

MERCHANT APPLICATION



Merchant # _____
 New Location Additional Location
2590 Willamette Drive NE • Suite 202 • Lacey, WA 98516
 Tel: 360-357-1400 Fax: 360-357-1425
www.fasttransact.com ISO#: 9765

▶ Business Information

Legal Name:			Name of Account (Doing Business As):		
Legal Address:			Physical Street Address (No P.O. Box):		
City:	State:	Zip:	City:	State:	Zip:
Phone #: ()	Contact:		DBA Phone #: ()		
Must Choose One Mailing Address: <input type="checkbox"/> DBA Address <input type="checkbox"/> Legal Address		E-Mail Address:	Website Address: www.		
Federal Tax #	# of Locations	Years in Business	Years Owned Business		
Bank Reference:			Contact:	Phone #: ()	

▶ Owners or Officers • Individual Ownership Must be Equal to or Greater than 50%

Name:	Title:	Date of Birth:	Applicant's SS #:	% Equity Ownership:
1.				
Residence Address:		City:	State:	Zip:
# Years:	Driver's Lic. #:	State:	Home Phone: ()	
Name:	Title:	Date of Birth:	Applicant's SS #:	% Equity Ownership:
2.				
Residence Address:		City:	State:	Zip:
# Years:	Driver's Lic. #:	State:	Home Phone: ()	

▶ Business Profile

Type of Ownership: Sole Proprietor Partnership PA or PC
 Corporation Limited Liability Company Not For Profit

Type of Goods or Services Sold: _____ SIC Code: _____

Do you currently accept Visa/Mastercard? Yes No : Name of Current Processor: _____
(If yes, you should submit 3 current months' statements.)

Has Merchant or any associated principal disclosed below filed Yes Date: _____
 bankruptcy or been subject to involuntary bankruptcy? No

▶ Sales Profile

Merchant Type:	Visa/MasterCard Sales Profile (Be Accurate):
<input type="checkbox"/> Retail	Card Swipe %
<input type="checkbox"/> Restaurant	Manual Key Entry with Imprint, Card Present %
<input type="checkbox"/> Lodging	Mail Order/Telephone %
<input type="checkbox"/> Service	Internet %
<input type="checkbox"/> Internet	
<input type="checkbox"/> Home Based	
<input type="checkbox"/> Other	Total = 100%

▶ Business Trade Suppliers • List Two

Name:	Address:	Contact:	Phone #: ()
Name:	Address:	Contact:	Phone #: ()

▶ Merchant Site Survey Report • To Be Completed by Sales Representative

Merchant Location: Retail Location with Store Front Office Building Internet Residence Other _____

Area Zoned: Commercial Industrial Residential Square Footage: 0-250 251-500 501-2,000 2,001+

Does the amount of inventory and merchandise on shelves and floor appear consistent with this type of business? Yes No
 If No, explain: _____

The Merchant: Owns Leases the Business Premises Landlord Name & Phone #: _____

Further Comments by Inspector (Must Complete) _____

I hereby verify that this application has been fully completed by merchant applicant and that I have physically inspected the business premises of the merchant at this address and the information stated above is true and correct to the best of my knowledge and belief.

Verified and Inspected by: _____ Office #: 9765 Representative #: _____ Representative Signature: _____ Date: _____

X Credit Card Advance **X**

► Visa / Mastercard Standard Retail / High Risk Retail Rates

Merchant Chooses to accept the following:	
VS/MC (Other Cards) Discount Rate:	_____ %
VS/MC Debit Card Discount Rate:	_____ %
VS/MC MID Qualified:	_____ %
VS/MC Non Qualified:	_____ %
AMEX Discount Rate:	_____ %
Discover Discount Rate:	_____ %

