SUMMARY OF BUSINESS & GOVERNMENT SERVICES AGREEMENT AMENDMENTS JANUARY 2025

As stated in Section 20 of your Business & Government Services Master Agreement (Master Agreement), the Bank may amend the Agreement, Services or Appendices in our sole discretion from time to time. This letter is to provide you notice of amendments to those documents as stated below. As stated in your Master Agreement you will be deemed to have accepted these amendments by accessing or using any of the Services after the effective date of March 20th, 2025. Please note that when you opened your account there were separate agreements for government and non-government customers. These agreements were substantially the same, so we have merged those agreements to form one agreement that covers both government and non-government customers.

We encourage you to visit **https://www.androscogginbank.com/business/library-of-agreements-appendices/** to review the Master Agreement in its entirety. Below we are providing a high-level summary of the amendments for your convenience. **YOU SHOULD PRINT AND SAVE BOTH THIS SUMMARY AND THE UPDATED VERSION OF THE AGREEMENT FOR YOUR FUTURE REFERENCE.**

General

We have made some clerical updates or corrections to the following documents, such as consistently using the term "Customer" rather than "Client". We are not identifying all clerical updates (which include but are not limited to paragraph lettering or numbering changes), but we are providing you a summary of the substantive changes. Unless otherwise indicated, all other provision of the agreements and appendices remain in full force and effect.

1. Business & Government Services Master Agreement

Definitions

Except for in the definition section and Section 14.1 the term "Authorized Representative" is replaced with the term "Authorized User(s)" or "User(s)" which means an Authorized Representative(s), Administrator(s) and/or Authorized User(s)".

The following definitions have been replaced:

"Business & Government Service(s)", "Treasury Service(s) or "Service(s)" means, collectively, any one or all of the various electronic, online, mobile banking and/or associated cash management services maintained and provided by the Bank (and/or the Bank's third-party service providers) to Customer from time to time pursuant to this Agreement, the Appendices, exhibits, Set-Up form(s) and any service guides or manuals made available to Customer by the Bank, which are accessible using a personal computer or mobile device including a smartphone, tablet, or any other eligible handheld or wearable communication device.

"Fee Schedule" means, at any given time, the Bank's then current schedule of customer fees and charges applicable to the Deposit Account(s) opened by Customer and maintained with the Bank, as well as those fees and charges applicable to the Customer's Treasury services as reflected in the Account

Analysis (which may also be referred to as the Pricing Proforma) or as a charge communicated via email by a Treasury Sales Officer provided at the time of Treasury service(s) rollout."
The following definitions have been added:

"“Security Procedures” means those protective measures identified in Schedule A of this Agreement and the Business Online Banking Service Appendix that are required for all Customers who request to use and are approved by the Bank to use any or all of the Treasury Services which include: Treasury Management or Government services, Online Banking, Mobile Banking and Mobile Deposit, unless otherwise indicated.

Section 2.2: the following is added to section 2.2:
“Customer, through its Administrator(s) and/or Authorized User(s) is responsible for all access or use of the Services in accordance with this Agreement whether Customer facilitates access/modifications to access or requests the assistance of the Bank in facilitating/modifying access to the Services. Customer agrees that in facilitating access and/or modifying access Bank is acting as Customer’s agent and has no fiduciary duty to Customer.”

Section 10.1: it is deleted and replaced in its entirety as follows:
“In providing the Services, Bank shall be entitled to rely upon the accuracy of all information and authorizations received from Customer or an Authorized Representative and the authenticity of any signatures purporting to be of Customer or an Authorized Representative. Customer agrees to promptly modify the information in the Services or access to the Services or notify Bank of any changes to any information or authorization provided to Bank in connection with the Services and further agrees to promptly execute any new or additional documentation Bank reasonably deems necessary from time to time in order to continue to provide the Services to Customer.”

Section 10.2: the following sentences are added to Section 10.2:

“This includes but is not limited to Customer declining to implement any Bank recommended security procedures on any and all Accounts, whether or not there are additional costs/fees/charges to Customer associated with the security procedure. See **Schedule A** for Security Procedures. In the event that the Bank pays any fraudulent, unauthorized, altered, counterfeit or other fraudulent item that has not been verified by the Customer pursuant to the Security Procedures: 1. Customer shall bear any direct loss if Customer failed to properly utilize Fraud Prevention Actions and the Bank will not be required to re-credit Customer’s Account or otherwise have any liability for paying such items. 2. The appointment of liability herein applies solely to fraudulent items and does not affect any other type of loss addresses elsewhere in the Agreement.”

2. SCHEDULE A – SECURITY PROCEDURES

A new Schedule A – Security Procedures is added to the Master Agreement. We encourage you to review Schedule A in its entirety at: **https://www.androscogginbank.com/business/library-of-agreements-appendices/**

Please note that if you are a Business & Government Services Customer that also has online banking, these Security Procedures are part of the Online Banking Agreement and you are already subject to them. However, the Security Procedures have been updated and a summary of those updates is provided in the Business Online Banking Services Appendix section below.

