Schedule 3

TransArmor Service Schedule

This Schedule adds the TransArmor Service Schedule to the Payment Solutions Agreement (**Agreement**) between First Data and Company. The terms of the Agreement and this Schedule apply to the TransArmor Service, but if anything in this Schedule conflicts with the Agreement, this Schedule will control. The TransArmor Service is a Service under the Agreement and is provided by First Data and not by Bank. Bank is not a party to this Schedule and is not liable to Company in connection with the Service or this Schedule.

Capitalized words or phrases not defined in this Schedule use the definitions given to them in the Agreement.

24 TransArmor Services

24.1 First Data will provide the Company with an encryption key or other encryption capability that will encrypt (make unreadable) Card data when submitting an authorization request from the Company's point of sale terminals to First Data's systems. During the period when the transaction is being transmitted to First Data for authorization processing, sensitive track data, EMV tag equivalent track data, or Card number will be encrypted. First Data will then generate a Token or retrieve a Multi-Pay Token assigned to the Card number and return the Token or Multi-Pay Token to the Company in the authorization response. These encryption and tokenization services are the **TransArmor Services**. A **Token** is an alpha-numeric value that: (1) is randomly generated when a Card number is initially submitted by the Company for authorization processing; (2) becomes associated with the Card within First Data's systems; and (3) may not be retrieved by First Data within its systems in connection with processing future transactions involving the same Card number when submitted by the Company for authorization processing. A **Multi-Pay Token** is a specific alpha-numeric value that is: (a) randomly generated when a Card number is requested to be registered by the Company as the Company's specific Token upon receipt of Cardholder approval to register the Card number; (b) becomes associated with the Company and the Card within First Data's systems; (c) can be stored by the Company in the Company's systems in lieu of the Card number; (d) can be used to initiate a transaction submitted by the Company that registered the Token for authorization processing for Cardholder initiated or recurring payments; (e) may be retrieved by the Company within its systems in connection with processing future Transactions involving the same Card number or Registered Token when submitted by the Company for authorization processing; and (f) is returned to the Company from First Data's systems as part of the Register Token response and/or authorization response. As an option to assist Company with PCI Scope Reduction, Company may elect to subscribe to First Data's PCI Council validated Point to Point Encryption listed solution (**TransArmor P2PE**) that provides encryption of Card data.

24.2 The TransArmor Service applies only to Card transactions sent from the Company to First Data for authorization and interchange settlement pursuant to the Agreement, and specifically excludes electronic check transactions and other Card types that are not capable of being Tokenized. First Data and the Company may agree to include additional transaction types in the TransArmor Service when made available by First Data. If the Company enters Card data into a point of sale device that does not support the TransArmor Service, this Card data will not be encrypted during the period when the transaction is being transmitted to First Data for authorization processing and the Company assumes all risk associated with its transmission if Card data is stolen during transmittal to First Data's systems.

24.3 The TransArmor Services described in this Schedule are provided by First Data and not the Bank. The Bank has no performance obligations or liabilities to the Company in connection with the TransArmor Services.

25 PCI DSS Limitations

25.1 Use of the TransArmor Service will not, on its own, cause the Company to be compliant with, or eliminate the Company's obligation to comply with PCI DSS or any other Network Rules. The Company must demonstrate and maintain a current PCI DSS compliance certification. The Company's 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 Company's business, passing quarterly network scans performed by an Approved Scan Vendor. Company must successfully meet the above requirements to obtain PCI DSS compliance validation; provided, however, Company is not required to perform quarterly network scans, if Company uses a validated P2PE solution (e.g., TransArmor P2PE) in accordance with the P2PE Instruction Manual accompanying the validated P2PE solution.

25.2 Use of the TransArmor Service is not a guarantee against an unauthorized breach of Company's point of sale systems or any facility where the Company processes or stores transaction data (together, **Company Systems**).

26 Intellectual Property

First Data reserves all right, title, interest, or license (express or implied) to the TransArmor Services, Token, Multi-Pay Token, or associated intellectual property that it provides to the Company in connection with the TransArmor Services. Except as allowed under this Agreement, Company will not otherwise use, reverse engineer, decompile, distribute, lease, sublicense, sell, modify, copy or create derivative works from the TransArmor Services, Token, Multi-Pay Token, TransArmor P2PE solution or associated intellectual property.