► Fees

VS/MC Transaction Fee:	_____	Per Item
Non-Bankcard Transaction Fee:	_____ .25	Per Item
Statement Fee:	_____	Monthly
VIMAS Online Service:	_____	Monthly
Monthly Minimum:	_____ \$20.00	Monthly
Annual Fee:	_____ \$55.00	Per Year
Debit Transaction Fee Plus Network Fees:	_____	Per Item
EBT Transaction Fee:	_____	Per Item
EBT Statement Fee:	_____	Monthly
Batch Fee:	_____ .25	Per Batch
Manual Imprinter: QTY: _____	_____	One Time
Chargeback/ACH Reject Fee:	_____ \$25.00	Per Item
Retrieval Fee:	_____ \$5.00	Per Item
Voice Authorization Fee:	_____ .95	Per Call
Early Termination Fee:	_____ \$250.00	One Time
Others (please specify): _____		

► Mail / Phone / Internet / Touchtone Rates

Merchant Chooses to accept the following:	
VS/MC (Other Cards) Discount Rate:	_____ %
VS/MC Debit Card Discount Rate:	_____ %
VS/MC MID Qualified:	_____ %
VS/MC Non Qualified:	_____ %
AMEX Discount Rate:	_____ %
Discover Discount Rate:	_____ %

► Fees

VS/MC Transaction Fee:	_____	Per Item
Non-Bankcard Transaction Fee:	_____	Per Item
Statement Fee:	_____	Monthly
VIMAS Online Service:	_____	Monthly
Monthly Minimum:	_____ \$25.00	Monthly
Annual Fee:	_____ \$55.00	Per Year
MOTO/Internet Surcharge:	_____ .05	Per Item
AVS Surcharge:	_____ .05	Per Item
Batch Fee:	_____ .30	Per Batch
Manual Imprinter: QTY: _____	_____	One Time
Chargeback/ACH Reject Fee:	_____ \$25.00	Per Item
Retrieval Fee:	_____ \$5.00	Per Item
Voice Authorization Fee:	_____ .95	Per Call
Early Termination Fee:	_____ \$250.00	One Time
Others (please specify): _____		

► Merchant Benefits Club

Yes, I want to participate in the optional Merchant Benefits Club which includes equipment support and replacement for an additional \$9.50 per terminal per month. Initials: **X**

► American Express

By signing below, I represent that the information I have provided on the Application is complete and accurate and I authorize American Express Travel Related Services Company, Inc ("American Express") to verify the information on this Application and to receive and exchange information about me, including, requesting reports from consumer reporting agencies. If I ask American Express whether or not a consumer report was requested, American Express will tell me, and if American Express received a report, American Express will give me the name and address of the agency that furnished it. I understand that upon American Express' approval of the business entity indicated above to accept the American Express Card, the Terms and Conditions for American Express® Card Acceptance ("Terms and Conditions") will be sent to such business entity along with a Welcome Letter. By accepting the American Express card for the purchase of goods and/or services, you agree to be bound by the Terms and Conditions.

Signature: **X**

SIGN HERE

Date: _____

► Discover

By signing below, I represent that the information I have provided on this application is complete and accurate. I hereby request for Discover® Card acceptance to be added to my Cynergy Data Merchant Application. I understand that the Terms and Conditions for Discover Card Acceptance (Terms and Conditions) will be sent to the business indicated above upon approval by Discover Financial Services, Inc. for this business entity to accept the Discover Card by Discover Financial Services, Inc. By accepting the Discover Card for the purchase of goods and/or services, I agree to be bound by the Terms and Conditions.

Signature: **X**

SIGN HERE

Date: _____

► Debit/Credit Authorization • Staple Voided Check Here

Merchant authorizes Processor or Bank to present Automated Clearing House credits, Automated Clearing House debits, wire transfers, or depository transfer checks to and from the following account and to and from any other account for which Processor or Bank are authorized to perform such functions under the Merchant Processing Agreement, for the purposes set forth in the Merchant Processing Agreement. This authorization extends to such entries in said account concerning lease, rental or purchase agreements for POS terminals and/or accompanying equipment and/or check guarantee fees and amounts due for supplies and materials. This Automated Clearing House authorization cannot be revoked until all Merchant obligations under this Agreement are satisfied, and Merchant gives Cynergy Data written notice of revocation.

