worldpay

Worldpay Integrated Payments
Merchant Application
CARD PROCESSING SERVICES

Merchant Business Information

Application Type: ◉ Never Accepted Cards ○ Processor Change ○ Ownership Change

Merchant Business Legal Name:
(as shown on your business income tax return)

Business Name:
(DBA/Outlet Name)

Business Website:

Federal Tax ID #:
(Employer Identification Number or, if Sole Proprietor, Social Security Number)

Year Business Established:

Type of Goods or Services Sold:

Year Acquired by Owner:

Physical Address (no PO Boxes)

Address:
City:
State:
Zip:
Phone Number:
Fax:

Mailing Address (if different from physical address)

Address:
City:
State:
Zip:
Phone:
Fax:

IRS Reporting Verification. *Payment settlement entities are required to report to the Internal Revenue Service the amount of reportable payment card transactions. Annually in January, you will receive a 1099-K providing details of your previous year reportable payment card transactions with a copy being filed electronically directly with the IRS.*
THE BUSINESS INFORMATION MUST MATCH IRS RECORDS, AND SHOULD AGREE WITH THE INFORMATION LISTED ON YOUR INCOME TAX RETURN. IF YOUR INFORMATION DOES NOT MATCH IRS RECORDS, THE PROCESSING OF YOUR MERCHANT APPLICATION MAY BE DELAYED AND YOU MAY BE SUBJECT TO MANDATORY BACKUP WITHHOLDING AS REQUIRED BY IRS REGULATIONS.

Disclosure

IMPORTANT MEMBER BANK RESPONSIBILITIES: (1) A Visa Member is the only entity approved to extend acceptance of Visa products directly to a Merchant. (2) A Visa Member must be a principal (signer) to the Merchant Agreement. (3) The Visa Member is responsible for educating Merchants on pertinent Visa Operating Regulations with which Merchants must comply. (4) The Visa Member is responsible for and must provide settlement funds to the Merchant. (5) The Visa Member is responsible for all funds held in reserve that are derived from settlement.
IMPORTANT MERCHANT RESPONSIBILITIES: (1) Ensure compliance with cardholder data security and storage requirements. (2) Maintain fraud and chargeback below thresholds. (3) Review and understand the terms of the Merchant Agreement. (4) Comply with Operating Regulations. The responsibilities listed above do not supersede the terms of the Merchant Agreement and are provided to ensure the Merchant understands some important obligations of each party and that the Visa Member (Acquirer) is the ultimate authority should the Merchant have any problems.
Member Bank Information: Name: Fifth Third Bank, 38 Fountain Square Plaza, Cincinnati, OH 45263 (866) 250-9764
Merchant Services Provider Contact Information: Worldpay Integrated Payments, 150 Mercury Village Drive, Durango, CO 81301 800-846-4472

Signature:

Name (printed):

Title:

Date:

Business Profile

Business Type:
○ Association/Estate/Trust* ○ Individual/Sole Proprietor* ☐ Publically Traded Corporation* ○ Partnership ○ Private Corporation
○ Limited Liability Company ○ Non-Profit/Tax Exempt ☐ SEC Registered (i.e. Inv. Advisor/Co, exchange/clearing)* ☐ Financial Institution* ○ Government Federal/State/Local*
*exempt from Beneficial Owner requirements and do not need to complete Control Owner or Beneficial Owner fields on page 3.
If tax exempt please send your sales tax exemption certificate to your sales representative

Seasonal Business: ○ Yes ◉ No If yes, enter the months of operation:

% Card Swiped 0 % Manually Keyed with Imprinter
% MOTO % Internet 100

Annual Visa/MC/Discover Sales ($):
Requested Highest Ticket ($):
Average Ticket ($):

The above sales volumes and average ticket $ representations are integral and a condition to the rates and fees set forth in the below rates and fees schedule. If your actual sales volumes or average ticket $ are different than the sales volumes or average ticket $ represented above, you understand and agree that your rates and fees may be changed.

Have you had more than 25 chargebacks within the last 12 months? ○ Yes ○ No

Do you accept transactions before the customer receives the product or service?
○ Yes ○ No
Percent of sales in this category:

Merchant Location:
◉ Retail Location with Store Front ○ Office Building
○ Residence ○ Other:

Market Type:
○ Retail ○ Supermarket ○ Restaurant
◉ E-Commerce ○ MO/TO ○ Lodging
○ Quick Serve ○ Other

Customer Return Policy:
○ Refund w/in days ☐ Exchange Only ○ None

Have you ever had a previous credit card processor terminate your merchant account?
○ Yes ◉ No
If yes, by whom?

Do you offer warranties, dues, subscriptions, memberships or other extended services?
○ Yes ◉ No
Duration of extended service or benefit (weeks):

% of Sales that are Business to Business

Does the Merchant use a Fulfillment House? ○ Yes ○ No
If yes, was the Fulfillment House inspected? ○ Yes ○ No

The Merchant: ○ Owns ◉ Leases the business premises

Surrounding Area: ◉ Commercial ○ Industrial ○ Residential

Designated Account: Bank Account to be used for Credit Card Processing Services:

Bank Name:	Financial Institution 9 Digit Routing Number:	DDA/Checking Account Number:

FUNDS MAY ONLY BE DEPOSITED INTO A BUSINESS CHECKING ACCOUNT. MERCHANT REPRESENTS AND ACKNOWLEDGES THAT THE ABOVE BANKING INFORMATION IS CORRECT AND, IF NO BANKING INFORMATION IS PROVIDED, THAT MERCHANT WILL BE UNABLE TO PROCESS TRANSACTIONS UNTIL BANKING INFORMATION IS PROVIDED TO PROCESSOR.

Rates and Fees Schedule

Pricing Type: ○ Tiered ◉ Interchange Plus	Rate	Per item	Other Services	Rate	Per item
Visa/MasterCard/Discover/PayPal Credit	%		○ Tiered ◉ Interchange Plus PIN Debit		
Visa/MasterCard/Discover Debit	%		○ American Express Direct Program	Set By Amex	
◉ American Express OptBlue® Program			Existing American Express Account? ○ Yes ○ No		
Estimated American Express Volume:			If Yes, Existing American Express SE#:		
EBT			EBT Merchant FNS #:		

If your annual estimated American Express Sales are greater than $1,000,000 you are not eligible for the American Express OptBlue® Program.

○ By checking this box, Merchant elects to opt out of the American Express Program

☐ By checking this box, Merchant elects to opt out of receiving American Express Marketing Materials. If you have elected for the Marketing Opt-out, you may continue to receive marketing communications while American Express updates its records, and you will continue to receive important transaction or relationship messages from American Express. If you have not elected for the Marketing Opt-Out, your mailing address, phone number, email address, fax number, and/or cell (or mobile) phone number may be used by American Express to send commercial marketing messages, which may include information about American Express products, services and resources.

