Androscoggin Bank

BUSINESS & GOVERNMENT SERVICES MASTER AGREEMENT: BUSINESS ONLINE BANKING SERVICE APPENDIX

Customer: _____

Date of Master Agreement: _____ Date of Appendix: _____

THIS BUSINESS ONLINE BANKING SERVICE APPENDIX (hereinafter, this "**Appendix**") is incorporated by reference into the Business & Government Services Master Agreement (the "**Master Agreement**") by and between ANDROSCOGGIN BANK ("Bank") and the Customer identified above. This Appendix governs Customer's use of Bank's Business Online Banking Service (also referred to as the "Online Banking Service" or "Online Banking"). All capitalized terms used herein without definition shall have the meanings given to them in the parties' Master Agreement. Except as otherwise expressly provided in this Appendix, to the extent that this Appendix is inconsistent with the provisions of the Master Agreement, this Appendix and any amendment hereto from time to time shall control, but only to the extent necessary to resolve such conflict. This Appendix shall be effective when signed by both parties, and such date shall be as reflected above. If this Appendix conflicts in any way with the provisions of the Internet Banking Terms & Conditions that are accepted as part of the Online Banking enrollment process, this Appendix shall control

TERMS AND CONDITIONS

1. Eligibility. Customer is eligible to use Online Banking if Customer maintains an Account (checking, savings and/or loan), has executed the Master Agreement, satisfies the Computer requirements associated with Online Banking and maintains an email address, and if Bank has otherwise approved Customer's use of Online Banking as described further below.

2. Access. To use Online Banking, Customer must have a Computer with access to the Internet and an email address. Customer will be required to complete and submit the Set-Up Forms associated with Online Banking and as required by Bank. Once Bank has received such Set-Up Forms and verified Customer's Account information, Bank will send Customer (by, e.g., telephone, secure email or similar method as Bank may elect from time to time) confirmation of Bank's acceptance of Customer's enrollment. During the enrollment process Bank will assign Customer a user code and password. Customer's enrollment in Online Banking will enable Customer to access only those Accounts that Customer has designated for access with Online Banking in Customer's Set-Up Forms. Customer can also add or remove access to any of Customer's Accounts through Online Banking by completing required Set-Up Forms. Access to Customer's Accounts through Online Banking will be based upon the identification of Authorized Users and authority levels specified by Customer in Customer's Set-Up Forms. Except as may otherwise be set forth in this Appendix, Bank shall have no responsibility or obligations whatsoever to monitor transactions through Online Banking to determine that they are made by or on behalf of Customer.

3. Administrator and Authorized Users.

3.1 Customer is solely responsible for designating a Senior Administrator, as set forth in the Set-Up Forms. The Senior Administrator may designate additional Administrator(s). For the purpose of this Agreement, the term "Administrator" will include "Senior Administrator," except where otherwise specified.

3.2 Customer understands that its Administrator(s) will control, and Customer authorizes Administrator(s) to control, access by Authorized Users of the Online Banking Service by instructing Bank to issue Access Devices. The Administrator(s) may instruct Bank to add, change or terminate Customer's Authorized User(s) or de-activate an Access Device(s) from time to time and in the Administrator(s)'s sole discretion.

3.3 Customer will require each Administrator and each Authorized User to review and comply with all provisions of the Master Agreement, this Appendix, any Addenda and all other applicable Appendices and/or agreements. Customer acknowledges and agrees that it is fully responsible for the failure of any Administrator or any Authorized User to so comply. Customer is responsible for any payment, transfer and other use of the Online Banking Service and any charges incurred by any Administrator and any Authorized User, even if such Administrator or Authorized User exceeds his/her authorization as established by Customer.