DDA: **INVESTIGATIVE CONSUMER REPORT:** An investigative or consumer report may be made in connection with application. MERCHANT authorizes BANK or any of its agents to investigate the references provided or any other statements or data obtained from MERCHANT, from any of the undersigned individual credit or financial responsibility. You have a right, upon written request, to a complete and accurate disclosure of the nature and scope of the investigation requested.

AVERAGE TICKET SIZE: _____

AVERAGE MONTHLY VOLUME: _____

Each person certifies that the average ticket size and sales volume indicated is accurate and agrees that any transaction or monthly volume that exceeds either of the above amounts could result in delayed and/or withheld settlement of funds. Also, see paragraphs 4c and 13b of the MERCHANT Processing Agreement regarding suspension and termination of MERCHANT.

IMPORTANT NOTICE: All information contained in this application was completed, supplied and/or reviewed by the undersigned Merchant. Processor shall not be responsible for any change in printed terms unless specifically agreed to in writing by an officer of Processor and/or Bank of America, N.A., Charlotte, NC. By signing below you are agreeing to the provisions stated within this merchant application, on the reverse side (the Merchant Agreement) and acknowledge receipt of the merchant operating guide. Those provisions must be read before signing. By signing below, you agree to the terms on the front and back of this MERCHANT Processing Agreement and the merchant operating guide.

► Individual Guaranty • No Titles

As a primary inducement to Processor and Bank to enter into this Agreement, the undersigned Guarantor(s), by signing this Agreement, jointly and severally, unconditionally and irrevocably, personally guarantee the continuing full and faithful performance and payment by Merchant of each of its duties and obligations to Processor and Bank under this Agreement or any other agreement currently in effect or in the future entered into between Merchant or its principals and Processor or Bank, as such agreements now exist or are amended from time to time, with or without notice. Guarantor(s) understands further that Processor or Bank may proceed directly against Guarantor(s) without first exhausting their remedies against any other person or entity responsible to it or any security held by Processor and Bank or Merchant. This guarantee will not be discharged or affected by the death of the undersigned, will bind all heirs, administrators, representatives and assigns and may be enforced by or for the benefit of any successor of Processor and Bank. Guarantor(s) understand that the inducement to Processor and Bank to enter into this agreement is consideration for the guaranty, and that this guaranty remains in full force and effect even if the Guarantor(s) receive no additional benefit from the guaranty.

AGREED AND ACCEPTED

SIGN HERE

X _____ Date

#1 From Application - Signature

X _____ Date

#2 From Application - Signature

► For All Corporations • Corporate Resolution

The indicated officer(s) identified in numbers 1 and/or 2 below have the authorization to execute the MERCHANT Processing Agreement on behalf of the here within named corporation. **MERCHANT UNDERSTANDS THAT THIS AGREEMENT SHALL NOT TAKE EFFECT UNTIL MERCHANT HAS BEEN APPROVED BY BANK AND A MERCHANT NUMBER IS ISSUED.**

Print Legal Name of Merchant Business

SIGN HERE

X _____ Date

#1 From Application - Signature

X _____ Date

#2 From Application - Signature

X _____ Date

Accepted by Processor

X _____ Date

Accepted by Bank of America, N.A., Charlotte, NC.

Merchant Processing Agreement

This Merchant Processing Agreement ("Agreement") is entered into on the Effective Date defined in Section 13.A, below, between the business indicated on the Merchant Application ("Merchant" or "you"), Cynergy Data ("CD"), BA Merchant Services, LLC, ("BAMS") (CD and BA Merchant Services, LLC. are collectively referred to as Processor), and Bank of America, N.A. ("Bank").