3. POSITIVE PAY SERVICES APPENDIX

Section 4 now reads:

"Customer Liability. Utilizing Positive Pay on all Accounts is part of the Bank's Security Procedures. If Customer declines to enroll all Accounts, at fees set forth in the Bank's Fee Schedule, Customer accepts any and all liability for fraudulent, unauthorized, altered, counterfeit or other fraudulent items paid that may have been prevented had Customer enrolled said Account in the Service."

Schedule B:
If you need to modify your Authorized Users as set forth in your current Schedule B, you will do so using the Online Services - User Role Setup form. Schedule B has been removed from the agreement in its entirety and is now incorporated into the User Role Setup form. The substance of the information required to set up Authorized Users has not changed. However, until such time that you request a modification, your existing Schedule B will remain in full force and effect.

The remainder of the agreement remains in full force and effect with the following subsequent numbering changes: former section 4 is now numbered 5; former section 5 is now numbered 6, former section 6 is now numbered 7; former section 7 is now numbered 8.

4. ACH BLOCK & FILTER SERVICE APPENDIX

Section 8 now reads:

"8. Customer Liability.
8.1 Utilizing ACH Block & Filter on all Accounts is part of the Bank's Security Procedures. If Customer declines to enroll all Accounts, at fees set forth in the Bank's Fee Schedule, Customer accepts any and all liability for fraudulent transfers made that may have been prevented had Customer enrolled said Account(s) in the Service. "

Subsequently, former section 8 is now numbered 9, former section 9 is now numbered 10, and former section 10 is now numbered 11.

Schedule A:

If you need to modify the Blocks and Filters as set forth in your current Schedule A, those modifications will be done using the Online Services - Services Setup, Online Services - Account Setup, and Online Services - User Role Setup forms as Schedule A has been removed from the agreement in its entirely and incorporated into the referenced forms. The substantive information required has not changed. However, until such time that you request a modification, your existing Schedule A shall remain in full force and effect.

5. BUSINESS ONLINE BANKING SERVICES APPENDIX

Section 4.1 the following language was added:
"In the event that Bank pays any fraudulent, unauthorized, altered, counterfeit or other fraudulent item that has not been verified by the Customer pursuant to the Security Procedures: 1. Customer shall bear any direct loss if Customer failed to properly utilize Fraud Prevention Actions and Bank will not be required to re-credit Customer's Account or otherwise have any liability for paying such items. 2. The appointment of liability herein applies solely to fraudulent items and does not affect any other type of loss addresses elsewhere in the Agreement."

Section 5.2 will now read:
"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, which may require separate agreements/appendices (even if not stated below):….."

Schedule A: Security Procedures for Online Banking & Related Services:
Clarified that this Schedule A also applies to Treasury/Business & Government Services and that some Security Procedures may require the Customer to obtain additional Services at Customer's own cost.

Callbacks:
Existing paragraph is replaced in its entirety with the following:
"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, Administrator and/or Authorized User 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."

New section added as follows:

"Additional Fraud Risk Prevention. The Bank offers 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 this Appendix; and
b. Enroll all Accounts in the Bank's ACH Block & Filter service as it is described within its agreement and/or this 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 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 available to you. While no product or service will be completely effective, the Bank believes that products and services we may 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 your 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, 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, we will discuss with you ways to minimize losses to Customer and the Bank. 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 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 Bank, and in no event shall Bank be liable for Customer errors."

The following "acknowledgment" section is deleted and replaced as follows:
YOUR CONTINUED USE OF THE ONLINE BANKING SERVICE CONSTITUTES YOUR AGREEMENT WITH THESE SECURITY PROCEDURES.

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.

6. BUSINESS DEPOSIT TERMS & CONDITIONS ("Agreement")

The following amendments apply to your Agreement whether or not you have online banking.

As stated in Part 1, section d of your current Agreement we reserve the right to modify the terms of that Agreement at any time, which we may do by sending to you, in your statement (whether you have elected to receive paper or electronic statements) or to your statement mailing address or email address if you have elected to participate in electronic communications, a written notice of the modification. Such modification will be effective upon the date specified in the notice.

As such, we are providing you written notice of the following modifications to your Agreement, which take effect on March 20th, 2025. We encourage you to review the Agreement in its entirety at: **https://www.androscogginbank.com/business/library-of-agreements-appendices/**. We are providing a high level summary of the amendments below for your convenience**. You should print/save the agreement and this summary for your future reference. THESE CHANGES MAY IMPACT YOUR LIABILITY. You should contact your Bank representative to enroll in fraud prevention products we offer before the effective date of these changes, otherwise you will be deemed to have waived those fraud prevention measures which may subject you to liability.**

Although the Agreement has been reformatted and the numbers of sections may have been updated, unless otherwise stated, all provisions of the Agreement not modified by this letter, remain in full force and effect.

Throughout the agreement "Schedule of Charges" has been revised to use the term "Schedule of Fees and Charges".

We have added the following provisions:

PART 1 – GENERAL PROVISIONS:

"d). Your Fraud Liability:

We may deny a claim for losses due to forged, altered or unauthorized transactions, items or signatures, if you do not guard against improper access to your checks, statements, deposit slips, endorsement and signature stamps, and account information. We may also deny your claim if you do not monitor your account and report problems as provided in this Agreement.

