying carrier's liability for negligence related to the provision of emergency Wireless Services on a mandatory basis is limited to the greater of $20 and three times the amount (if any) Paymentech or underlying carrier would otherwise be entitled to receive as a refund for the provision of defective service. However, Paymentech or underlying carrier's liability is not limited by this subsection in cases of deliberate fault, gross negligence or anti competitive conduct on Paymentech or underlying carrier's part or in cases of breach of contract where the breach results from Paymentech or underlying carrier's gross negligence.

11) Miscellaneous:

Sections 5, 6, 7, 8, 9, 10 and 11 herein shall survive termination of the Merchant Agreement.

CHASE™
Paymentech

1 800 265.5158
24/7 Merchant Support

1 877 552.5533
Business Sales Centre

CHASE™ Paymentech

WKCAN/005-EN 02/10
Printed in Canada