Schedule N
Account Verification Services

This Account Verification Services Service Schedule (**Schedule**) is attached to and subject to the terms of the ASP Services Exhibit to 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 Fiserv Solutions, LLC (**Fiserv or Provider**), an Affiliate of 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. Background. Provider will provide the services in this Account Verification Services Schedule ("**Schedule**") to support the Participant's ("Customer" or "Participant" as used herein) payments to individuals and other entities.

(a) Account Verification Services. The Account Verification Services are described below ("**Account Verification Services**") are designed to validate that Deposit Accounts to be used for ACH funds transfers are owned by or accessible by the intended recipient ("**Payee**"). The Account Verification Services provide the following verification methods: (i) instant account verifications (i.e., validation against a third party database provided by Early Warning Services); (ii) real-time account verifications (i.e., validation using AllData aggregation); and (iii) trial deposits. ACH funds transfers are outside the scope of the Account Verification Services. "Deposit Account" means a U.S. checking, savings, or money market account. Customer acknowledges that not all Deposit Accounts and Deposit Account types can be successfully verified through the Account Verification Services.

(b) U.S. Only Services. Customer will only utilize the Account Verification Services with Payees' U.S. Deposit Accounts.

2. Risk and Compliance.

(a) Account Verification Service. Provider is relying on data provided by third parties and does not investigate and is not responsible for the accuracy of such data in connection with its performance of the Account Verification Service. Customer acknowledges and agrees that in conjunction with Account Verification Services: (i) third party data may be obtained from databases whose accuracy, timelines and coverage are not guaranteed; (ii) such data may be only be used to verify a Payee's Deposit Account and for no other purpose; (iii) Provider does not warrant or guarantee the identity of a Payee or Payee's Deposit Account, but merely receives a result from a third party provider ("**Result**") which is derived, in part, from information provided by Customer to Provider;; and (iv) the Result and related Account Verification Services will be only used for the purpose of verifying the identity of the Payee Deposit Account and will not be used, in whole or in part, as a basis for determining the eligibility of a Payee for credit, insurance or employment or to take 'adverse action,' as defined in the Fair Credit Reporting Act ("**FCRA**") or similar laws. Customer acknowledges and agrees that Provider and its third party providers described herein recommend that Customer use a manual verification process if a Result does not meet

or exceed the threshold for a positive verification, or if Customer receives a flag (indicating a possible match) from a fraud detection database.

(b) Risk. The Account Verification Services are dependent on information provided by third party data providers that may or may not be accurate, and information provided by the Customer; Provider can neither guarantee nor confirm the right to access an account by any Payee, or whether the Payee owns any Deposit Account. For example, and without limitation, if a criminal has the login credentials for the Payee's account with Customer, as well as with the Payee's external account and successfully validates the trial deposits made available through Account Verification Services at the external account, then the Account Verification Services may not identify such criminal as anyone other than the Payee. The Account Verification Services do not include any services pertaining to funds transfers; Provider is not responsible for funds transfer losses, monitoring transactions for fraud or other risks as part of the Account Verification Services.

(c) Payee License and Consent. Customer will be required to share with Provider certain data, including without limitation: (a) the Payee's name and tax identification number; and (b) Deposit Account information (e.g. ABA Routing and Transit Number that are specific to a Payee' Deposit Account) (collectively, "**Payee Data**"). Customer consents to Provider's disclosure of the Payee Data to certain Provider supplier(s) solely in connection with the verification and authentication of Payees and Deposit Accounts and subject to the terms and conditions of this Schedule. Customer acknowledges that such Account Verification Services are proprietary and confidential. Customer grants to Provider and Provider's applicable supplier(s) a non-exclusive, non-transferable, except as provided herein, right to use, copy, store, modify and display the Payee Data solely to the extent necessary to provide the Account Verification Services pursuant to this Schedule. Customer has or will obtain all necessary Payee agreements or consents as may be reasonably required to grant such license rights to Provider and its suppliers.

(d) Compliance. Customer certifies with respect to any Account Verification Services that Customer will obtain such services solely for the purpose of verifying a Payee Deposit Account, and specifically not to determine the Payee's eligibility for credit, insurance, employment or any other product or service. At its own expense, Customer will comply with all applicable laws and regulations regarding the use and receipt of the Account Verification Services.

3. Early Warning Account Verification Service. The following additional terms apply to Customer's receipt of Account Verification Services through Early Warning Services LLC ("**EWS**"). EWS is a consumer reporting agency and is the administrator of what is known as the "**National Shared Database**", which contains contributed consumer and business account data from hundreds of participating financial institutions and other organizations.

(a) Description of EWS Account Verification Service. The Account Verification Services performed through EWS consists of EWS' Account Ownership Service and Account Status Service ("**EWS Account Verification Service**") which provides information on the ownership of the Deposit Account, whether the Payee associated with the Deposit Account is authorized to transact on the given Deposit Account, and in the case of the Account Status Service, whether a presented Account number is open, closed, or not located in the National Shared Database. The EWS Account Verification Services allows Provider to make an electronic inquiry to EWS through a Provider connection with EWS in order to receive information from the National Shared Database transmitted in response to such inquiry ("**Response Data**").

(b) Authorized Use. Response Data is based on information from the National Shared Database reported as of the last contribution submitted to the National Shared Database. Response Data is not a guarantee of Account or payment status. Customer shall use the EWS Account Verification Services and

Response Data, and responses that are comprised of or derived from, in whole or in part, Response Data, (i) subject to the terms and conditions of this Schedule, and (ii) solely for the purpose of determining whether to initiate a payment to a particular Deposit Account via the automated clearinghouse (ACH) as the method of payment, and (iii) for no other purpose. Customer shall not provide or disclose the Response Data to any other person or entity, including any other local, state or federal government agency or its contractors.

(c) Time Sensitive. Response Data is time-sensitive and shall only be used in connection with the specific inquiry for which it was requested.

(d) Contribution Requirements. Customer acknowledges and agrees, on behalf of itself and Payees, that all information submitted by Customer in an inquiry or otherwise contributed by Customer pursuant to this Section 3 is contributed to the National Shared Database, and may be used by EWS for the purpose of providing the EWS Account Verification Services and its other services in compliance with all applicable laws. Customer, on behalf of itself and Payees, authorizes EWS to use such information for the purpose of (a) preparing statistical reports and conducting data analytics, parsing routines, data modeling and other analyses to test and evaluate EWS' service; (b) developing and providing new services or enhancements to existing services; and (c) developing and providing services to third parties engaged in the business of offering identity theft protection services to consumers, provided that no personally identifiable information shall be returned to any such third parties. The reports and results of the analyses described in clause (a) may be provided to other inquirers and contributors of EWS, provided that such reports and analyses do not identify specific inquiry data or Response Data with respect to Customer.

(e) Survival. Section 3 will survive termination of the EWS Account Verification Services.

4. Account Verification Services Fees. – See Schedule B