Schedule A – SECURITY PROCEDURES

*Except as may otherwise be noted, the following Security Procedures are **required** for all Customers who request to use and are approved by the Bank to use any or all of the following Services: Treasury/Business & Government Services, Online Banking, Mobile Banking and Mobile Deposit, unless otherwise indicated. Compliance with the Security Procedures may require Customer to obtain additional Services, which may have additional costs related to the Service(s):*

Online Banking / Mobile Banking Service User ID: This is the individual electronic identification, in letters and numerals and associated password, assigned by the Bank to the Administrator, and to each of those Authorized Users requested by the Administrator, that will be used for log-in by the Administrator and Authorized User(s). The Administrator and each Authorized User will have an individual, unique User ID and password.

Online Banking / Mobile Banking Service User Password: At set-up, the Bank will provide an individual, temporary password to the Administrator and the Administrator will assign a temporary password to each Authorized User(s). The Administrator and Authorized User(s) will be required to change their individual password upon the first sign-on to a unique password known only to him/her. Passwords are case-sensitive and require a minimum number of eight (8) alpha-numeric and upper-lowercase characters and must utilize at least one (1) special character and at least one (1) number, as the Bank may set forth from time to time. The Bank strongly recommends that the Administrator and Authorized User(s) change his or her individual password at least every ninety (90) days for security purposes. Passwords shall not be associated with any commonly known personal identification, such as the User's name, date of birth, telephone numbers, addresses, children's names, or pets' names, and should be memorized rather than written down. Upon three unsuccessful attempts to use a password, access to Online Banking will be suspended. To re-establish authorization to use Online Banking, Customer must contact the Bank to have the password re-set.

Mobile Deposit Login: To access Mobile Deposit, where applicable, Customer must log in to Mobile Banking using its User Name and Password.

Enhanced Log-In Security: In addition to the above individual User ID and individual passwords, access to Online Banking includes, as part of the Access Devices, a multi-factor authentication security procedure at first log-in for Customer, including Customer's Administrator and Authorized Users. This additional security procedure involves an additional credential for each User that is in addition to User ID and individual password security (hereinafter "Enhanced Log-in Security"). Enhanced Log-in Security includes, but is not limited to, additional log-in security features such as identification and verification of IP addresses, computer registration, access filters and other information. Enhanced Log-In Security may also require each User of Online Banking to establish and utilize, in addition to individual User ID and passwords, his/her own individual authentication through the use of personal identifying questions and image verification. Further authentication and monitoring by the Bank and/or its third party service provider(s) may occur automatically due to the detection of unusual source or log-in occurrences in relation to that access identity.

Single Sign-On: Once set-up in Online Banking with authentication protocols and Access Devices as described above, the Administrator can access all of the authorized functionality in or through Online Banking (unless otherwise restricted by Bank) without a separate sign-on, and can access those functions through a single sign-on feature. Authorized User(s) can also access certain features through single sign-on when authorized to access those features by the Administrator.

Additional Authentication: An additional required Security Procedure incorporates use of tokens for use with certain transactional functionality associated with ACH transactions and wire transfers. A token may be issued to any Authorized User(s), for example, of Online Banking, and for use in initiating and/or approving ACH transactions and wire transfers. Notwithstanding the foregoing, the Bank reserves the right to require the use of a token for all or certain other functionality from time to time, in its sole discretion, including by way of example only and not by way of limitation, the use of a token with certain administrative functionality and for the creation of ACH and wire templates, as applicable.

Minimum Computer Requirements: Online Banking may be used with various Internet browsers as the Bank may specify from time to time. To provide the highest degree of confidentiality and to protect the security of Customer's financial information, Customer must have an Internet browser that supports a minimum of 128-bit encryption and secure sockets layer version 3.0 or higher. Any use of Online Banking with lower than 128-bit encryption is strictly prohibited. To the extent Customer is able to access Online Banking using lower than 128-bit encryption, the Bank specifically disclaims any and all responsibility and liability for losses resulting from Customer's use of such lower encryption. Bank may change these requirements from time to time.