The most favorable tiered discount and interchange plus pricing available for each payment plan type including the rates and per item and authorization fees, per transaction type are based upon you complying with all processing requirements as established by the applicable governing authority (i.e., a fully qualified transaction). See Section 6 of the Terms and Conditions for more information regarding non-qualifying surcharges and other fees. Per item fees are calculated per transaction, and rates and other percentage fees are calculated by multiplying the rates or fees and your applicable transaction volume. For American Express preauthorization, preauthorization capture, and settlement type transactions, the per item fee shall separately apply to such transaction types. A list of additional fees/rates can be found below under the heading "Other Rates and Fees" and certain of the Association Fees and Assessments can be found at http://info.vantiv.com/vipcontract.html.
Where Tiered discount rate pricing is provided, as indicated above, the fees quoted in the above rates and fees schedule plus Association and Network charged fees and assessments apply with transactions that are not fully qualified transactions being additionally subject to non-qualified surcharges up to 2.59% and $.10 in addition to the rates quoted. Where Interchange Plus pricing is provided and otherwise for Other Services, as indicated above, the fees quoted in the above rates and fees schedule shall apply plus interchange rates and Association and Network charged fees and assessments with transactions that are not fully qualified transactions being additionally subject to higher interchange rates and assessments published by the applicable Associations and Networks plus a fee up to 1.95%. For a complete list of interchange rates for Visa and MasterCard, visit the websites: http://www.visa.com and www.mastercard.com. You acknowledge that interchange rates and Association and Network fees and assessments are subject to change without notice.

Other Rates and Fees

Batch/ACH Fee (per occurrence)	$0.00	Retrieval Fee (per occurrence)	$2.50	FastAccess™ Funding (per occurrence)[3]	
Voice Authorization Fee (per occurrence)	$.60	Minimum Monthly Discount	$25.00	☐ Next Day Funding (Per month) Batch must be closed by 7pm ET	$0.00
Voice AVS Fee (per occurrence)	$.60	Application Fee	$0.00	Monthly Statement Fee	$0.00
Dial Back-Up Fee (per item)	$0.10	Account Updater Setup Fee (per MID)[1]	$0.00	Non-Sufficient Funds (per occurrence)	$15.00
Account Maintenance Fee (per month)	$0.00	Account Updater Monthly Fee[1]	$0.00	Monthly Signature Merchant Location Fee	
Tokenization Monthly Fee (per MID)[1] Payment Account Identifier (PAI) Maximum	$0.00	Account Updater Charge (per valid update)[1]		TriPOS Setup Fee	$0.00
		Chargeback Service Fee[2]		TriPOS Monthly Fee	$0.00
Additional Fee per each PAI in excess of PAI Maximum[1]	.10	Optional Service – CheckGateway ACH Service (per occurrence)			

[1] See Section A.3 of Addendum A for Additional TransForm Tokenization and Account Update pricing and terms.
[2] See Section A.4 of Addendum A for Chargeback Service Fee information.
[3] See Section A.7 of Addendum A for FastAccess™ Funding terms.

OmniShield Security and Risk Fee Schedule

○ OmniShield Assure™	◉ OmniShield CNP	○ OmniShield Enterprise
Required for PCI Level 4 merchants ***Includes**: PCI Assist, Breach Assist, Point to Point Encryption, and EMV Support services. *Inclusions dependent upon Merchant payment solution **Pricing:** $ $24.95 /Month/MID	Required for PCI Level 3 merchants **Includes**: PCI Assist, Breach Assist **Provides access to**: eProtect **Pricing:** As set forth on separate OmniShield Price Quote	Available for PCI Level 1 and PCI Level 2 merchants **Provides access to**: PCI Assist, Point to Point Encryption, EMV Support services, eProtect **Pricing:** As set forth on separate OmniShield Price Quote

PCI Non-Validation Fee (NVF) / Non-Compliance Fee (NCF) $19.95/Month/MID. For additional OmniShield Security and other security service terms and information, see Section 6.G of the Merchant Processing Agreement Terms and Conditions.

Cardholder Data Storage Compliance & Service Provider

Do you use a third party to store, process or transmit cardholder data? ○ Yes ◉ No
Do you store cardholder data? ○ Yes ◉ No

Primary Service Provider or Software Developer: CT Checkout
Software used by third party: n/a Version #: n/a

Are you compliant with the Payment Card Industry Data Security Standards? ◉ Yes ○ No Identify Security Assessor and certificate number: Last Certification Date:

Have you ever experienced an Account Data Compromise? ○ Yes ◉ No If yes, provide date of compromise: If yes, have you completed remediation? ○ Yes ○ No

All merchants must comply with the Payment Card Industry Data Security Standard ("**PCI DSS**"). Merchant is required to maintain the security of card data and to comply with the requirements of the PCI DSS. Merchant must validate its compliance with the PCI DSS and provide us with evidence that Merchant: (a) has successfully completed a Self Assessment Questionnaire and scan(s), if applicable, and (b) is compliant with the PCI DSS. We may offer one or more PCI products or services (the "**PCI Program**") to assist merchants in securing card data and complying with PCI DSS. Information on the PCI Program is set forth in Section 6.G of the Terms and Conditions and the applicable fees for the PCI Program are set forth above in this Merchant Application within the OmniShield Security and Risk Fee Schedule. All gateway or other vendor supplied software must be compliant with the Payment Application Data Security Standard rules ("**PA-DSS**").

Term of Agreement

Initial Term: 1 Year(s). See Sections 1.A and 7.B of the Terms and Conditions for information regarding the Term of this Agreement and Early Termination, including early termination fees.

Equipment and Third Party Product and Services Fees

In addition to other amounts owed under the Agreement, you will owe us the following amounts for equipment and the below indicated purchased products and services. You authorize us to debit the Designated Account in the amount of such charges, in accordance with Section 14 of the Terms and Conditions.

Description	Quantity	Per Item Cost or Fee	Other Terms
*Total Cost/Fees			*plus any applicable shipping fees and sales tax.

Shipping Address for Equipment: City: State: Zip:

Terminal Setup Information: Please select the appropriate setup of your equipment. (These settings can be changed after the equipment is deployed if necessary)

Processing Platform: ◯ IP Processing with Dial Backup ◯ Dial Only
Tips enabled: ◯ Yes ◯ No Reporting by Server/Cashier Number: ◯ Disabled ◉ Enabled

PIN Pad needed for Debit or EBT transactions requiring PIN entry
To Receive Funding batch must be settled manually at the end of your business days

Card Verification Methods (CVM):

◯ All – Includes support for Chip+PIN and Chip+Signature (if no CVM is selected this will be the default selection)

◯ Require Signature only – If this box is selected we will only require signature and will not prompt for PIN on Chip+PIN preferring cards. **Note, if you check this box you may be liable for chargebacks on lost and stolen cards with certain card brands. This may not be available through all POS systems, contact your POS Provider to determine if your POS System supports this option.

