SCHEDULE J

TRANSARMOR[SM] SERVICE

The TransArmor[SM] service ("TransArmor Service" as defined below) is provided to CUSTOMER by PROVIDER and not Bank. Bank is not a party to this Schedule J insofar as it applies to the TransArmor Service, and Bank is not liable to CUSTOMER in any way with respect to such services. For the purposes of this Schedule J, the words "we", "our" and "us" refer only to the PROVIDER and not the Bank.

The TransArmor Service provided, transactions processed and other matters contemplated under this Schedule J are subject to the MSA, as applicable, except to the extent the terms of this Schedule J directly conflict with another provision the MSA, in which case the terms of this Schedule J will control.

1. Definitions. Capitalized terms used and defined herein shall have the meanings given to such terms as set forth in this Schedule J. If not defined herein, capitalized terms shall have the meanings given to such terms in the MSA.

"Legacy Data Conversion" means that process by which historical information containing primary account Numbers (PAN) from transactions completed by CUSTOMER prior to implementation of TransArmor will be converted to information containing a Token.

"Registered PAN" is defined as the processing of creating a CUSTOMER specific Token for a PAN.

Multi-Pay Token" shall mean CUSTOMER's specific alpha-numeric value that is: (i) randomly generated when a Card number is requested to be registered by CUSTOMER as CUSTOMER's specific Token upon receipt of Cardholder approval to register the Card number; (ii) becomes associated with CUSTOMER and the Card within PROVIDER and its Affiliates' systems; (iii) can be stored by CUSTOMER in CUSTOMER's systems in lieu of the Card number to represent the Card number; (iv) can be used to initiate a Transaction submitted by CUSTOMER that registered the Token for authorization processing for Cardholder initiated or recurring payments; (v) may be retrieved by CUSTOMER or its Affiliates within their systems in connection with processing future Transactions involving the same Card number or Registered Token when submitted by CUSTOMER for authorization processing; and (vi) is returned to CUSTOMER from PROVIDER or its Affiliates' systems as part of the Register PAN response and/or authorization response.

"Token" means an alpha-numeric value that: (i) is randomly generated when a Card number used in a Transaction is initially submitted by CUSTOMER for authorization processing; (ii) becomes associated with the Card within PROVIDER and its Affiliates' systems; (iii) may not be retrieved by PROVIDER or its Affiliates within their systems in connection with processing future Transactions involving the same Card number when submitted by CUSTOMER for authorization processing; and (iv) is returned to CUSTOMER from PROVIDER or its Affiliates' systems as part of the authorization response.

"Token Request" shall mean CUSTOMER's ability to obtain a Multi-Pay Token for credit card information only without an immediate authorization required which permits CUSTOMER to store a Multi-Pay Token for future transactions involving its customer.

"TransArmor Service" means those services described in Section 3 and may be either TransArmor VeriFone Edition Service or TransArmor Base Service as selected by CUSTOMER in Section 3.

2. Grant of License. PROVIDER grants to CUSTOMER a non-transferable, non-assignable, non-exclusive, revocable sub-license during the term of this Schedule J to use the TransArmor Service and the TransArmor Service Marks in accordance with this Schedule J, including without limitation the TransArmor Rules and Procedures as set forth in Section 4 below. Any rights with respect to the TransArmor Service not expressly granted by PROVIDER in this Schedule J are deemed withheld.

3. Services. The TransArmor Service applies only to Card transactions sent from CUSTOMER to PROVIDER for authorization and interchange settlement pursuant to the MSA, and specifically excludes electronic check transactions, STAR contactless transactions read in contactless mode, Wright Express Transactions, Voyager Transactions, and other Card types that are not capable of being Tokenized. PROVIDER and CUSTOMER may agree to include additional transaction types in the TransArmor Service when made available by PROVIDER. PROVIDER will provide an encryption key or other encryption capability to CUSTOMER to be used to encrypt (make unreadable) Card data during transport of the authorization request from CUSTOMER's point of sale to PROVIDER's systems. During the period when the transaction is being transmitted to PROVIDER for authorization processing, all historical transaction data, including card number and full magnetic stripe data (track data and expiration date), will be encrypted. PROVIDER will then generate or retrieve a unique, randomly generated Token or Multi-Pay Token assigned to the Card number that will be returned to CUSTOMER in the authorization response. CUSTOMER must select one of the two options for the TransArmor Service:

- TransArmor VeriFone Edition. This service option is limited to those CUSTOMERS which have an eligible VeriFone point of sale ("POS") devices and desire the software or hardware based encryption and tokenization to be activated through the VeriFone device.