3.4 If an Authorized User authorizes other persons/entities to use the Authorized User's Access Devices in any manner, such authorization will be considered unlimited in amount and manner until Customer has notified Bank in writing as set forth in the Master Agreement or this Appendix, that Customer has revoked the authorization and changed, or caused Bank to change, the subject Authorized User's Access Devices. Customer is responsible for any transactions made by such persons/entities until Customer notifies Bank that transfers by that person/entity are no longer authorized and Bank has had a reasonable opportunity to act upon the requested change. Bank will not be liable for and will not reimburse Customer for any losses that may occur as a result of this authorized use of an Authorized User's Access Devices.

3.5 Customer shall notify Bank of any changes in access to or use of the Online Banking Service by the Administrator(s) or Authorized User(s) in accordance with the terms of the Master Agreement or this Appendix. Notwithstanding the foregoing, whenever an Administrator or Authorized User leaves Customer's employ or Customer otherwise revokes an Administrator's or Authorized User's authority to access or use the Online Banking Service, Customer must notify Bank in writing immediately.

Bank Use Only

By: _____ Misc. Information: _____

Scan: _____ _____

4. Access Devices; Security Procedures.

4.1 Upon successful enrollment, Customer can access the Online Banking Service from Bank's designated website, using the Online Banking Service's Access Devices and security procedures applicable to Customer's access to and use of Online Banking, as described in **Schedule A** attached hereto and in associated Appendices and/or Addenda from time to time (hereinafter the "Security Procedures"). As further described in **Schedule A**, Bank will assign Customer a user code and a temporary password at enrollment. An Administrator or Bank must set up access rights for each Authorized User(s). Individual passwords require a minimum of eight (8) and a maximum of fifteen (15) characters, and must include at least one letter and one number. Passwords are case sensitive. Passwords should not be associated with any commonly known personal identification, such as, social security number, address, date of birth, names of children, and should be memorized rather than written down. The Administrator(s) and Authorized User(s) are advised to change their individual passwords every forty-five (45) to sixty (60) days for security purposes.

4.2 Customer accepts as its sole responsibility the use, protection and maintenance of confidentiality of, and access to, the Access Devices. Customer agrees to take reasonable precautions to safeguard the Access Devices and keep them confidential. Customer agrees not to reveal the Access Devices to any unauthorized person. Customer further agrees to notify Bank immediately if Customer believes that the confidentiality of the Access Devices has been compromised in any manner.

4.3 The Access Devices identify and authenticate Customer (including the Administrator(s) and Authorized Users) to Bank when Customer accesses or uses the Online Banking Service. Customer authorizes Bank to rely on the Access Devices to identify Customer when Customer accesses or uses any of the Online Banking Service and as signature authorization for any payment, transfer or other use of the Online Banking Service. Customer acknowledges and agrees that Bank is authorized to act on any and all communications or instructions received using the Access Devices, regardless of whether the communications or instructions are authorized. Bank owns the Access Devices, and Customer may not transfer them to any other person or entity.

4.4 Customer understands that access to the Online Banking Service will be denied if invalid Access Devices are used or if the user exceeds the number of invalid attempts allowed by Bank.

4.5 Customer acknowledges and agrees that the Access Devices and other Security Procedures applicable to Customer's use of the Online Banking Service and set forth in the Master Agreement, this Appendix and associated Appendices are a commercially reasonable method for the purpose of verifying whether any payment, transfer or other use of the Online Banking Service was initiated by Customer. Customer also agrees that any election Customer may make to change or waive any Security Procedures required or recommended by Bank is at Customer's risk and that any loss resulting in whole or in part from such change or waiver will be Customer's responsibility. Customer further acknowledges and agrees that the Access Devices are not intended and that it is commercially reasonable that the Access Devices are not intended to detect any errors relating to or arising out of a payment, transfer or any other use of the Online Banking Service.

5. Features of the Online Banking Service.

5.1 By subscribing to the Online Banking Service, Customer will have access to the basic feature of the Online Banking Service, which allow Customer to view its Account(s).