Authorized Representative and Signer Information

Authorized Representative/Signer Name: Date of Birth: Social Security Number:

Street Address (Physical, no PO Boxes): City: State: Zip:

Email: Own or Rent? Years There: Home Phone:

To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify and record information that identifies each person (including business entities) who opens an account. What this means for you: When you open an account, we will ask for your name, physical address, date of birth, taxpayer identification number and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents. The undersigned entity(ies) and individuals hereby unconditionally authorize us and Member Bank or its agents to: (i) investigate the information and references contained herein, and to obtain additional information about the Merchant and such individual(s) by pulling credit bureau and criminal background checks on the Merchant and its principals, including obtaining reports from consumer reporting agencies on individuals signing below as an owner, general partner, authorized representative, or Guarantor of Merchant, or providing their Social Security Number on the Application (if such individual asks us or Member Bank whether or not a consumer report was requested, we and/or Member Bank will tell such individual and, if we and/or Member Bank received a report, we and/or Member Bank will give the individual the name and address of the agency that furnished it) and (ii) update such information periodically throughout the terms of service of the Agreement.

Beneficial/Control Ownership – REQUIRED for Partnerships, Private Corporations, Limited Liability Companies, & Tax Exempt Organizations

To help the government fight financial crime, federal regulation requires certain financial institutions to obtain, verify, and record information about the beneficial owners of certain legal entity customers. Legal entities can be abused to disguise involvement in terrorist financing, money laundering, tax evasion, corruption, fraud, and other financial crimes. Requiring the disclosure of key individuals who own or control a legal entity (i.e., the beneficial owners) helps law enforcement investigate and prosecute these crimes. For more information go to, https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions.

Control Owner - An individual with significant responsibility to control, manage, or direct the legal entity

Full Name: Date of Birth: Social Security#:

Street Address (Physical, no PO Boxes): City: State: Zip:

Check this box if Control Owner listed above is also a Beneficial Owner, if this box is checked you do not need to relist the Control Owner as a Beneficial Owner below.

Beneficial Owner #1 – An owner who owns 25% or more of the legal entity

Full Name: Date of Birth: Social Security#:

Street Address (Physical, no PO Boxes): City: State: Zip:

Beneficial Owner #2 – An owner who owns 25% or more of the legal entity

Full Name: Date of Birth: Social Security#:

Street Address (Physical, no PO Boxes): City: State: Zip:

Beneficial Owner #3 – An owner who owns 25% or more of the legal entity

Full Name: Date of Birth: Social Security#:

Street Address (Physical, no PO Boxes): City: State: Zip:

Beneficial Owner #4 – An owner who owns 25% or more of the legal entity

Full Name: Date of Birth: Social Security#:

Street Address (Physical, no PO Boxes): City: State: Zip:

Additional Contact Information

Name:		Name:	
Role:	☐ Authorized Representative ☐ Primary Contact ☐ Manager	Role:	◯ Authorized Representative ◯ Primary Contact ◯ Manager
Phone Number:		Phone Number:	
Email Address:		Email Address:	

Authorized Representative: Has full rights to your account including: (i) changing banking information, contacts on account(s), and DBA information, and (ii) may view transactions on the portal and will be an admin on the portal, which grants employee access to the account(s).
Primary Contact: Can view transactions on the portal, call in transaction problems, change contacts on account(s), and change DBA information on all of your accounts. This may be an Accountant or General Manager. This person may also sign for gift card and terminal orders.
Manager: This person may call in transaction problems and view individual store transactions on the website.

Merchant Authorization

- Unless otherwise explicitly stated, all capitalized terms that are used but not defined in this Application have the meanings specified in the Agreement Terms and Conditions. This Agreement is between Worldpay Integrated Payments ("**Processor**", "**us**", "**our**" or "**we**"), the legal entity or sole proprietor identified on page 1 of this Application (the "**Merchant**", **"you" or "your"**), and the Member Bank named on page 1 of this Application ("**Member Bank**"). Member Bank is a member of Visa, U.S.A., Inc. ("**Visa**"), MasterCard International, Inc. ("**MasterCard**"), and Discover Financial Services, LLC ("**Discover**"). We are a registered independent sales organization of Visa, a member service provider of MasterCard and a registered acquirer for Discover.
- No modifications, alterations, or manual changes (including lining out fees, unless otherwise pre-approved and/or pre-designated by us) made to the Agreement will be effective unless we consent to them in a separate writing. This Agreement may be executed in counterparts. A scanned, facsimile, or duplicate copy of this Agreement executed by the parties shall be treated as an original.
- The undersigned individual **("Signer")** represents and warrants that Signer is authorized to sign on behalf of Merchant and to bind Merchant to the terms of this Agreement. By Signer's signature below on behalf of Merchant, Signer certifies that: (i) Merchant has received a full and complete copy of this Agreement, (iii) Signer has read, understands, and accepts all of the terms and conditions in this paragraph and elsewhere in the Agreement, and (iv) all information provided in this Application is true and accurate.
- You irrevocably authorize us to initiate Automated Clearing House ("**ACH**") debit and/or credit entries from and to the Designated Accounts for all fees, costs, and amounts due to us or payable to you pursuant to this Agreement and ACH rules and regulations. In the event that a credit or debit entry is erroneously initiated, you authorize us immediately to correct such error. This ACH Authorization shall remain in full force and effect until we have collected payment on all fees, costs, and amounts due or which may become due pursuant to this Agreement. The Designated Account(s) may not be changed or altered without thirty (30) days prior written notification to us and the execution of any forms or instruments deemed reasonably necessary by us.
- The acceptance and processing of Merchant Sales Drafts by Member Bank and/or us shall be deemed the consent and execution by us and Member Bank of the Agreement and furthermore shall evidence ours and Member Bank's receipt of and approval and agreement to this Application signed by you. If you do not want to participate in the American Express Program, the applicable Opt Out Box has been marked.
- By signing below, Signer(s), on behalf of the Merchant: (i) agree(s) to be bound by all of the provisions of the Agreement, including the choice of law, jurisdiction, and venue provisions contained in the Terms and Conditions, and (ii) acknowledge(s) Merchant is aware of and must comply with the Rules Summary, and Association Operating Regulations. Signer(s) individually authorize(s) us or our representative to: (i) investigate Signer and/or Merchant by utilizing a third-party credit reporting agency, (ii) share information provided in this Application with third parties for fraud and risk purposes, and (iii) conduct an initial and ongoing comprehensive credit inquiry and/or investigation. In the event we do not approve your application for Services, you authorize us to share any information you have provided in this Agreement with our strategic partners for the possible provision of substantially similar services.
- Point of Sale Authorization: You hereby authorize the below listed point of sale representatives access to sensitive merchant account information to manage and configure your point of sale system functionality and complete installation.
  Your authorized point of sale reseller is: CT Checkout Your authorized point of sale developer is: CT Checkout

You acknowledge receipt of the "**Merchant Processing Agreement**" also referred to as the "**Agreement**" which consists of this page and the three (3) preceding pages including the Rates and Fee Schedule (the "**Application**"), and any other applicable amendments, schedules, exhibits, and attachments, including the documents listed below which accompany this Application or are otherwise provided to you via http://info.vantiv.com/vipcontract.html. This Agreement between the parties supersedes all prior agreements or representations between the parties whether written or oral regarding the subject matter of the Agreement. You represent that you have read the Agreement, including the portions contained on the Worldpay agreement website (http://info.vantiv.com/vipcontract.html), and you understand its terms and agree to be bound by them (including terms that we add or amend from time to time without notice and in our sole discretion). Whether or not we have formally approved your application, your submission of a transaction for processing, whether to us, Member Bank, or our third-party providers, is an expression of your consent to the terms of the Agreement. You can request a copy of the Agreement at any time by contacting a Customer Service Representative at (866) 622-2390 or your Relationship Manager. If you disagree with any terms and conditions set forth in the Agreement, do not accept service or sign this Application.