Recitals
Merchant desires to accept Debit Cards and/or Other Cards, as indicated on the Merchant Application, validly issued by members of Visa U.S.A., Inc. ("Visa") and MasterCard International, Incorporated ("MasterCard"). "Debit Card" means all Visa or MasterCard cards issued by a non-U.S. bank, a Visa or MasterCard card that accesses a consumer's asset account within 14 days after purchase, including but not limited to Visa or MasterCard issued stored value, prepaid, payroll, EBT, gift, and consumer check cards, and debit cards validly issued by the debit card networks indicated in Section 4.G below ("Debit Networks"), such as on-line (i.e., internet) debit cards, and all Visa or MasterCard cards issued by a non-U.S. bank, a Visa or MasterCard card that accesses a consumer's asset account within 14 days after purchase, including but not limited to Visa or MasterCard issued stored value, prepaid, payroll, EBT, gift, and consumer check cards, including but not limited to business and consumer credit cards and business debit cards. The category of card acceptance you have indicated on the Merchant Application will collectively be referred to as "Cards." Bank and Processor desire to provide Card processing services to Merchant. Therefore, Merchant, Processor and Bank agree as follows:

Terms and Conditions

1. Honoring Cards.

A. Disqualification. You will honor, without discrimination, any Debit Card and/or Other Card, as indicated by you on the Merchant Application, properly tendered by a Cardholder. "Cardholder" means a person presenting a Card and purporting to be the person in whose name the Card is issued. If you elect to accept only one of the card acceptance categories but later submit a transaction from a card in a different category, you agree that Processor and Bank may process the transaction and assess the appropriate fee, and that all terms of this Agreement will apply to that transaction. You will not establish a minimum or maximum transaction amount as a condition for honoring a Card. Cardholders will be entitled to the same services and return privileges you would normally cash back to a Cardholder who is not permitted by the Card Associations to honor the Card. Processor and Bank will not impose any special card rules unless permitted by the Card Associations in connection with the acceptance of a Card. "Card Association" means Visa, MasterCard, Discover, American Express, Japanese Credit Bureau, and/or a Debit Network, as applicable.

B. Cardholder Identification. You will identify the Cardholder and check the expiration date and signature on each Card. You will not honor any Card if: (i) the Card has expired; (ii) the signature on the sales draft does not correspond with the signature on the Card; (iii) the account number embossed on the Card does not match the account number on the Card's magnetic strip (as printed on the Card); or (iv) the Card is not a Visa or MasterCard card. If you are advised by Processor or Bank that you are required to provide personal information, such as a home or business telephone number, a home or business address, or a driver's license number as a condition for honoring a Card unless permitted under the Laws and Rules (defined in Section 14, below). You may require a Cardholder to complete a postcard or similar device that includes the Cardholder's account number, Card expiration date, signature, or any other Card account data in plain view when mailed.

C. Card Recovery. You will use your reasonable, best efforts to recover any Card: (i) on Visa Cards if the printed four digits above the embossed account number do not match the account number on the Card's magnetic strip; (ii) if you are advised by Processor or Bank (or a designee) the issuer of the Card or the designated voice authorization center to retain it; (iii) if you have reasonable grounds to believe the Card is counterfeit, fraudulent or stolen, or not authorized by the Cardholder; or (iv) for MasterCard Cards, the embossed account number, indent printed account number and/or encoded account number do not agree or the Card does not have a MasterCard hologram on the lower right corner of the Card face.

D. Surcharge. You will not add any amount to the posted price of goods or services you offer as a condition of paying with a Card, except the surcharge permitted by the applicable Laws and Rules. You may offer a discount from the standard price to induce a person to pay by cash, check or similar means rather than by using a Card.

E. Return Policy. You will properly disclose to the Cardholder at the time of the Card transaction and in accordance with the Rules, any limitation you have on accepting returned merchandise.

F. No Claim Against Cardholder. You will not have any claim against or right to receive payment from a Cardholder unless Processor and Bank refuses to accept the Sales Draft (as defined in Section 3) or revokes a prior acceptance of the Sales Draft after receipt of the Sales Draft. You will not accept any payment from a Cardholder relating to previous charges for merchandise or services included in a Sales Draft, and if you receive any such payments you promptly will remit them to Processor and Bank.