We offer certain fraud prevention and detection products and services to business customers. If we have offered you one or more of these services, and you decline to use them or fail to implement them,

or you fail to follow the procedures necessary for proper use of these products or services, or you fail to follow other precautions reasonable for your particular circumstances, you are precluded from asserting any claims against us for paying any unauthorized, altered, counterfeit or other fraudulent item that such product, service, or precaution was designed to detect or deter, and we will not be required to re-credit your account or otherwise have any liability for paying such items. In addition to the liability limitations above, you agree that, at a minimum, you will use the Positive Pay product we offer or recommend to you (or any subsequent product we may offer providing similar or better protection against fraud within a reasonable time after we offer or recommend it to you). In the event that we pay any fraudulent, unauthorized, altered, counterfeit or other fraudulent item that has not been verified by you pursuant to Positive Pay: 1.You shall bear any direct loss if you failed to properly utilize Positive Pay and we will not be required to re-credit your account or otherwise have any liability for paying such items. 2. We shall bear any direct loss if you properly utilize Positive Pay but we honored such fraudulent item contrary to the Positive Pay preferences you have established with us in writing. The appointment of liability herein applies solely to fraudulent items and does not affect any other type of loss addressed elsewhere in this Agreement."

"e). General Liability Limitations. Our maximum liability is the lesser of your actual damages proved or the amount of the missing deposit or the forgery, alteration or other unauthorized withdrawal, reduced in all cases by the amount of the loss that could have been avoided by your use of ordinary care. We are not liable to you for special or consequential losses or damages of any kind, including loss of profits and opportunity for attorneys' fees incurred by you."

"k). Online or Mobile Services. If you open an account or obtain a product or service from us using our online or mobile services, we may record your personal information from a scan or a copy of your driver's license or other personal identification card, or we may receive an image or make a copy of your driver's license or other personal identification card. We may store or retain this information to the extent permitted by law.

l). Sample of Your Signature. To determine the authenticity of your signatures, we may refer to the signature card or to a check or other document upon which your signature appears. We may use an automated process to reproduce and retain your signature from a check upon which your signature appears and use that as your authorized signature. For example, if you open a checking account using our online or mobile services you agree that we will use the maker signature on the first check to clear the account as your authorized signature.

m). Business Insurance Rights. You agree to pursue all rights you may have under any insurance coverage you maintain before making a claim against us in connection with any transaction involving your accounts. You will provide us with all reasonable information about your coverage, including the name of your insurance carrier, policy number, policy limits and applicable deductibles. Our liability is reduced by the amount of all insurance proceeds you receive or are entitled to receive. At our request, you agree to assign to us your rights under your insurance policy."

PART 3 – RULES GOVERNING DEPOSIT ACCOUNTS

" k). Fraud Account Closure. If you or we suspect that your account is or may be compromised, we may recommend that you close your account and open a new account. If there are any unauthorized transactions on your account, we recommend you close your account and open a new one. If we recommend that you close your account and you do not do so, we are not liable to you for subsequent losses or damages on the account due to unauthorized transactions. When you open a new account, you are responsible for notifying any third parties that need to know your new account number."

“dd) Risk of Loss. You agree to bear the risk of loss if: you elect to have your checks printed by a vendor that has not been approved by us; or you make your check out in a way (such as using a lightly colored ink) that causes critical data to disappear or be obscured upon truncation, or you make your check out in a way (such as using a lightly colored ink) that causes critical data to disappear or be obscured upon truncation.

In addition, we have made amendments to **Part 1 former paragraph d (now f)**:
"Modifications of Agreement by Bank: We reserve the right to modify the terms in this Agreement at any time. Unless otherwise required by law, we may modify this Agreement, as well as any fees, charges or terms of your account(s), by sending to you, in your statement (whether you have elected to receive paper or electronic statements) or to your statement mailing address or email address if you have elected to participate in electronic communications, a written notice of the modification. Such modification will be effective upon the date specified in the notice."

PART 4 – INTEREST-BEARING ACCOUNTS

Paragraph d) Limits on Telephone and Preauthorized Transfers is deleted, and former paragraph e, is now paragraph d.

PART 5 – ELECTRIC FUND TRANSFERS

The following paragraphs are revised as follows**:**

a. In former paragraph i) now h) – Error Resolution Procedures Notes, we have reduced the time in which you have to notify us of any problem or error regarding an electronic transfer from sixty (60) days to thirty (30) days.
b. In former paragraph k) now j) - Types of Available Transfers, we have added that you may use online or mobile banking to transfer funds to other financial institutions.
c. In former paragraph l) now k) – Limitations on Cash Withdrawals, we have clarified limits on online or mobile banking transfers by adding the following language:
"If you transfer funds to another financial institution through online or mobile banking the standard daily limit is $15,000 per day, or $30,000 per month within the first 30-days of online account access. After 30-days your limits increase to $25,000 per day, or $50,000 per month. Your limit may be different. If you exceed your limit, we may remove online banking access and/or overdraw your account and assess any applicable charges.”