Schedule I
TransArmor Service and TransArmor P2PE Schedule

This TransArmor Service and TransArmor P2PE Service Schedule (**Schedule**) is attached to and subject to the terms of the Payment Solutions Agreement (**Agreement**) dated December 20, 2021 between SunTrust Merchant Services, LLC (**STMS**), Truist Bank (**Bank**), and South Carolina Treasurer (**STO**). The Services provided in this Schedule are provided by STMS and not Bank and Bank shall have no liability in connection with this Schedule. All capitalized terms in this Schedule shall have the same meaning as defined in the Agreement. In the event of a conflict between the Agreement and this Schedule, the terms of this Schedule will control except that the State Terms and Conditions incorporated into the Agreement shall control over the Schedule.

1 TransArmor Services

1.1 STMS will provide PARTICIPANT with an encryption key or other encryption capability that will encrypt (make unreadable) Card data when submitting an authorization request from PARTICIPANT's point of sale terminals to STMS's systems. During the period when the transaction is being transmitted to STMS for authorization processing, Card number and full magnetic stripe data (track data and expiration date), will be encrypted. STMS 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 PARTICIPANT 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 PARTICIPANT for authorization processing; (2) becomes associated with the Card withinSTMS's systems; and (3) may not be retrieved by STMS within its systems in connection with processing future transactions involving the same Card number when submitted by PARTICIPANT 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 PARTICIPANT as PARTICIPANT's specific Token upon receipt of Cardholder approval to register the Card number; (b) becomes associated with PARTICIPANT and the Card within STMS's systems; (c) can be stored by PARTICIPANT in PARTICIPANT's systems in lieu of the Card number; (d) can be used to initiate a transaction submitted by PARTICIPANT that registered the Token for authorization processing for Cardholder initiated or recurring payments;
(e) may be retrieved by PARTICIPANT within its systems in connection with processing future Transactions involving the same Card number or Registered Token when submitted by PARTICIPANT for authorization processing; and (f) is returned to PARTICIPANT from STMS's systems as part of the Register PAN response and/or authorization response. A Registered PAN is the processing of creating a Client specific Token for a Primary Account Number (**PAN**). As an option to assist PARTICIPANT with PCI Scope Reduction, PARTICIPANT may elect to subscribe to STMS's PCI Council validated Point to Point Encryption listed solution (**TransArmor P2PE**) that provides encryption of Card data.

1.2 The TransArmor Service applies only to Card transactions sent from PARTICIPANT to STMS for authorization and interchange settlement pursuant to the Agreement, and specifically excludes electronic check transactions, STAR contactless transactions read in contactless mode, and other Card types that are not capable of being Tokenized. STMS and PARTICIPANT may agree to include additional transaction types in the TransArmor Service when made available by STMS. If PARTICIPANT 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 STMS for authorization processing and PARTICIPANT assumes all risk associated with its transmission if Card data is stolen during transmittal to STMS's systems.

1.3 The TransArmor Services described in this Schedule are provided by STMS and not the Bank. The Bank has no performance obligations or liabilities to PARTICIPANT in connection with the TransArmor Services.

2 PCI DSS Limitations

2.1 Use of the TransArmor Service will not, on its own, cause PARTICIPANT to be compliant with, or eliminate PARTICIPANT's obligation to comply with PCI DSS or any other Network Rules. PARTICIPANT must

demonstrate and maintain a current PCI DSS compliance certification. PARTICIPANT'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 PARTICIPANT's business, passing quarterly network scans performed by an Approved Scan Vendor. PARTICIPANT must successfully meet the above requirements to obtain PCI DSS compliance validation; provided, however, PARTICIPANT is not required to perform quarterly network scans, if PARTICIPANT uses a validated P2PE solution (e.g., TransArmor P2PE) in accordance with the P2PE Instruction Manual accompanying the validated P2PE solution.

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

3 Intellectual Property

STMS 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 PARTICIPANT in connection with the TransArmor Services. Except as allowed under this Agreement, PARTICIPANT 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.

4 TransArmor Limited Warranty

Subject to the terms of this Schedule, STMS warrants that the Token or Multi-Pay Token, as applicable, returned to PARTICIPANT 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 PARTICIPANT Systems. This warranty is the **TransArmor Limited Warranty**. To be eligible for the TransArmor Limited Warranty, PARTICIPANT must maintain a processing relationship with STMS 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, STMS will indemnify PARTICIPANT for direct damages, including third party claims, resulting from STMS's breach of the TransArmor Limited Warranty; which is (1) PARTICIPANT's express and sole remedy for STMS's breach of the TransArmor Limited Warranty, and (2) STMS's entire liability for its breach of the TransArmor Limited Warranty. The TransArmor Limited Warranty is void if (1) PARTICIPANT 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) PARTICIPANT is grossly negligent or engages in intentional misconduct.

5 Fees

PARTICIPANT will pay STMS the fees in Schedule B.

6 TransArmor Rules and Procedures

6.1 PARTICIPANT must ensure that all third parties and software used by PARTICIPANT in connection with PARTICIPANT's payment card processing are compliant with PCI DSS.

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

6.3 PARTICIPANT 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, includingsettlement processing, retrieval processing, chargeback and adjustment processing, and transaction reviews.

6.4 Any point of sale device, gateway, or value-added reseller used by PARTICIPANT in connection with the

TransArmor Service must be certified by STMS for use with the TransArmor Service.

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

6.6 PARTICIPANT must utilize truncated report viewing and data extract creation within reporting tools provided by STMS.

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

6.8 PARTICIPANT 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.

6.9 PARTICIPANT must obtain a Cardholder's written or electronic consent to store a Multi-Pay Token to represent the Cardholder's Card number for future purchases.

6.10 PARTICIPANT must store the Multi-Pay Token in PARTICIPANT Systems in lieu of the Card number for allCardholder profile records.

6.11 PARTICIPANT 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 aUser ID and password.

6.12 If PARTICIPANT ends its processing relationship with STMS, PARTICIPANT must permanently delete all Tokens or Multi-Pay Tokens, as applicable, from all PARTICIPANT Systems within 90 days after terminationor expiration of the processing relationship.

6.13 PARTICIPANT use of the TransArmor P2PE Solution must comply with (a) STMS's requirements outlined in the P2PE Implementation Manual (**PIM**) and (b) PCI Council requirements in PARTICIPANT'suse of the TransArmor P2PE service for PARTICIPANT Systems to be P2PE validated, including but not limited to PARTICIPANT's use of STMS's approved validated key injection facilities. Additionally, PARTICIPANT is also responsible to keep track of all PARTICIPANT Systems 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

PARTICIPANT Systems inventory at the minimum of once per year to maintain P2PE validation.

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