G. Disputes With Cardholder. All disputes between you and any Cardholder relating to any Card transaction will be settled between you and the Cardholder. Neither Processor or Bank bear any responsibility for such transactions.

2. Authorization.

A. Required on all Transactions. You will obtain a prior authorization for the total amount of a transaction via electronic terminal or device completing any transaction, and you will not process any transaction that has not been authorized. You will follow any instructions received during the authorization process. Upon receipt of authorization you may consummate only the transaction authorized and must note on the Sales Draft the authorization number. Where authorization is obtained, you will be deemed to warrant the true identity of the customer as the Cardholder.

B. Effect. Authorizations are not a guarantee of acceptance or payment of the Sales Draft. Authorizations do not waive any provisions of this Agreement or otherwise validate a fraudulent transaction or a transaction involving the use of an expired Card. Processor and Bank may prohibit you from accepting a Card for authorization electronically, and if your terminal is unable to read the magnetic stripe on the card, you will obtain an imprint of the card and the Cardholder's signature on the imprinted draft before presenting the Sales Draft to Processor and Bank for processing. Failure to do so may result in the assessment of a transaction surcharge on non-qualifying transactions.

3. Presentation of Sales Drafts.

A. Forms. You will use a Sales Draft ("Sales Draft") or other form approved by Processor and Bank to document each Card transaction. Each Sales Draft will be legibly imprinted with: (i) the merchant's name, location and account number; (ii) the information embossed on the Card presented by the Cardholder (either electronically or manually, and truncated, if applicable); (iii) the date of the transaction; (iv) a brief description of the goods or services involved; (v) the transaction authorization number; (vi) the total amount of the sale including any applicable taxes, or credit transaction; and (vii) adjacent to the signature line, a notation that all sales are final, if applicable.

B. Signatures. Sales Drafts must be signed by the Cardholder unless the Card transaction is a valid mail/telephone order. Cardholder signatures on Sales Drafts will be legibly imprinted with the merchant's name, location and account number. You will not require the Cardholder to sign the Sales Draft before you enter the final transaction amount in the Sales Draft.

C. Reproduction of Information. If the following information embossed on the Card and the Merchant's name is not legibly imprinted on the Sales Draft, you will legibly reproduce on the Sales Draft before submitting it to Processor and Bank: (i) the Cardholder's name; (ii) account number (truncated, if applicable); (iii) expiration date and (iv) the Merchant's name and place of business. Additionally, for MasterCard transactions you will legibly reproduce the name of the Bank issuing the Card as it appears on the Card.

D. Delivery and Retention of Sales Drafts. You will deliver a complete copy of the Sales Draft or credit voucher to the Cardholder at the time of the transaction. You will retain the "merchant copy" of the Sales Draft or credit memorandum for at least 3 years following the date of completion of the Card transaction (or such longer period as the Rules require).

E. Electronic Transmission. In using electronic authorization and/or data capture services, you will enter the data related to a sales or credit transaction into a computer terminal or magnetic stripe reading terminal no later than the close of business on the date the transaction is processed. You will not accept any payment from a Cardholder relating to previous charges for merchandise or services included in a Sales Draft, and if you receive any such payments you promptly will remit them to Processor and Bank. Processor and Bank's requirements for processing transactions. Information regarding a sales or credit transaction transmitted with a computer or magnetic stripe reading terminal will be transmitted by you to Processor and Bank or their agent in the form Processor and Bank from time to time specifies or as required under the Rules. If Processor or Bank requests a copy of a Sales Draft, credit voucher or other transaction evidence, you will provide it within 24 hours following the request.