5.2 In addition to the Online Banking Service's basic feature, additional features or modules related to the Online Banking Service may be offered from time to time by Bank, in its sole and exclusive discretion, including but not limited to the following:

(i) Bill Payment. Bill Payment transactions are subject to the terms and conditions of and require Customer's execution of the Bill Payment Service Addendum. The Bill Payment Service allows Customer to initiate payments or transfers either electronically or by check from a checking Account.

(ii) Wire Transfers. Wire transfers are subject to the terms and conditions of and require Customer's execution of Bank's Wire Transfer Service Addendum. The Wire Transfer Service allows Customer to transfer funds electronically, typically from Customer's Account(s) to other account(s) with Bank or to account(s) at other banks.

(iii) ACH Originations. ACH originations are subject to the terms and conditions of and require Customer's execution of Bank's ACH Origination Service Addendum. The ACH Origination Service allows Customer to initiate and approve (with pre-authorization) certain ACH transactions that Customer desires Bank to enter into the ACH network on Customer's behalf.

(iv) eStatements. eStatements are subject to the terms and conditions of and require Customer's execution of the eStatements Service Addendum. The eStatements feature allows Customer to view, as applicable, certain of Customer's current Deposit Account and Credit Account statements and associated Account notices (e.g., regulatory notices, change in terms notices, etc.) for those Accounts via the Online Banking Service's site.

(v) Business Mobile Banking. Business Mobile Banking transactions are subject to the terms and conditions of and require Customer's acceptance of the Internet Banking Terms and Conditions. The Business Mobile Banking feature allows Customer to use a downloadable software application on a smartphone or other eligible mobile device to perform certain electronic banking tasks.

(vi) Mobile Remote Deposit Capture. Mobile Remote Deposit Capture transactions are subject to the terms and conditions of and require Customer's acceptance of the terms of the Mobile Remote Deposit Service as provided to Customer by Bank. The Mobile Remote Deposit Capture feature allows Customer to make deposits to Customer's Accounts from remote locations by using an eligible camera-enabled mobile device to capture images of original paper checks and delivering the images and associated deposit information to Bank or Bank's designated processor.

Additional electronic banking services may be added by Bank from time to time in Bank's sole discretion. The use of certain features or modules related to the Online Banking Service may incur fees or other charges, which are disclosed in the Fee Schedule.

6. Transaction Procedures: Internal Transfers. Internal Transfers may be processed in three (3) different transaction modes as follows:

6.1 One-Time Express Transfers.

(i) One-Time Express Transfers initiated before 5:00 p.m. on any Business Day will be processed on the same Business Day, and those initiated after 5:00 p.m. on a Business Day or at any time on a day that is not a Business Day will be processed on the next Business Day.

(ii) Customer must have sufficient Available Funds (either in the Account or via an overdraft line of credit) on the day and at the time Customer requests the One-Time Express Transfer or electronic transaction. One-Time Express Transfers may not be canceled for any reason once Customer has ended Customer's Online Banking Service session, as funds are immediately deducted from Customer's designated Account.

6.2 Scheduled Future Transfers. If Customer designates an Internal Transfer as a Scheduled Future Transfer, Customer may request that the transaction be made on a future date that Customer may designate which is in advance of the Scheduled Initiation Date. The "Scheduled Initiation Date" will be the effective date Customer enters, or the previous Business Day should the effective date fall on a weekend or holiday. Customer must have sufficient Available Funds by midnight of the night before the Scheduled Initiation Date; however, funds will be deducted from Customer's designated Account on the Scheduled Initiation Date. Scheduled Future Transfers may be canceled up to one (1) Business Day in advance of the Schedule Initiation Date.

6.3 Recurring Transfers. If Customer designates an Internal Transfer as a Recurring Transfer, Customer may request, and Bank will use, a Scheduled Initiation Date that re-occurs on a specified regular basis (e.g., weekly, semi-monthly, monthly, etc.). Customer will designate a "start" and an "end" date. Customer must have sufficient Available Funds by midnight of the night before the Scheduled Initiation Date; however, funds will be deducted from Customer's designated Account on the Scheduled Initiation Date. Recurring Transfers may be canceled up to one (1) Business Day in advance of the Schedule Initiation Date.