- Terms and Conditions
- Addendum A – General Services Addendum
- Network Interchange Schedules (as applicable)
- Association and Network Fees Schedule
- Rules Summary
- Privacy Notice

SIGN HERE

Merchant Signatures (Owner / Authorized Signer):

☒ Name (printed): Title: Date:

Unlimited Personal Guaranty

In exchange for Processor's and Member Bank's acceptance of this Agreement, the person signing immediately below this paragraph (each a "**Guarantor**") is signing this Agreement as a Guarantor of the Merchant. By signing below, each Guarantor: (i) accepts and agrees to be bound by the Continuing Unlimited Guaranty provisions contained in Section 11 of the Terms and Conditions, and (ii) acknowledges and confirms that Guarantor received and read those Continuing Unlimited Guaranty provisions. The individual signing below authorizes us, Member Bank, and/or either of their representatives to conduct an initial and ongoing comprehensive credit inquiry and/or investigation of Guarantor by utilizing a third-party credit-reporting agency.

SIGN HERE

☒ , an individual Name (printed): Date:

Home Address (Physical Address Only – No PO Boxes)	Years at Address	Date of Birth	Phone Number

This Application must be returned to Worldpay on or before January 15, 2019

This General Services Addendum including all exhibits, schedules and supplemental addenda hereto and all documents and materials referenced herein ("Addendum A") will be an addendum to the Merchant Processing Agreement ("Agreement") between Processor, Member Bank and Merchant in accordance with the provisions as set forth in the Agreement. If there is a conflict in the terms or pricing provided in this Addendum A and the pricing or terms in any price schedule or amendment otherwise contained in the Agreement, the pricing or terms contained in the Agreement, without reference to this Addendum A, will control.

A. Services

1. Security Services.

a. Terms and Conditions.
(i) OmniShield – generically refers to Processor's multiple security and risk products and services that collectively are meant to help merchants address payment fraud, data security, compliance and financial loss risks. OmniShield products and services are available to purchase through one of the following packages:

- OmniShield Enterprise
- OmniShield Assure
- OmniShield CNP

(ii) Merchant Risks – refers to the four, major risk areas associated with accepting, transporting and storing cardholder data

- Fraud – The use of a lost, stolen or counterfeit payment card by an unauthorized user that may result in additional merchant liability
- Data Security – The ability to convert clear, PCI sensitive payment data into a surrogate, PCI non-sensitive value that if captured by an unauthorized user cannot be used to commit fraud against the original cardholder
- Compliance – The ability to handle PCI sensitive payment card data in alignment with appropriate network rules and PCI standards
- Financial Loss – The potential impact of a merchant failing to address Fraud, Data Security and/or Compliance requirements (e.g., fines, fees, remediation costs, law suites, etc.)

(iii) OmniShield Enterprise – A service offering, limited to PCI Level 1 and PCI Level 2 merchants that subsequently requires the merchant to individually select one or more of the following security and risk products and services:

- PCI Assist
- EMV Support Services
- Encryption
- Tokenization
- eProtect (eProtect requires Tokenization to also be enabled)

(iv) OmniShield Assure – A required service offering for PCI Level 4 merchants and is limited to PCI Level 4 merchants only and bundles together all the following security and risk products and services:

- PCI Assist
- Breach Assist
- EMV Support Services
- Encryption
- Tokenization

(v) OmniShield CNP – A required service offering for PCI Level 3 and other 100% Card Not Present PCI Level 4 merchants and is limited to PCI Level 3 merchants and other 100% Card Not Present PCI Level 4 merchants only, and bundles together all the following security and risk products and services:

- PCI Assist
- Breach Assist

Additionally, PCI Level 3 merchants and 100% Card Not Present PCI Level 4 merchants may also select and buy separately:

- Tokenization
- eProtect (eProtect requires Tokenization to also be enabled)

(vi) PCI Assist – PCI Assist is a set of streamlined online tools to help merchants achieve, maintain and track PCI compliance. PCI Assist helps clients review PCI DSS compliance requirements and complete their Self Assessment Questionnaire (SAQ) and, as recommended, conduct periodic vulnerability scans of their network. PCI Assist is required for SAQ merchants to report their compliance status to Processor.

(vii) Non-Validation Fee (NVF) / Non-Compliance Fee (NCF) – In alignment with Terms and Conditions section 2, Merchant is responsible for demonstrating compliance with PCI DSS programs. Failure to report compliance validation status or reporting a failed status to Processor will result in a NVF/NCF being assessed. Active merchants will have a 60-day grace period to validate and report compliance validation status. Merchant's compliance validation and reporting status will be evaluated monthly. This fee will only be assessed if the Merchant has failed to report the status or has reported a failed status and will not be assessed once Merchant meets compliance requirements.

(viii) EMV Support – Europay, MasterCard, and Visa ("EMV") is a set of global standards for credit, debit and contactless card payments. EMV chip cards help prevent in-store fraud and are nearly impossible to counterfeit. Starting October 1, 2015 merchants who have not made the investment in chip-enabled technology may be held liable for card-present fraud. EMV acceptance requires an EMV enabled standalone terminal or POS system. Processor is enabled to process in-store EMV transactions to help reduce fraud liability.

(ix) EMV Non-Enabled Fee - The EMV Non-Enabled Fee is applicable if Merchant does not have EMV enabled equipment and/or software. The EMV Non-Enabled Fee is determined based on the chargeback liability risk of Merchant's MCC as determined by Processor. Transactions will be evaluated monthly at the MID level and assessed at the chain level when applicable. This fee is based on the gross sales amount of each card present transaction.

(x) Breach Assist – In the event Merchant is enrolled in the Breach Assist Program ("BAP") offered by Processor through OmniShield or otherwise, the indemnification required by Merchant under this Agreement will only be reduced by amounts up to the limits set by the service provider that are actually recovered by Processor in connection with the BAP and only to the extent that such amounts are specifically related to a data breach involving solely Merchant. The limited indemnity waiver provided by the BAP will not cover all the costs associated with a data breach. The specific terms and conditions of the BAP are available for Merchant to review at www.RoyalGroupServices.com/breach-assist/ or by contacting a customer service representative at 1-800-393-1345.