4. Deposit of Funds and Funds Due Merchant.

A. Deposits. You agree that this Agreement is a contract of financial accommodation within the meaning of the Bankruptcy Code, 11 U.S.C § 365 as amended from time to time. Subject to this Section, Bank will deposit to the Designated Account (defined in Section 6 below) funds evidenced by Sales Drafts (whether evidenced in writing or by electronic means) complying with the terms of this Agreement and the Rules and will provide you provisional credit for such funds (less recoupment of any credit(s), adjustments, fines, charges, expenses, or fees). You understand and agree that Bank may withhold or deposit and payment to you will occur until the expiration of any chargeback period for: a) mail order, telephone order, or internet transactions on Cards issued by non-U.S. financial institutions, and a b) if Processor or Bank determine, in their sole and reasonable discretion, that a transaction or batch of transactions poses a risk of loss. Neither Processor nor Bank are responsible for any losses you may incur, including but not limited to NSF fees, due to such delayed deposit of funds. You acknowledge that your obligation to Processor and Bank for all amounts owed under this Agreement arise out of the same transaction as Processor and Bank's obligation to deposit funds to the Designated Account.

ii. Provisional Credit. Notwithstanding the previous sentences, under no circumstance will Processor or Bank be responsible for processing credits or adjustments related to Sales Drafts not originally processed by Processor and Bank. All Sales Drafts and deposits are subject to audit and final checking by Processor and Bank and may be adjusted for inaccuracies. You acknowledge that all credits provided to you are provisional and subject to chargebacks and adjustments: (i) in accordance with the Rules; (ii) for any of your obligations to Processor and Bank; and (iii) in any other situation constituting suspected fraud or a breach of this Agreement, whether or not the authorization is granted to offset from incoming transactions and to debit the Designated Account for individual or groups of funds evidenced by Sales Drafts. Final credit for those conditional funds will be granted within Processor and Bank's sole discretion.

iii. Processing Limits. Processor and Bank may impose a cap on the volume and ticket amount of Sales Drafts that they will process for you, as indicated to you by Processor and Bank. This limit may be changed by Processor and Bank upon written notice to you.

B. Chargebacks. You are fully liable for all transactions returned for whatever reason, otherwise known as "chargebacks." You will determine whether or not a transaction is charged back to Processor and Bank, and you may elect to grant conditional credit for individual or groups of funds evidenced by Sales Drafts. Final credit for those conditional funds will be granted within Processor and Bank's sole discretion.

C. Excessive Activity. Your presentation to Processor and Bank of Excessive Activity will be a breach of this Agreement and cause for immediate termination of this Agreement. "Excessive Activity" means, during any monthly period: (i) the dollar amount of chargebacks and/or retrieval requests in excess of 1% of the average monthly dollar amount of your Card transactions; (ii) sales activity in excess of the average monthly dollar amount of your Card transactions; or (iii) the number of retrieval requests in excess of the average monthly dollar amount of your Card transactions. You authorize, upon the occurrence of Excessive Activity, Processor and Bank to take any action they deem necessary including but not limited to, suspension or termination of processing privileges or creation or maintenance of a Reserve Account in accordance with this Agreement.

D. Credit Memoranda. You will issue a credit memorandum in any approved form, instead of making a cash advance, a disbursement to a Cardholder's account, or a debit to the Designated Account for the total face amount of each credit memorandum submitted to Bank. You will not submit a credit relating to any Sales Draft not originally submitted to Bank, nor will you submit a credit that exceeds the amount of the original Sales Draft. You will within the time period specified by the Rules, provide a credit memorandum or credit statement for every return of goods or forgiveness of debt for services which were the subject of a Card transaction.

ii. Revocation of Credit. Processor or Bank may refuse to accept any Sales Draft, and Processor and Bank may revoke prior acceptance of the Sales Draft of the balance of the transaction giving rise to the Sales Draft, if you do not comply with this Agreement, the Laws or the Rules; (b) the Cardholder disputes his liability to Processor and Bank for any reason, including but not limited to a contention that the Cardholder did not receive the goods or services, that the goods or services provided were not as ordered or pursuant to those chargeback rights enumerated in the Rules; or (c) the transaction giving rise to the Sales Draft was not directly between you and the Cardholder. You will pay Processor and Bank any amount previously credited to you for a Sales Draft not accepted by Processor and Bank or where accepted, is revoked by Processor and Bank.