7. Limits on Internal Transfers. Internal Transfers initiated through the Online Banking Service are subject to there being sufficient Available Funds in the affected Account to cover the transfer on the Scheduled Initiation Date. Except as provided herein, Internal Transfers are subject to the terms and conditions applicable to such Account as set forth in the governing Account Agreement. Bank reserves the right to limit the frequency and dollar amount of transfers for security reasons.

Customer's ability to transfer funds between and/or make payments from Customer's savings or money market Deposit Accounts is limited by federal and state law, as may be further set forth in the Deposit Account Agreement.

8. Internal Transfers: Set-Up.

8.1 Account Designation. Customer will designate Accounts between which Customer may transfer funds electronically through the Online Banking Service. All of these Accounts must be in Customer's name (as owner or co-owner, except as may otherwise be approved by Bank in its sole and exclusive discretion) and be eligible for Internal Transfer. Eligible Accounts for Internal Transfer include checking, savings, and money market Accounts.

8.2 Cut-off Time; Funds Availability. Although Customer receives immediate provisional credit upon completion of an Online Banking Service session for One-Time Express Transfers made during that session, Customer must make Internal Transfers before 5:00 p.m. on a Business Day for those funds to be posted on an Account on the same Business Day and available for non-Online Banking Service transactions. Internal Transfers designated as One-Time Express Transfers made after 5:00 p.m. on a Business Day or on a non-Business Day will be available for the payment of non-Online Banking Service transactions on the next Business Day.

9. Internal Transfers: Canceling or Modifying. A One-Time Express Transfer cannot be canceled or modified. In order to cancel or modify a Future Internal Transfer or Recurring Internal Transfer, Customer must use the Online Banking Service and follow the instructions provided to Customer. Customer must cancel or modify the Future Internal Transfer or Recurring Internal Transfer using the Online Banking Service before the cut-off times described above.

10. Stop Payment. Subject to Bank's approval, Customer may elect to use the Online Banking Service to initiate a stop payment request for any check written on Customer's Accounts. Customer agrees that any stop payment request shall be null and void after six (6) months from the date of the order, or such earlier time as communicated by Bank to Customer. Customer agrees to provide all required information relating to stop payment requests. If Customer fails to provide Bank with complete information or if the information Customer provides is incorrect, Customer agrees that Bank shall not be responsible for any failure to stop payment on such item. Customer understands that if the stop payment request comes too late for Bank to

have a reasonable time to act on it prior to paying, settling for, posting or becoming accountable for the check described in the request, then Customer's stop payment request shall be of no effect. Customer agrees not to make a claim against Bank if the check is paid through inadvertence, accident, oversight or if Bank is required to pay such check by a holder in due course or if by reason of such payment, other items drawn on Customer's Account(s) are returned insufficient. Customer agrees to indemnify and hold Bank harmless from and against any and all losses, damages and expenses, including court costs and attorney's fees, incurred by Bank due to Bank's refusal of payment of any check or other item in accordance with Customer's stop payment instructions. Unless otherwise provided in this Appendix, Customer may not stop payment of electronic fund transfers. Therefore, Customer should not employ electronic access for purchases or services unless Customer is satisfied that it will not need to stop payment.

11. Balance Reporting. This feature provides Customer with various online reports that display certain Account(s) balances, status summary and information detail that can be reviewed online and exported. This feature also provides online access to images of paid checks.