(xi) Encryption – Encryption is a two-part service offering designed to: (i) encrypt (make unreadable) PCI sensitive payment data at the origin of the payment transaction and, (ii) decrypt payment data information at the destination of the transaction. Processor's service offering availability requires alignment between the encryption technology deployed within the Merchant's terminals and the decryption technology hosted by the service provider, which may require the use or upgrading of certain terminals and/or equipment or new message specifications (which will be at Merchant's sole expense) and may not be supported on all terminals/equipment.
Merchant acknowledges and agrees that encryption functionality is required and may require Merchant to license encryption technology from appropriate third party provider or authorized reseller and that said licensed functionality may incur fees in addition to those set forth herein. Merchant also acknowledges that provision of Processor's service offering to Merchant may require a corresponding decryption technology license and that Processor's service offering is subject to availability of required decryption license from applicable third party provider. Upon reasonable notice, Processor maintains the right to cease, modify or enhance providing the service offering without penalty and will use commercially reasonable efforts to offer a substitute service if applicable.
The value proposition associated with encrypting and decryption payment data (i.e., affects to Merchant's risk and compliance requirements) is affected by where the payment data is encrypted, the terminal type used for encryption, and the location where the payment data is decrypted. Processor has identified three different Encryption service offerings:

- Card Data Encryption – risk reduction, no scope reduction
- Point to Point Encryption – risk transference and scope reduction in alignment with PCI QSA evaluation
- Validated Point to Point Encryption – risk transference and scope reduction in alignment with PCI guidelines for PCI listed P2PE solutions

Point to Point Encryption assumes: (i) Payment data is encrypted within a PCI-PTS certified Secure Cryptographic Device (SCD), using a NIST defined strong encryption algorithm, with encryption keys that were generated and handled in alignment with X9 standards and (ii) Encrypted payment data is only decrypted by Processor within Processor's data systems.
Payment data information protected by the encryption service offering may include Track 1 or Track 2 data, obtained through a magnetic card swipe read, or PAN Data, obtained through manual entry directly into the SCD. The encryption service offering applies only to transactions that were encrypted and sent by the SCD to Processor's authorization and settlement systems pursuant to the Agreement. Supported transactions include, but may not be limited to, those associated with credit (signature), debit (signature) and debit (PIN).

(xii) eProtect – eProtect is a two part service designed to (i) capture payment data information from a given webpage using embedded Card Not Present eCommerce Data Security technology and, (ii) submitting the card data to a Processor hosted Card Not Present eCommerce Data Security server to exchange the card data for a Registration ID / Low Value Token before the data is transmitted back to the Merchant's eCommerce website. Merchant acknowledges and agrees that it will acquire said Card Not Present eCommerce Data Security functionality from the Processor and is responsible for all development effort necessary to embed said technology as appropriate within one or more Merchant web pages. Information protected by the Card Not Present eCommerce Data Security Service includes Primary Account Number (PAN) Data manually entered into any webpage that includes embedded Card Not Present eCommerce Data Security technology. The resulting Registration ID / Low Value Token must subsequently be submitted to the Processor's processing systems within a configurable timeframe to facilitate the exchange of the Registration ID / Low Value Token for a High Value, Multi-Use Tokenization (see Tokenization Service). Merchant acknowledges that provision of the Card Not Present eCommerce Data Security services to Merchant is subject to Merchant completing integration and certification efforts with Processor. Merchant acknowledges that eProtect will result in Merchant automatically being enrolled in

Processor's Tokenization service.

(xiii) Tokenization - Tokenization is a service in which cardholder PAN data, once received by the Processor, is replaced with a surrogate ("Token") value. Deliverables of the Tokenization service include; (1) the creation of tokens and (2) the recognition and use of a Processor issued pre-existing token to support all post authorization transactions with the Processor, which includes initiating a new authorization with a token value. Data necessary to convert tokens back to PAN data will be maintained in Processor's systems. Merchant access to the Tokenization service requires integrating and certifying systems to token services using Processor's appropriate message specification. Message specifications are limited to those that exist in Processor's current Service offering. The Parties agree that the scope of the Tokenization service does not include the certification or systematic configuration of third parties or firmware licensing as selected by the Merchant to support Tokenization services. The processor has identified the following types of Tokenization services.

- OmniTokens are tokens generated in such a way as to retain some of the digits of the original card value, be format preserving (i.e., length preserving and character set preserving), and be consistent across numerous requests (i.e., the same card value will result in the same token value in the context of a given merchant). OmniTokens are not limited to a specific platform and can be used interchangeably between processor's different platforms.
- mTokens are tokens generated in such a way as to be unique for each given transaction and format non-preserving. The link between a card value and an mToken is indirect in that the mToken references a given transaction, which in turn references a given card value. Note: mTokens are limited to transactions processed through processor's S1 platform only.
- eTokens are tokens generated in such a way as to be unique for each given transaction and format non-preserving. eTokens are used as an index value into processor's data vault, which subsequently stores the associated card value Note: eTokens are limited to transactions processed through processor's Express platform only.

Non-Standard, GUI and Batch Tokenization are separate and unique service offerings and respective fees will be quoted to Merchant for the use of each service.

- "Standard Tokenization" is provided on a per transaction basis in-line with each authorization request
- "Non-Standard Tokenization" is provided as separate "non-authorization" message to the Processor that results in a token being generated and returned outside of a purchase transaction
- "Graphical User Interface (GUI) Tokenization" is provided for Merchant operations personnel with appropriate credentials to convert or revert card values and tokens via Processor provided product interface(s).
- "Batch Tokenization" / "Batch Detokenization" is provided as a file based service to support the mass conversion of any existing store of cardholder data, and will mean the process of receiving a file that includes multiple values, performing the tokenization / detokenization process as appropriate for each value and returning a response file that includes the corresponding appropriate value.

Upon Tokenization services termination, Merchant will have 90 days to request, via written request to Processor, a Batch De-Tokenization of the Merchant's token store, located within the Merchant's systems. For purposes herein, Batch De-Tokenization will mean the process of the Processor receiving a file from Merchant that includes multiple token values, Processor performing the de-tokenization process for each token value and Processor returning a response file to Merchant that includes the corresponding card values for each token. After 90 days, Processor will no longer be responsible for maintaining the data necessary to De-Tokenize Merchant's token store or able to guarantee availability of data. Upon mutual agreement, Processor may offer the Merchant De-Tokenization Data Management Services under a separate agreement to support the token store after the termination of the current agreement supporting Tokenization services.