Callbacks: For wire transfer requests initiated by Customer via Online Banking, an additional required security procedure incorporates the use of a call-back. The Bank will accept such wire transfer requests from persons identifying themselves as a User(s) of Customer, and the Bank will then verify the identity of such person by calling him/her back at a telephone number(s) previously provided to the Bank by Customer. Bank enforces this callback feature for all wire transfers of $50,000 or greater.

Additional Strongly Recommended Security Procedures:

From time to time and as applicable, the Bank may make available additional Security Procedures for use with Online Banking and related Services. The Bank strongly recommends the use of these additional Security Procedures to help deter and protect against unauthorized transactions associated with the Online Banking Services, including the following:

- **Dual Control:** The Bank strongly encourages Customer to segregate the duties of the Administrator who creates and approves Authorized Users, as well as those Authorized Users who can create transactions from those Authorized Users who can release and approve transactions. Company should put procedures in place that permit one Authorized User to create, edit, cancel, delete and restore certain transactions including but not limited to ACH Entries or files, Remote Deposit Capture batches or wire transfer requests with his/her Access Devices. A second *different* Authorized User with his/her Access Devices is required to approve, release or delete the transaction request. For Mobile Banking and Mobile Deposit, an Authorized User may approve a transaction using the Mobile Device associated with Mobile Banking and/or Mobile Deposit.

- **Browser Security Software:** As and when made available to Customer by the Bank or otherwise, browser security software may be downloaded on all Customer Computers used in conjunction with Online Banking to help protect against online fraud committed by financial malware and phishing attacks throughout the online banking process.

- **Cookie Restrictions:** An additional Security Procedure incorporates use of a cookie restriction with certain transactional or administrative functionality. Online Banking authenticates a browser cookie in order to allow access to transactional or administrative functions. If the browser cookie is not able to be authenticated (either due to a login from another device, or if the cookie has been removed), Customer/Authorized User will be restricted from accessing the transactional or administrative functions.

- **Mobile Device Security**: The Bank strongly encourages Customer to enable the "LOCK" feature on its Mobile Device for additional security.

- **Virus Protection**: The Bank strongly recommends utilization of reliable virus protection products on Customer's Computer and Mobile Device. Bank further strongly recommends that Customer routinely scan its Computer and Mobile Device using such reliable virus protection products, and remove any viruses found using such products.

- **Activity / Access Limits:** Customer (including through Customer's Administrator) may choose to implement activity and/or access limits for its Authorized User(s), as made available via the Online Banking Service from time to time. This may include, **by way of example only**, limitations on the Account(s) an Authorized User may access and/or the activities an Authorized User may perform (e.g., initiating transactions using the Internal Transfer, Bill Pay, ACH and/or Wire feature(s)), setting more restrictive withdrawal limits, and granting Authorized User(s) access to Mobile Banking and/or Mobile Deposit.

Additional Fraud Risk Prevention. The Bank offers the following and strongly recommends that Customer take the following actions (jointly referred to as “Fraud Prevention Actions”)

a. Enroll all Accounts in Positive Pay ("Positive Pay") service as it is described within its agreement and/or Appendix; and
b. Enroll all Accounts in the Bank's ACH Block & Filter service as it is described within its agreement and/or appendix;

Fraud Prevention Actions may require a fee or service charge that Customer is responsible for paying.

Without limiting the foregoing, Customer agrees that their failure to implement Fraud Prevention Actions, or if Customer fails to follow these or other precautions reasonable for Customer, that Customer is precluded from asserting any claims against the Bank for paying any Fraudulent Item (as defined below) that such product, service, or precaution was designed to detect or deter, and the Bank will not be required to re-credit Customer's account or otherwise have any liability for paying such items.