12. Financial Management (FM) Software. The Financial Management Software feature of the Online Banking Service ("FMS Service") allows Customer to use personal financial management software ("FMS Software") (e.g., Quicken®, or QuickBooks®*) to access the Online Banking Service and export Account information such as balance and transaction history. This Section 2 sets forth additional terms and conditions that apply whenever Customer uses or permits any other person(s) or entity to use the FMS Service. The terms and conditions contained in this Section are limited to use of the FMS Service, and do not include use of products and services directly accessible through the Online Banking Service without the use of FMS Software. The Online Banking Service utilizes current releases of Quicken® and QuickBooks®, as may be made available from time to time from the respective software manufacturer. Customer is responsible for obtaining and maintaining any software that is required for operation of the FMS Service. Customer's use of the FMS Software is governed by the software license agreement(s) included with each software application. Customer must agree to the terms and conditions of the software license agreement(s) during the installation of the FMS Software on Customer's Computer. Customer is responsible for the correct set-up and installation of the FMS Software, as well as maintenance, updates and upgrades to the FMS Software and/or Customer's Computer. Bank makes no warranties nor accepts any liability for such software. Bank is not responsible for any problems related to the FMS Software itself, Customer's Computer or Customer's ability to connect using the FMS Software as described in this Appendix.

12.1 The FMS Service. Information about Account activity is synchronized between Customer's FMS Software and the Online Banking Service website. Customer may access such information directly through the Online Banking Service. Information via Customer's FMS Software may differ from the information that is available directly through the Online Banking Service. Information available directly through the Online Banking Service may not be available via Customer's FMS Software, may be described using different terminology, or may be more current than the information available via Customer's FMS Software. The method of entering instructions via Customer's FMS Software may also differ from the method of entering instructions directly through the Online Banking Service. Bank is not responsible for such differences, whether or not attributable to Customer's use of FMS Software.

12.2 Customer is responsible for all transfers and payments that Customer authorizes using FMS Software. If Customer permits other persons to access the Online Banking Service using FMS Software, Customer is responsible for all transactions it authorizes from Account(s) accessed via FMS Software. Customer must establish its own internal security procedures for employees that Customer authorizes to use the Online Banking Service via FMS Software and to prevent unauthorized use by other employees or persons.

12.3 This Appendix describes Bank's responsibility for completing transfers and payments, and any exceptions from liability for its failure to do so. These rules apply to Customer's transactions using FMS Software. Bank is not responsible for any problems that Customer may have using FMS Software to connect to the Online Banking Service if no known problem exists with Bank's systems that might impede such connectivity, or if the problem is due to Customer's software, Computer or Internet service. Customer should verify all Account data obtained and transactions executed on Customer's Accounts using FMS Software. Bank's records of transactions, instructions and communications regarding Customer's Accounts and use of the Online Banking Service supersede any records stored or created on Customer's Computer through the use of FMS Software. Customer is responsible for any and all obligations to any software vendor arising from Customer's use of that vendor's FMS Software.

13. Authorization to Charge Accounts. Customer authorizes Bank and Bank's processor(s) to provide the Online Banking Service to Customer, and, if applicable, authorizes Bank or Bank's processor(s) to initiate automated clearing house (ACH) debits or charges to Customer's designated Account(s) for any transactions accomplished through the use of the Online Banking Service, including the amount of any Internal Transfer that Customer makes and any charges for the Online Banking Service.

14. Documentation and Verification of Transactions.

14.1 Confirmation Numbers. Upon completion of a transaction using the Online Banking Service, a confirmation number will be given. Customer should record this number, along with the transaction amount in Customer's checkbook register (or other permanent record), as this will help in resolving any problems that may occur. No printed receipts are issued through the Online Banking Service.

14.2 Statements. Customer will not receive a separate Online Banking statement. Transfers to and from Customer's Accounts using Online Banking will appear on the respective periodic statements for each of Customer's Accounts. In addition to, but not in lieu of, Customer periodic statement(s) received by mail, an electronic PDF copy of Customer's periodic statement(s) will be available for viewing via the Online Banking Service. Such PDF version of the periodic statement(s) will be available for a period of at least thirty (30) months.