(xiv) Security Services – Merchant may utilize OmniShield products and services ("Security Services") in conjunction with services provided wholly or partially by a third party with the support and agreement of Processor. Merchant bears all risk and responsibility for conducting Merchant's own due diligence regarding the fitness of Security Services for a particular purpose and for determining compliance with the Bank Rules, the Operating Regulations, and the Laws. Accordingly, Merchant's use of Security Services is at Merchant's own risk. Processor's decision to offer Security Services will not limit Merchant's duties and obligations contained in this provision or the Agreement. Processor does not warrant or guaranty that use of the Security Services , in itself, will: (i) result in Merchant's compliance with Bank Rules, Operating Regulations, and/or Laws; (ii) prevent any and all unauthorized breaches of your terminals, systems or facilities; or, (iii) be uninterrupted or error-free. Merchant agrees that it will not acquire any interest in (ownership, intellectual property or otherwise) in any of the third party provider software used to provide the Security Services. Merchant will not, and will have no right to, own, copy, distribute, sub-lease, sub-license, assign or otherwise transfer any portion of such third-party provider software used to provide the Security Services or any materials provided by Processor or to modify, decompile, or reverse engineer any such software, materials, or the Services.

(xv) triPOS® Service - The triPOS® Service is a turnkey, EMV certified payment processing application designed to process transactions that is compatible with the Processor's processing platform and helps reduce the scope of Merchants' PCI-DSS with P2PE and tokenization technology.

b. Pricing

(i) OmniShield Enterprise (see below footnotes 1 and 2)	Quoted
(ii) OmniShield Assure (see below footnotes 1 and 3)	See application
(iii) OmniShield CNP (see below footnotes 3 and 4)	Quoted
(iv) PCI Assist (see below footnotes 1 and 5)	Quoted
(v) P2PE(see below footnote 1)	Quoted
(vi) eProtect (see below footnote 1)	Quoted
(vii) OmniToken™ (see below footnote 1)	Quoted
(viii) Vault™	See application
(ix) PCI Non-Validation Fee (see below footnote 6)	$19.95/MID/Month
(x) EMV Non-Enabled Fee	
Low Risk	0.05% of the gross sales per month
Moderate Risk	0.15% of the gross sales per month
High Risk	0.27% of the gross sales per month
(xi) triPOS™ Service	See application

Footnotes to above Section A.1(b).

1. Pricing provided as a separate attached quote or for level 4 merchants on the Merchant Application
2. Available only to PCI Level 1 and PCI Level 2 merchants
3. Required by and available only to PCI Levels 4 merchants.
4. Required by and available only to PCI Level 3 merchants and 100% Card Not Present PCI Level 4 merchants
5. Required by merchants using an PCI DSS SAQ
6. Assessed only if merchant fails compliance validation or fails to report compliance validation

2. Electronic Benefits Transfer ("EBT") Services.

The Financial Management Services ("FMS") of the U.S. Department of Treasury, and/or various of the EBT Program State(s)/Alliance(s), have entered into agreement(s) with third party processor(s) (collectively and individually, "Contractor") to manage the EBT Program(s) implemented by FMS and/or the EBT Program State(s)/Alliance(s).

Processor has entered into agreements with one or more Contractors (collectively and individually "Processor Agreement") which permit Processor to be an acquirer processor in certain of the EBT Programs.

Acquirer Services will mean the data processing systems and procedures provided by Processor to facilitate Merchant's participation in the EBT Program(s). In the event Merchant receives any of the Acquirer Services or otherwise participates in any of the EBT Programs, Merchant agrees to the following obligations which are in addition to Merchant's obligations in the Agreement and in addition to any other obligations in the Operating Rules relating to the EBT Program(s) and/or Acquirer Service(s), as they may be amended from time to time.

1. Merchant will be solely responsible for obtaining a copy of the then current Operating Rules for each EBT Program in which Merchant elects to participate from the applicable Contractor, EBT Program State/Alliance, FMS or Processor, no less than 30 days prior to the commencement of Merchant's participation in each such EBT Program. Merchant agrees to abide by and fully comply with the documentation as may be in effect from time to time, and to perform and fulfill any and all obligations and responsibilities, and discharge any and all duties and liabilities relating to Processor, Contractors or retailers to which it may be subject in accordance with such documentation or other rules or regulations adopted by Contractor(s), FMS or the EBT Program States/Alliances, or which may arise in any other manner or from any other source related to the Acquirer Services or the EBT Program(s).

2. Merchant will provide personnel, one of whom will be a management level technical interface person, to monitor, oversee and maintain its devices participation in the EBT Program(s). This personnel will also be responsible for monitoring Merchant's compliance with documentation, including but not limited to, each EBT Program's procedures and requirements applicable to Customer and its processor and for ensuring Merchant fulfills all of its responsibilities in connection with its participation in each EBT Program.

3. Processor will make available to Merchant activity files of its EBT Program transactions in a Processor format, unless similar information is provided by Processor through other services provided to Merchant.

4. Processor will not provide: (i) routing of activity files received from Contractor(s) to Merchant; or (ii) any other files or reports not specifically described above. Merchant will be responsible for, and agrees to pay Processor, all telecommunications fees, assessments and related expenses in connection with Processor establishing and maintaining a link with each Contractor in order to provide Acquirer Service to Merchant. Processor may allocate such fees, assessments and related expenses in such manner as it deems advisable in its sole discretion.

5. Merchant agrees to allow the auditors of Processor, Contractor(s), FMS or the EBT Program State(s)/Alliance(s), to review the files held and procedures followed, and inspect the facilities used, by Merchant in connection with the Acquirer Services or the EBT Program(s). Processor may be required to perform on-site inspections of Merchant's premises and Merchant agrees to be responsible for Processor's out-of-pocket expenses and its standard fees for the time spent by Processor's personnel (which will be assessed at Processor's then current Standard Hourly Rate) in conducting such on-site inspections.

6. Merchant agrees to immediately notify Processor and the applicable Contractor in writing of any changes in the goods and services for which EBT Program cards are accepted as payment from participants in the applicable EBT Program.

7. Merchant authorizes Processor to provide Contractor(s), FMS and/or the EBT Program State/Alliance with such information about Merchant, as requested or required according to the Processor Agreement(s), the Retailer Agreement(s), the Operating Rules or the other documentation, or as may be required to participate in the EBT Program(s).

8. Merchant agrees to take all steps necessary to settle with Processor for EBT Program transactions involving Merchant's terminals in accordance with Processor's standards and documentation; and Merchant will be responsible for making any necessary reconciliation or adjustments in accordance with the documentation. Processor will provide Merchant standard Processor reports for the services provided to Merchant. Merchant will always maintain an open checking account at a financial institution which Processor or its agent can access through the Federal Reserve's Automated Clearing House ("ACH") system. Merchant authorizes Processor and its agents to debit and/or credit the account to settle any and all amounts due under the Agreement and any Addenda including, but not limited to, processing fees and transaction settlement. Unless otherwise agreed to in writing by Processor, Merchant will be treated as one settlement endpoint with respect to all transactions processed by Processor using Acquirer Services. Merchant will always maintain the account with sufficient cleared funds to meet its obligations under this Agreement. In the event Merchant desires to change the account or the financial institution where the account is located, Merchant will give Processor at least 30 days prior written notice of any such change.