- TransArmor Base Service. This service option provides software based encryption and tokenization that is available to all Customers to integrate into their POS or the point of sale device, if available.

4. Responsibilities of CUSTOMER. CUSTOMER is responsible to comply with the following regarding CUSTOMER's use of the TransArmor Service:

a. CUSTOMER is required to comply with the Association Rules, including taking all steps required to comply with the Payment Card Industry Data Security Standards (PCI DSS). CUSTOMER must ensure that all third parties and software use by CUSTOMER in connection with CUSTOMER'S payment card processing are compliant with PCI DSS. Use of the TransArmor Service will not, on its own, cause CUSTOMER to be compliant or eliminate CUSTOMER'S obligation to comply with PCI DSS or any other Association Rule. CUSTOMER must demonstrate and maintain current PCI DSS compliance certification. Compliance must be validated either by a Qualified Security Assessor (QSA) with corresponding Report on Compliance (ROC) or by successful completion of the applicable PCI DSS Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC), and if applicable to CUSTOMER's business, ensure passing quarterly network scans performed by an Approved Scan Vendor, all in accordance with Association Rules and PCI DSS.

b. Use of the TransArmor Service is not a guarantee against an unauthorized breach of CUSTOMER's point of sale systems or any facility where CUSTOMER processes and/or stores transaction data (collectively, "CUSTOMER Systems").

c. CUSTOMER must deploy the TransArmor Service (including implementing any upgrades to such service within a commercially reasonable period of time after receipt of such upgrades) throughout CUSTOMER's Systems including replacing existing Card numbers on CUSTOMER's Systems with Tokens or Multi-Pay Tokens, as applicable. Full Card numbers must never be retained, whether in electronic form or hard copy.

d. CUSTOMER must use the Token or Multi-Pay Token, as applicable, in lieu of the Card number for ALL activities subsequent to receipt of the authorization response associated with the transaction, including without limitation, settlement processing, retrieval processing, chargeback and adjustment processing and transaction reviews.

e. Any point of sale device, gateway and/or value-added reseller used by CUSTOMER in connection with the TransArmor Service must be certified by PROVIDER for use with the TransArmor Service.

f. If CUSTOMER sends or receives batch files containing completed Card transaction information to/from PROVIDER, CUSTOMER must utilize the service provided by PROVIDER to enable such files to contain only Tokens or Multi-Pay Tokens, as applicable, or truncated information.

g. CUSTOMER must utilize truncated report viewing and data extract creation within reporting tools provided by PROVIDER.

h. CUSTOMER is required to follow rules or procedures we may provide to CUSTOMER from time to time related to CUSTOMER's use of the TransArmor Service ("TransArmor Rules and Procedures"). We will provide CUSTOMER with thirty (30) days advance written notice of any such rules or procedures and any changes to such rules or procedures.

i. CUSTOMER has no right, title or interest in or to the TransArmor Service, any related software, materials or documentation, or any derivative works thereof, and nothing in this Schedule J assigns or transfers any such right, title or interest to CUSTOMER. CUSTOMER shall not take any action inconsistent with the stated title and ownership in this Schedule J. CUSTOMER will not file any action, in any forum that challenges the ownership of the TransArmor Service, any related software, materials or documentation. Failure to comply with this provision will constitute a material breach of this Schedule J. We have the right to immediately terminate this Schedule J and CUSTOMER's access to and use of the TransArmor Service in the event of a challenge by CUSTOMER. No additional rights are granted by implication, estoppel or otherwise.

j. CUSTOMER will not: (i) distribute, lease, license, sublicense or otherwise disseminate the TransArmor Service or any portion of it to any third party; (ii) modify, enhance, translate, supplement, create derivative works from, reverse engineer, decompile or otherwise reduce to human-readable form the TransArmor Service or any portion of it; or (iii) sell, license or otherwise distribute the TransArmor Service or any portion of it; (iv) make any copies, or permit any copying, of the TransArmor Service or any portion of it; or (v) use any portion of the TransArmor Service as a standalone program or in any way independently from the TransArmor Service. If any portion of the TransArmor Service contains any copyright notice or any other legend denoting the proprietary interest of PROVIDER or any third party, CUSTOMER will not remove, alter, modify, relocate or erase such notice or legend on such item.