* Quicken® (and QuickBooks®) is a registered trademark of Intuit Inc.

15. Customer Responsibilities; Security.

15.1 Customer is responsible for all transfers, payments or other Online Banking Service transactions that Customer authorizes to be made using the Online Banking Service.

15.2 Customer agrees not to disclose any proprietary information regarding the Online Banking Service to any third party (except to Customer's Administrator(s) and Authorized User(s)). Customer also agrees to comply with any operating, security and recognition procedures Bank may establish from time to time with respect to the Online Banking Service. Customer will be denied access to the Online Banking Service if Customer fails to comply with any of these procedures. Customer acknowledges that there can be no guarantee of secure transmissions over the Internet and that the Online Banking Service's Security Procedures are reasonable. Customer is responsible for reviewing the transaction reports Bank provides on-line and in Customer's monthly statements to detect unauthorized or suspicious transactions. In addition to any other provision hereof regarding authorization of transactions using the Online Banking Service, all transactions will be deemed to be authorized by Customer and to be correctly executed after Bank first provides Customer with a statement or online transaction report showing that transaction, unless Customer has provided written notice that the transaction was unauthorized or erroneously executed within the timeframes set forth in Section of the Master Agreement.

16. Disclosure of Account Information. In accordance with Bank's privacy policy, Bank will disclose information to third parties about Customer's Account(s) or Customer's Online Banking transactions:

(i) when it is necessary in order to complete transfers;

(ii) to verify the existence and/or condition of Customer's Account(s) for a third party, such as a credit bureau or merchant;

(iii) to comply with a government agency or court order or the request of a state or federal regulatory agency;

(iv) if Customer gives permission to Bank; and

(v) on a closed Account, if Bank believes Customer has mishandled it.

17. Contacting Bank. Customer may contact Bank at the phone number and address provided in Section 26 of the Master Agreement to: (a) request a stop payment, (b) inquire about the receipt and/or amount of credits to Customer's Account(s), (c) notify Bank if Customer's Access Devices are lost or stolen, (d) notify Bank of unauthorized transactions appearing on Customer's statement, or (e) change Customer's mailing or email address.

18. Joint Accounts. When Customer's access to the Online Banking is linked to one or more jointly owned Accounts, Bank may act on the verbal, written or electronic instructions of any joint owner of those Accounts. Each owner of a Deposit Account is authorized to access all of the Available Funds held in that Deposit Account through Online Banking.

19. Hyperlinks. Bank may elect to display one or more hyperlinks on the Online Banking Service website from time to time. A hyperlink is any highlighted words or phrases in a document that allows Customer to click through to another section of the same document or to another document on the Internet. A hyperlink may allow Customer to click through to a third party website over which Bank has no control. Bank disclaims any responsibility for the content, products and services provided at linked third party websites. Bank is not liable for any failure of the products or services advertised on third party websites. Customer should be aware that third party websites may have privacy policies that differ from Bank's; it is Customer's responsibility to review privacy policies at the linked third party websites to determine whether those policies are acceptable to Customer. The linked third party websites may provide less security than Bank's website.

20. Hours of Access. Online Banking is generally available seven (7) days a week, twenty-four (24) hours a day. Customer may restrict the day(s) and/or time(s) that its Administrator(s) and/or Authorized User(s) may access to Online Banking. Some or all features of Online Banking may not be available from time to time due to problems arising in connection with transmissions over the Internet, as well as emergency or scheduled system maintenance. Bank will post a notice of any extended periods of non-availability on the Online Banking site. Certain transactions posted outside normal business hours, such as those using the Bill Payment Service, will not take effect until the next Business Day.