4. Miscellaneous. You will not present for processing or credit, directly or indirectly, any transaction not originated as a result of a Card transaction directly between you and a Cardholder or any transaction you know or should know to be fraudulent or not authorized by the Cardholder. You will not sell or disclose to third parties Card account information other than in the course of performing your obligations under this Agreement.

i. "Debit Networks" means those debit card networks accepted by Processor, including but not limited to the following organizations and their successors: Star, NYCE, Pulse, Interlink, AFFN, Alaska, Jeanie, Accel, and Money Station.

ii. Credit Refunds. You will attempt to settle in good faith any dispute between you and a Cardholder involving a transaction. You will establish a fair, consistent policy for the exchange and return of merchandise and for the adjustment of amounts due on Debit Card sales. You will promptly initiate a refund to the customer (which may be made in cash, by an adjustment draft or with a cashier's check, as permitted by the Rules) whenever you determine that a Debit Card transaction should be canceled or reversed.

iii. Adjustments. Except as the Debit Networks may permit, you will not make any cash refunds or payments for returns or adjustments on Debit Card transactions but will instead complete an adjustment form provided or approved by Processor. The Debit Card Sales Draft for which no refund or return will be accepted by you must be clearly and conspicuously marked (including on the Cardholder's copy) as "final sale" or "no return" and must comply with the Rules.

vi. Error Resolution. You will refer Debit Card Cardholders with questions or problems to the institution that issued the Debit Card. You will cooperate with Processor and with each applicable Debit Network and its other members to resolve any alleged errors relating to transactions. You will permit and will pay all expenses of periodic examination and audit of functions related to each Debit Network, at such frequency as the applicable Debit Network deems appropriate. Audits will meet Debit Network standards, and the results will be made available to the Debit Network.

5. Other

A. Mail/Telephone Order. Processor and Bank caution against mail orders or telephone orders or any transaction in which the Cardholder and Card are not present ("mail/telephone orders") due to the high incidence of customer disputes. You will perform AVS and obtain the expiration date of the Card for a mail/telephone order and submit the expiration date when obtaining authorization of the Card transaction. For mail/telephone order transactions, you will type or print legibly on the signature line the following as applicable: telephone order or "TO" or mail order or "MO" You must promptly notify Processor and Bank if your retail/mail order/telemarketing order is cancelled, or if you receive a cancellation notice from the Cardholder. Processor and Bank may cease accepting mail/telephone order transactions, or limit its acceptance of such transactions, or increase their fees, or terminate this Agreement, or impose a Reserve Account (defined in Section 7.A), if this mix changes. You may not deposit a mail/telephone order Sales Draft before the product is shipped.

B. Recurring Transactions. For recurring transactions, you must obtain a written request from the Cardholder for the goods and services to be charged to the Cardholders account, the frequency of the recurring charge, and the duration of time during which such charge may be billed, including the date of the first billing cycle. You must obtain a cancellation notice from the Cardholder (i) the notice from Processor or Bank, or (ii) a response that the Card is not to be honored. You must print legibly on the Sales Draft the words "Recurring Transaction".

C. Multiple Sales Drafts. You will include a description and total amount of goods and services purchased in a single transaction on a single Sales Draft or transaction record, unless (i) partial payment is entered on the Sales Draft or transaction record and the balance of the transaction amount is paid in cash or by check at the time of transaction, or (ii) a Sales Draft represents an advance deposit on a Card transaction completed in accordance with this Agreement and the Rules.

D. Partial Completion.

i. Prior Consent. You will not accept for payment by Card any amount representing a deposit or partial payment for goods or services to be delivered in the future without the prior written consent of Processor or Bank. Such consent will be subject to Bank's final approval. The acceptance of a Card for payment or partial payment of goods or services to be delivered in the future without prior consent will be deemed a breach of this Agreement and cause for immediate termination, in addition to any other remedies available under this Agreement.

ii. Acceptance. If you have obtained prior written consent, then you will complete such Card transactions in accordance with the terms set forth in this Agreement, the Rules, and the Laws. Cardholders must execute one Sales Draft when making a deposit with a Card and a second Sales Draft when paying the balance. You will note upon the Sales Draft the words "deposit" or "balance" as appropriate. You will not deposit the Sales Draft labeled "balance" until the goods have been delivered to Cardholder or you have fully performed the services.