3. TransForm® Tokenization Services.

a. TransForm Tokenization. In addition to the terms of the Agreement, these TransForm Tokenization Service terms apply to Merchant's use of the Account Updater Service and TransForm Tokenization Service to store authorized customer billing information for recurring transactions and may be provided by Processor and one or more affiliates of Processor.

b. Definitions. The following terms when used in this Agreement will have the meanings set forth in this section:

i. "Account Updater Service" means a service provided through the Associations that enables Merchants to determine if a cardholder's account number has been updated by the cardholder's issuer, provided that the cardholder's issuer is a participant in the Account Updater program. The availability or functionality of the Account Updater Service may be modified by the Associations or Processor's acquiring bank upon notice to Merchant.

ii. "Authentication Data" means the full magnetic stripe data, the CVV2/CVC2/CID and the PIN or PIN block located on credit cards and debit cards.

iii. "PAD" means payment account data, including but not limited to credit and debit card account data, expiration month and year, cardholder name, checking account number, and customer bank routing information.

iv. "PAI" means Payment Account Identifier. PAI is a unique identifier that is assigned by Processor that references a payment account record.

v. "TransForm® Tokenization Service" means the Processor service designed to move Merchant's customer cardholder data offsite to Processor's PCI DSS compliant storage facility. Processor's servers create and then return a unique PAI to the Merchant's software application. Encryption is used to protect cardholder data while in transit. Using the PAI, Merchant can bill a card on file and/or schedule automatic payments, enabling the Merchant to securely process transactions from payment account records.

c. Pricing. The rate and fees set forth in the Application for TransForm Tokenization and Account Updater apply. Processor will charge Merchant the monthly fee set forth in the Application per MID for its use of the TransForm Tokenization Service.

i. TransForm Tokenization Service Storage Fees. Merchant agrees to pay Processor the TransForm Tokenization fixed monthly fee listed in the Application which, if not listed is $30.00, per MID provided that the total PAIs stored for such MID does not exceed the PAI Maximum per month (the "PAI Maximum") which such PAI Maximum is listed in the Application which, if not listed is 500. Should the total PAIs stored in any month for such MID exceed the PAI Maximum, Merchant agrees to pay the additional fee listed in the Application which, if not listed, is $0.09, per each PAI stored in such month for such MID in excess of the PAI Maximum.

ii. Account Updater Service Pricing. Merchant agrees to pay Processor the Account Updater setup fee, fixed monthly fee, and updater fee listed in the Application which amounts, if not listed in the Application, are respectively $99.00, $30.00, and $0.80. Merchant may terminate receipt of the Account Updater Service at any time upon 30 days prior written notice to Processor without further liability for the Account Updater Services other than for charges incurred but unpaid as of the effective date of such termination. Processor will charge Merchant the one-time set-up fee per Merchant identification number ("MID"), a fixed monthly charge per MID, and a charge per valid update for use of the Account Updater Service. The set-up fee is applied upon the start or re-start of Account Updater Service for each MID. A "valid update" is as an update in which a match for the cardholder's account number is made and either; (i) a new account number is provided, (ii) information that the account has been closed is provided, (iii) a new expiration date is provided, or (iv) a "contact cardholder" message has been provided.

d. Term. These TransForm Tokenization terms will run coterminous with the Merchant Processing Agreement. Processor may additionally terminate provision of the TransForm Tokenization Services on 30 days prior written notice to Merchant for any or no reason; or immediately (a) if Merchant is in material breach of its obligations under the Agreement, including these TranForm Tokenization terms, (b) in order to comply with applicable law or requests of governmental, administrative or judicial authorities, or (c) if Processor reasonably believes that continuing to provide the TransForm Tokenization Service to Merchant could create a substantial economic or technical burden or material security risk for Processor.

e. Access to Information After Termination. Upon termination of Merchant's use of the TransForm Tokenization Services and within five business days of agreement between the parties on the means of transfer and after Merchant's payment of the data retrieval fee based on the number of Merchant's stored records as set forth in the table below, Processor will provide a data file including all stored records to a PCI DSS compliant facility designated by Merchant. The data retrieval fee will be calculated cumulatively so that all stored records will be billed at the same lower fee per record once a higher volume tier is reached. Records may only be provided to a PCI DSS compliant facility with file format and encryption requirements to be determined in Processor's reasonable discretion.

STORED DATA	DATA RETRIEVAL FEE
1 - 5,000 PAI's	$2,000 (minimum data retrieval fee)
5001 - 250,000 PAI's	$0.40 per stored record
250,001 - 500,000 PAI's	$0.35 per stored record
500,001 - 750,000 PAI's	$0.25 per stored record
750,001+ PAI's	$0.20 per stored record

f. Communication Methods. Merchant will establish and maintain secure data communication connections and will transmit data to Processor in the format required by Processor.

g. Use of TransForm Tokenization. Merchant will immediately update PAD upon additions, deletions, and changes to the underlying data. Merchant will create, delete, and query payment account records in accordance with instructions provided by Processor.

h. Use of Account Updater. Merchant must have an existing relationship with the cardholder in order to make an inquiry using the Account Updater Service and hereby agrees to comply with the Merchant requirements of the Account Updater terms of use as set forth in the Operating Regulations. The Account Updater Service may not interface with third party software or third party services, if Merchant uses third party software or a third party service to process recurring transactions then Merchant understands and agrees that Merchant may be required to make manual updates to recurring transaction information based on Account Updater Service updates.

i. Disclaimer of Warranties. The TransForm® Tokenization Service is being provided to Merchant by Processor "as-is" and without any warranty of any kind. Processor disclaims any express or implied warranty, including but not limited to implied warranties of merchantability, non-infringement, or fitness for a particular purpose.

j. Indemnification. In addition to the indemnification obligations of Merchant under the Terms and Conditions to the Agreement, Merchant agrees to indemnify, defend and hold harmless Member Bank and Processor, its employees, officers, agents, shareholders, representatives and directors from any and all fines, penalties, losses, claims, expenses (including attorney fees and the allocable costs of in-house counsel), or other liabilities resulting from or in connection with; (i) Merchant's use of the TransForm Tokenization Service, (ii) Merchant's storage of any cardholder data, or (iii) Merchant's breach of the herein TransForm Tokenization terms.

k. Limitation of Liability. In addition to Processor's limits of liability set forth under the Terms and Conditions to the Agreement, under no circumstances will Processor be liable to Merchant or any third party for any indirect, special, incidental, consequential, punitive, exemplary or multiple damages arising out of or related to Processor's provision of the TransForm Tokenization Service hereunder, regardless of the legal theory on which such claim is based (whether based in contract, tort, warranty, strict liability, negligence, or any other legal theory), even if Processor has been advised, knew, or should have known of the possibility of such damages (which include, but are not limited to, loss of profits, revenue, savings, software, data or goodwill, the claims of third parties, and/or injury to persons or property). The parties expressly agree that the total liability of Processor (including, without limitation, for Processor's performance or the failure of such performance hereunder, or for any breach hereof) will be exclusively limited to an amount equal to the aggregate TransForm Tokenization service fees actually received by Processor from Merchant during the one month period ending on the date on which the event giving rise to the claim for damages occurred. Merchant accepts the restrictions on its right to recover additional damages as part of its bargain with Processor, and Merchant understands and acknowledges that, without such restrictions, the consideration for the services provided hereunder would be higher.