21. Overdrafts. Customer agrees to initiate or schedule all transfers or payment transactions only when there is or will be sufficient Available Funds in the Account for that transfer or payment. The completion of any transfer or payment order is subject to sufficient Available Funds in the Account at the time the transaction is posted. If Customer's Account has insufficient Available Funds to perform any fund transfer Customer has requested for a given Business Day, Bank may either pay or return it. Bank is not required to provide notification to Customer in any form that the transfer or payment order was not honored, and it is Customer's responsibility to make other arrangements to facilitate the processing of the transaction or payment by other means, which may include rescheduling or reinitiating the transaction in Online Banking. Customer agrees to pay the outstanding overdraft and any fee(s) associated with the overdraft in accordance with Bank's Fee Schedule, whether the item is paid or returned. The honoring of one or more of Customer's overdrafts, however, does not obligate Bank to honor any future overdrafts. Bank may assess a fee to Customer's Account for processing an item that is presented for payment for which there are no funds, insufficient funds or unavailable funds. Please refer to the Fee Schedule for the amount of this fee. If Customer has an "Overdraft Protection" feature with Customer's Deposit Account, any check or debit that overdraws such Deposit Account will be honored up to Customer's available credit limit.

22. Limits on Amounts and Frequency of Online Banking Transactions.

22.1 Transactions initiated through Online Banking may be limited in number or dollar amount. Bank reserves the right to limit the amount or number of any type of transaction for any customer at any time. Bank may limit the amount and or the number of transactions for any specific customer group or entity as Bank deems appropriate in its sole and exclusive discretion. Additional information regarding limitations on the amount of transfers can be found in the applicable Deposit Account Agreement. Any transaction limitation that is disclosed in these documents, in other areas, or is part of the Fee Schedule may be applied to any and all transactions initiated in Online Banking. Bank may amend, change, or abolish transaction limits of any kind at any time. Bank will use commercially reasonable efforts to give prior notice of such changes, but is not bound to do so except where governed by applicable law. All transactions are subject, in addition to any limitations on dollar amount or amount, to internal review by Bank from time to time, including but not limited to the review of factors such as the sending Account, receiving Account, the amount of the specific transaction, the aggregate amounts of other transactions processed or ordered by the customer, fraud screening, and other factors that Bank deems applicable and appropriate. If Bank determines that there are risks associated with the transaction, Bank may delay or cancel the transaction. Bank may request additional information regarding the transaction before it is finalized or any funds are released. In addition, if a hold has been placed on the deposits made to an Account from which Customer wishes to transfer funds, Customer cannot transfer the portion of the funds held until the hold expires.

23. Unauthorized Online Banking Service Transactions.

23.1 Customer will notify Bank at once if Customer believes its Access Devices have been stolen or compromised. Customer's Administrator must instruct Bank to de-activate, and has the sole responsibility for instructing Bank to de-activate, any such Access Device(s). In addition, Customer will notify Bank at once if Customer believes someone has transferred or may transfer money from Customer's Account(s) without Customer's permission or if Customer suspects any fraudulent activity on Customer's Account. In no event will Bank be liable for any unauthorized transaction(s) that occurs with any Access Devices, unless otherwise provided by applicable law.

23.2 When Customer gives someone its Access Device(s), Customer is authorizing that person to use the Online Banking Service, and Customer is responsible for all transactions the person performs using the Online Banking Service. All transactions that person performs, even transactions Customer did not intend or want performed, are authorized transactions. Transactions that Customer or someone acting with Customer initiates with fraudulent intent are also authorized transactions. For Customer's protection, Customer should sign-off after every Online Banking Service session and close Customer's browser to ensure confidentiality.

24. Fees / Charges.

24.1 Customer agrees to compensate Bank for the Online Banking Service in accordance with any applicable Fee Schedules or other agreement(s) between Bank and Customer in effect from time to time that may apply to the Online Banking Service (the "Service Fees"). By and upon entering into this Appendix, Customer acknowledges receipt and acceptance of the Service Fees and agrees to be bound by their terms, as those terms may be amended from time to time.