E. Electronic Commerce. Processor does not present any Sales Draft or other memorandum to Bank for processing (whether by electronic means or otherwise) which relates to the sale of goods or services for future delivery without Processor or Bank's prior written authorization. Such consent will be subject to Bank's final approval. If Processor or Bank have given such consent, you represent and warrant to Processor and Bank that you will not rely on any proceeds or credit resulting from such transactions to purchase or furnish goods or services. You will maintain sufficient working capital to provide for the delivery of goods or services at the agreed upon future date, independent of any credit or proceeds resulting from sales drafts or other memoranda taken in connection with such transactions.

F. Electronic Commerce. You may process electronic commerce ("EC") transactions only if you have so indicated on the Application, and only if you have obtained CD's consent. If you submit EC transactions without such consent, Processor may immediately terminate this Agreement. If you have indicated on the Application that you will be submitting EC transactions, you acknowledge that you have received a copy of the Visa Cardholder Information Security Program ("CISP") manual. If you present EC transactions, such transactions must comply with the CISP requirements and all other applicable Rules and Law. You understand that electronic commerce transactions are high risk and are subject to a higher incidence of chargebacks. You are liable for all chargebacks and losses related to EC transactions, whether or not: i) EC transactions have been encrypted; and ii) you have obtained consent to engage in such transactions. Encryption is not a guarantee of payment and will not waive any provision of this Agreement or otherwise validate a fraudulent transaction. You must offer Cardholders a secure transaction method, such as Secure Sockets Layer (SSL) or 3-D Secure. All communication costs related to EC transactions are your responsibility. You understand that Processor will not manage the EC telecommunications link and that it is your responsibility to manage that link. All EC transactions will be settled under the Rules.

G. Requirements. For goods to be shipped on EC transactions, you may obtain authorization up to 7 calendar days prior to the shipment date. You need not to obtain a second authorization if the Sales Draft amount is within 15% of the authorized amount, provided that the additional amount represents shipping costs. Further, your web site must contain all of the following information: a) complete description of the goods or services offered, b) returned merchandise and refund policy, c) customer service contact, including electronic mail address and/or telephone number, d) transaction currency (such as U.S. or Canadian dollars), e) export or legal restrictions, f) your delivery policy, g) your return policy, h) your shipping and handling charges, i) your payment method, and h) the Visa flag symbol in full color. If you store cardholder account numbers, expiration dates, and other personal cardholder data in a database, you must follow Visa and MasterCard guidelines on securing such data. You shall immediately notify Processor of any suspected or confirmed loss or theft of any transaction information. In addition, you must provide reasonable access to Visa, MasterCard, a Debit Network or independent third party to verify your ability to prevent future security breaches in a manner consistent with the requirements of any Rule.

H. Security. You agree that you are, and will remain, fully compliant with the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

I. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

J. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

K. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

L. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

M. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

N. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

O. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

P. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

Q. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

R. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

S. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

T. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

U. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

V. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

W. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

X. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

Y. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

Z. Upon your request, Processor and Bank will provide you with a copy of the Payment Card Industry Data Security Standard required by the Card Associations, including but not limited to undertaking the required annual or quarterly self-assessments and Web infrastructure scans, as appropriate. If you accept EC transactions, you must: 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 antivirus software; 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 and audit data to detect, report, and prevent security system and process; manage data privacy policy that addresses information security for employees and contractors; and restrict physical access to cardholder 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. Further, you must reference the protection of cardholder information and compliance with the Visa CISP Rules in contracts with other service providers. You agree to indemnify and reimburse Processor and Bank immediately for any loss, liability, assessment or fine incurred due to your breach of this Section.