k. CUSTOMER will only use the TransArmor Service for CUSTOMER's internal business purposes in a manner consistent with this Agreement.

l. CUSTOMER will use only unaltered version(s) of the TransArmor Service and will not use, operate or combine the TransArmor Service or any related software, materials or documentation, or any derivative works thereof with other products, materials or services in a manner inconsistent with the uses contemplated in this Schedule J.

m. CUSTOMER will promptly notify PROVIDER of a breach of any terms of this Schedule J.

n. CUSTOMER must obtain a Cardholder's written or electronic consent to store a Multi-Pay Token to represent such Cardholder's Card number for future purchases.

o. CUSTOMER must store the Multi-Pay Token in its CUSTOMER systems in lieu of the Card number for all Cardholder profile records.

p. CUSTOMER must require Cardholders to log into their Cardholder profile in order to initiate a Transaction with the Registered Token. This login must require two factors authentication, such as a User ID and password.

q. If CUSTOMER ceases a processing relationship, then CUSTOMER must permanently delete all Tokens or Multi-Pay Tokens, as applicable, contemplated under this Schedule J from all CUSTOMER systems no later than ninety (90) days after the termination or expiration of the processing relationship.

5. Term; Amendment; Termination. The TransArmor Service being provided under this Schedule J is coterminous with the MSA.

Unless prohibited by applicable law, PROVIDER may modify this Schedule J by providing written notice of such modifications to CUSTOMER. CUSTOMER may choose not to accept the requirements of any such modifications by notifying PROVIDER in writing within thirty (30) days after receiving such notice that CUSTOMER is terminating the TransArmor Service provided under this Schedule J.

In addition to any termination rights in the MSA, PROVIDER may terminate this Schedule J immediately if CUSTOMER'S material breach of the terms contained in this Schedule J remains uncured for ten days following CUSTOMER's receipt of written notice of such breach from PROVIDER.

6. Fees. Customer will pay for all fees as set forth in Schedule C of the MSA.

7. TransArmor Limited Warranty. PROVIDER warrants that the Token or Multi-Pay Token, as applicable, returned to CUSTOMER, as a result of using the TransArmor Service, cannot be used to initiate a financial sale transaction by an unauthorized entity/person outside the CUSTOMER Systems. This warranty by PROVIDER is referred to herein as the "Limited Warranty" and is subject to the terms and conditions set forth in this Schedule J. To be eligible for the Limited Warranty, CUSTOMER must maintain a processing relationship with PROVIDER and be in compliance with all the terms of the MSA, including this Schedule J, and any other agreement relating to Transaction Cards eligible for the TransArmor Service; provided that such compliance by CUSTOMER directly or indirectly impacts the security of the Tokens or Multi-Pay Tokens, as applicable. Subject to the terms, conditions and limitations set forth in the MSA, including the limitation of liability provisions, PROVIDER agrees to indemnify and hold CUSTOMER harmless from direct damages, including third party claims, resulting from PROVIDER's breach of the Limited Warranty. The express remedy for PROVIDER's breach of the Limited Warranty set forth in this paragraph constitutes PROVIDER's entire liability and CUSTOMER's sole and exclusive remedy for PROVIDER's breach of the Limited Warranty. The Limited Warranty is void if (i) CUSTOMER uses the TransArmor Service in a manner not contemplated by, or in violation of, the MSA, including this Schedule J, or any other agreement relating to Transaction Cards eligible for the TransArmor Service or (ii) CUSTOMER is grossly negligent or engages in intentional misconduct.

8. TransArmor Disclaimer. IN ADDITION TO THE DISCLAIMERS SET FORTH IN THE AGREEMENT, THE FOLLOWING DISCLAIMER APPLIES TO THE TRANSARMOR SERVICE: EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION, PROVIDER MAKES NO REPRESENTATIONS, WARRANTIES OR COVENANTS, EXPRESS OR IMPLIED WITH REGARD TO THE TRANSARMOR SERVICE INCLUDING THE UNINTERRUPTED OR ERROR-FREE OPERATION OF THE TRANSARMOR SERVICE OR NONINFRINGEMENT.