4. **Chargeback Service Fee**.

The below tiered Chargeback Service Fee shall apply to Merchant. Beginning on the Effective Date the Chargeback Service Fee will be charged monthly per MID at the below Tier 1 amount and thereafter, on a semi-annual basis, which first such semi-annual period may be less than six (6) months, Merchant's highest annual number of chargebacks within the term of the Agreement, shall determine the applicable monthly fee tier assessed. In the event Merchant has twenty-six (26) or more chargebacks in any annual period, thereafter Merchant will be charged $25.00 per chargeback, in lieu of a monthly fee. If Merchant has less than twelve (12) months of transaction history with Processor, Merchant's actual number of chargebacks will be annualized in the above semi-annual reviews to determine the below applicable tier. Notwithstanding the foregoing, if Processor at any time, in its reasonable discretion, believes that Merchant will have twenty-six (26) or more chargebacks in any annual period, upon notice to Merchant, Processor may charge Merchant a fee of $25.00 per chargeback, in lieu of a monthly fee.

Tier	Annual Number of Chargebacks	Monthly Fee
1	0	$7.50
2	1-2	$10.00
3	3-4	$15.00
4	5-8	$20.00
5	9-12	$25.00
6	13-17	$30.00
7	18-21	$35.00
8	22-25	$40.00

5. Additional Services or Expenses.

Merchant agrees that Processor may charge Merchant for any non-specified service it provides Merchant ("Additional Service") or expense it incurs on behalf of Merchant ("Additional Expense") any time after Merchant's initial receipt of the same, and Merchant agrees to pay for such service (at Processor's standard fees in effect from time to time) or expense in accordance with this Agreement. Merchant acknowledges and agrees that it will notify Processor in writing and in accordance with the notice provisions of the Agreement in the event Merchant does not want the Additional Service and that such written notice will be sent to and actually received by Processor within 90 days of Merchant's first receipt of the Additional Service ("Additional Service Cancellation"). Merchant will not dispute, and will be unconditionally obligated to pay for, any Additional Service fees for which Merchant has not provided and Processor has not actually received an Additional Service Cancellation in accordance with the foregoing and any Additional Expense.

6. Store and Forward Service.

The Store and Forward service is a secondary, offline option of credit card acceptance enabled typically in the event of internet connectivity down-time. Store and Forward may be applicable as a temporary solution for businesses needing to accept payments in environments without access to the internet, such as trade shows or farmer's markets. Optionally, businesses sometimes elect to process offline transactions with a working internet during times of peak business demand. When Store and Forward is enabled, it allows merchants to store transactions offline until either internet connectivity has been restored or the business need subsides. Offline transactions are then forwarded to Processor for a valid card issuer authorization. From the cardholder's perspective, the transaction flow is unchanged, yet the important distinction for the merchant is that the transaction is not authorized in real time and may in fact decline when forwarded. Where there are benefits to this functionality in maintaining transaction up-time especially during times of internet uncertainty, there are also risks and an assumption of liability by you which need to be carefully considered as set forth below in this section. You understand and agree that use of the Store and Forward Services is dependent on the point of sale system configuration and capabilities for the processing of such service transactions which you are solely responsible. Further, with regard to the Store and Forward services, it is important that you and your point of sale service providers and integrated software vendors understand and agree that there are inherent risks when not obtaining an authorization at the time of the transaction and those risks, between you and us, rest solely on you. Transactions processed via Store and Forward are high risk and may be declined, error out, or otherwise fail to process when forwarded to us. When enabling Store and Forward, you accept full liability for all transactions, whether or not an authorization approval code is received, including loss of revenue due to declined or failed transactions, chargebacks, and losses, fees, fines, and penalties related to transactions processed via the Store and Forward application. Further, we are not liable to you in the event the transaction data is not stored within the point of sale device for any reason. We make no warranty, expressed or implied, with respect to servicing, processing, or acceptance of Store and Forward transactions and you assume all liability when using or otherwise accepting to process in a Store and Forward/offline manner.

7. FastAccess™ Funding Service.

a. FastAccess™ Funding Program Services. The FastAccess funding program provides accelerated funding of Merchant's card transactions, typically between two and five hours after settlement of Merchant's credit and debit card transactions, by way of Original Credit Transaction ("OCT") through VisaNet or Maestro which permits Processor through Member Bank to initiate credits to a designated Visa or MasterCard debit card account that Merchant will be requested to provide (the "FastAccess Services"). Prior to using the FastAccess Services Merchant must provide Processor a debit card account in a PCI compliant manner. The debit card account designated by Merchant must be a U.S. issued debit card with an institution that is enabled for OCT transactions. Merchant authorizes Processor to initiate a zero dollar authorization to such account as part of the establishment of Merchant's use of the FastAccess Services.

b. Pricing. The fee for the FastAccess Services is listed on the Merchant Application and charged on a per occurrence/deposit basis. If no fee is listed on the Merchant Application then Merchant will be charged Processor's then standard rate for the use of the FastAccess Services.

c. FastAccess Services Terms, Conditions and Limits. The FastAccess Services are part of the Services under the Merchant Processing Agreement and subject to the terms and conditions of Merchant's use of Services under the Merchant Processing Agreement as well as the terms, restrictions, and condition in this Addendum A which include those listed below:

i. Limits. The per transaction limit applicable to the FastAccess Services is $15,000.00. Daily limits also apply.

ii. Limitations on Availability of FastAccess Service. FastAccess Services is not supported by all Card issuers.

iii. Changes to or Removal of Attributes, Requirements, and Functionality. Visa, Maestro, and Processor may at any time change or remove any of the attributes, requirements, and functional specifications related to the OCT and FastAccess funding program or withdraw such services entirely.

iv. Default Settlement and Suspension of Service. Transactions that do not meet the requirements, exceed the limits, or are otherwise not settled via the FastAccess Services shall route your settlement via the normal ACH Card transaction settlement solution under the Services. The trigger of certain limits or limitations may suspend the use of the FastAccess Services.

d. Disclaimer and Limitation of Liability. Merchant understands and agrees that the disclaimer of warranties and limitation of liabilities applicable to Processor and Member Bank set forth under the Merchant Processing Agreement apply to the herein FastAccess Services and neither Processor nor Member Bank shall be liable to Merchant for any loss, delay, error, interruptions or damage of any kind or character, whether direct, indirect or consequential, resulting from the use, delay, inoperability, or other failure of the FastAccess Services.