27 TransArmor Limited Warranty

Subject to the terms of this Schedule, First Data warrants that the Token or Multi-Pay Token, as applicable, returned to the Company as a result of using the TransArmor Service cannot be used to initiate a financial sale transaction by an unauthorized entity or person outside the Company Systems. This warranty is the **TransArmor Limited Warranty**. To be eligible for the TransArmor Limited Warranty, the Company must maintain a processing relationship with First Data and be in compliance with all the terms of the Agreement, this Schedule, and any other agreements relating to Cards that are eligible for the TransArmor Service that impact the security of Tokens or Multi-Pay Tokens. Subject to the Agreement's terms, including its limitations of liability, First Data will indemnify the Company for direct damages, including third party claims, resulting from First Data's breach of the TransArmor Limited Warranty; which is (1) the Company's express and sole remedy for First Data's breach of the TransArmor Limited Warranty, and (2) First Data's entire liability for its breach of the TransArmor Limited Warranty. The TransArmor Limited Warranty is void if (1) the Company uses the TransArmor Service in a manner not contemplated by, or in violation of, the Agreement, this Schedule, or any other agreement relating to Cards that are eligible for the TransArmor Service; or (2) the Company is grossly negligent or engages in intentional misconduct.

28 Fees

The Company will pay First Data the fees described below (**TransArmor Fees**) for the TransArmor Services. The TransArmor Fees are in addition to the other fees charged to process the Company's transactions under the Agreement.

TransArmor Fees	Amount	Driver
TransArmor Transaction Fee	$_____	per transaction
TransArmor P2PE Transaction Fee	$_____	per transaction
Multi-Pay Token Registration Fee	$_____	per request
Registered PAN[1] Fee	$_____	per request
Legacy Data Conversion[2] Fee	$_____	per record converted

[1] A **Registered PAN** is the process of providing a Card's primary account number for a Company specific Token.

[2] **Legacy Data Conversion** is the process by which the Company's historical information containing Card primary account numbers prior to implementation of TransArmor will be delivered to First Data by the Company and converted to information containing a Multi-Pay Token.

29 TransArmor Rules and Procedures

29.1 The Company must ensure that all third parties and software used by the Company in connection with the Company's payment card processing are compliant with PCI DSS.

29.2 The Company 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 the Company's Systems including replacing existing Card numbers on the Company's Systems with Tokens or Multi-Pay Tokens, as applicable. Full Card numbers must never be retained, whether in electronic form or hard copy.

29.3 The Company 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 settlement processing, retrieval processing, chargeback and adjustment processing, and transaction reviews.

29.4 Any point of sale device, gateway, or value-added reseller used by the Company in connection with the TransArmor Service must be certified by First Data for use with the TransArmor Service.

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

29.6 The Company must utilize truncated report viewing and data extract creation within reporting tools provided by First Data.

29.7 The Company will only use the TransArmor Service for the Company's internal business purposes in a manner consistent with the Agreement and this Schedule.

29.8 The Company 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.

29.9 Company must maintain compliance with Network Rules and PCI Council requirements when storing a Multi-Pay Token in place of a Cardholder's Card number and require authentication for Cardholders to initiate a Transaction with the Multi-Pay Token.

29.10 The Company must store the Multi-Pay Token in the Company Systems in lieu of the Card number for all Cardholder profile records.

29.11 If the Company ends its processing relationship with First Data, the Company must permanently delete all Tokens or Multi-Pay Tokens, as applicable, from all Company Systems within 90 days after termination or expiration of the processing relationship.

29.12 Company use of the TransArmor P2PE Solution must comply with (a) First Data's requirements outlined in the P2PE Implementation Manual (**PIM**) and (b) PCI Council requirements in Company's use of the TransArmor P2PE service for Company Systems to be P2PE validated, including but not limited to Company's use of First Data's approved validated key injection facilities. Additionally, Company is also responsible to keep track of all points of interaction (POI)for the following states: (1) in secure storage awaiting deployment, (2) deployed/in service, (3) disabled/out for repair, (4) decommissioned and returned for secure destruction and (5) in transit; and to regularly manage Company Systems inventory at the minimum of once per year to maintain P2PE validation.

29.13 First Data may refer to Company as a TransArmor Service customer by name, trademark, trade name, logo or other symbol in its publicly distributed releases or materials, including customer lists (which may be published on a website). Upon First Data's request, Company will respond to inquiries from prospective customers about Company's experience with the TransArmor Service.