24.2 Customer authorizes Bank to charge the Primary Account for all applicable charges and fees for the Online Banking Service to the extent that such charges and fees are not offset by earnings credits or other allowances for Customer's Deposit Account(s) with Bank. If the balance of Available Funds in the Primary Account is not sufficient to cover such fees, Bank may charge such fees to any other Deposit Account maintained by Customer with Bank.

24.3 Bank may amend the Service Fee(s) at any time. Bank will give notice to Customer of such changes in accordance with applicable law.

25. Termination. The parties may terminate this Appendix in accordance with the terms and conditions of the parties' Master Agreement. This Appendix will automatically and immediately terminate if the parties' Master Agreement terminates, or if any Deposit Account upon which Online Banking is dependent is terminated. Any termination of this Appendix shall not affect any of Bank's rights and Customer's obligations with respect to transfer requests or related instructions initiated by Customer prior to the effective time of such termination, or the payment obligations of Customer with respect to services performed hereunder by Bank prior to the effective time of such termination, or any other obligations that survive termination of this Appendix. The provisions of this Appendix that are necessary to give effect to the purposes of this Appendix shall survive its termination.

26. Effectiveness. Customer agrees to all the terms and conditions of this Appendix. The liability of Bank under this Appendix shall in all cases be subject to the provisions of the Master Agreement, including, without limitation, any provisions thereof that exclude or limit warranties made by, damages payable by or remedies available from Bank. This Appendix replaces and supersedes all prior arrangements on file with respect to the services described herein and shall remain in full force and effect until termination or such time as a different or amended Appendix is accepted in writing by Bank or the Master Agreement is terminated.

IN WITNESS WHEREOF, Customer and Bank have duly caused this Appendix to be executed by an Authorized Representative.

CUSTOMER

Customer Name: _____

Address: _____

_____

By: _____

Print Name: _____

Title: _____

ANDROSCOGGIN BANK

By: _____

Print Name: _____

Title: _____

*Except as may otherwise be noted, the following Security Procedures are **required** for all customers who request to use and are approved by Bank to use any or all of the following Business Services: Online Banking, Mobile Banking and Mobile Deposit, unless otherwise indicated:*

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

Online Banking / Mobile Banking Service User Password: At set-up, Bank will provide an individual, temporary password to each Administrator(s) and the Administrator(s) will assign a temporary password to each Authorized User(s). Each Administrator(s) 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, as the Bank may set forth from time to time. Each Administrator and each Authorized User will have an individual, unique User ID and password. Bank strongly recommends that each Administrator(s) and Authorized User(s) change his or her individual password at least every ninety (90) days for security purposes. Passwords should 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 revoked. To re-establish authorization to use Online Banking, Customer must contact 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 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(s) 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(s).

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, 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 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, 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. Bank will accept such wire transfer requests from persons identifying themselves as an Authorized Representative of Customer, and Bank will then verify the identity of such person by calling him/her back at a telephone number(s) previously provided to Bank by Customer. Bank enforces this callback feature for all wire transfers of $50,000 or greater.

Customer Initials: _____

Additional Strongly Recommended Security Procedures:

From time to time and as applicable, Bank may make available additional Security Procedures for use with Online Banking and related Services. 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:** Bank strongly encourages Customer to segregate the duties of those Administrators who create and approve 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 AC 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 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/user will be restricted from accessing the transactional or administrative functions.

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

- **Virus Protection:** 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(s)) 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, AC and/or Wire feature(s)), setting more restrictive withdrawal limits, and granting Authorized User(s) access to Mobile Banking and/or Mobile Deposit.

CUSTOMER ACKNOWLEDGES AND AGREES THAT, COLLECTIVELY, THE SECURITY PROCEDURES 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 ANY ELECTION CUSTOMER MAY MAKE TO WAIVE OR CHANGE (WHERE PERMITTED BY BANK IN ITS SOLE AND EXCLUSIVE DISCRETION) THE 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 BY WAIVING 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.

Customer Initials: _____