As used in this Agreement, a Fraudulent Item is any item that is not properly payable and that the Positive Pay system is designed to detect, including, without limitation, any item that is unauthorized, altered, counterfeit, or on which the amount has been altered. The term Fraudulent Item shall not apply to forged endorsements.

Additional Fraud Prevention Precautions:

The Bank makes available to its Customers certain products and services that are designed to detect and/or deter check fraud. While no product or service will be completely effective, the Bank believes that the products and services we offer will reduce the likelihood that certain types of fraudulent items will be paid against your Account. There are several fraud precautions and prevention measures available that you can and should take to decrease the risk of unauthorized transactions from your Account(s). Such precautions and prevention measures include, but are not limited to:

- Safeguarding and not disclosing to third parties information about Customer's Account, such as the account number(s);
- Safeguarding materials and information which can be used to access Customer's Account, including but not limited to, Customer's checkbook, blank or unused checks, electronic access devices including ATM cards, personal identification numbers, and any passwords or other access-related information, to prevent them from being misused by an unauthorized party;
- Calling Customer Service immediately if you suspect any problem with Customer's Account or unauthorized activity, or Customer's checkbook or unused checks are lost, stolen or misplaced;
- Reviewing carefully Customer's checkbook and unused checks for unauthorized activity if Customer suspects that any of these items may have been stolen or tampered with, or if Customer is the victim of theft or its property is burglarized;
- Promptly and carefully reviewing Customer's statement each month for unauthorized activity or missing deposits;
- Closing Customer's Account immediate upon discovery of any known or suspected unauthorized activity. When Customer reports missing, stolen, or unauthorized checks, the Bank may recommend that any account(s) that has been compromised by unauthorized or fraudulent activity be closed. If Customer declines this recommendation and elects to leave its account open, the Bank will discuss ways to minimize losses to Customer and the Bank. The Bank reserves the right to unilaterally close the Account(s) in the event the possibility or probability of losses with respect to such Account(s) is reasonably unacceptable to the Bank; and
- Maintaining close control over your facsimile signature devices to immediately detect any unauthorized use of those devices.

Security or operational procedures for the detection of Customer errors in creating any transaction, electronic item or electronic file are not provided by the Bank, and in no event shall the Bank be liable for Customer errors.

CUSTOMER ACKNOWLEDGES AND AGREES THAT, THE BANK HAS MADE AVAILABLE SERVICES DESIGNED TO REDUCE THE LIKELIHOOD OF PAYMENT FRAUD, AND COLLECTIVELY, THE SECURITY PROCEDURES (WHICH INCLUDE BUT ARE NOT LIMITED TO FRAUD PREVENTION ACTIONS) DESCRIBED IN THIS SCHEDULE ARE COMMERCIALLY REASONABLE METHODS FOR THE PURPOSE OF VERIFYING WHETHER ANY PAYMENT, TRANSFER OR OTHER REQUEST WAS INITIATED BY CUSTOMER. CUSTOMER AGREES THAT ITS FAILURE TO FOLLOW SECURITY PROCEDURES OR ANY ELECTION CUSTOMER MAY MAKE TO WAIVE OR CHANGE (WHERE PERMITTED BY BANK IN ITS SOLE AND EXCLUSIVE DISCRETION) RECOMMENDED SECURITY PROCEDURES ASSOCIATED WITH THE SERVICES ARE AT CUSTOMER'S SOLE RISK. CUSTOMER FURTHER AGREES THAT ANY PAYMENT, TRANSFER OR OTHER REQUEST TRANSMITTED OR PURPORTED TO BE TRANSMITTED BY CUSTOMER AFTER WAIVING PORTIONS OF THE SECURITY PROCEDURES SHALL BE TREATED AS AUTHORIZED, AND CUSTOMER SHALL BE RESPONSIBLE FOR ANY LOSS RESULTING IN WHOLE OR IN PART FROM SUCH WAIVER.