TRUIST

Treasury Terms and Conditions

Table of Contents

(Ctrl+Click the item to jump to that section)

TRUIST

Part I: General Terms and Conditions for All Services

Agreement Formation & Structure

1. Legal Agreement. These Truist Treasury Terms and Conditions are a legal agreement between Truist Bank ("Bank," "we" or "us") and its client ("Client," "you," or "your"), consisting of the General Terms and Conditions (Part I) and additional Service-Specific Terms and Conditions (Part II). Part I applies to all treasury management services provided by Bank, as listed in Part II (each a "Service," and together, the "Services"), to Client. Part II applies on a Service-specific basis, such that terms for Services that are not utilized by Client or implemented in connection with any Client account are not applicable to Client. You have agreed to these Treasury Terms and Conditions (the "Agreement") by utilizing any Service listed in Part II.

2. Other Agreements. Your relationship with Bank is also governed by a Commercial Bank Services Agreement ("CBSA") between you and the Bank. If there is any conflict between the terms of this Agreement and the CBSA, this Agreement will control. If you previously entered into a Treasury Management Agreement with Bank, this Agreement supersedes and replaces that Treasury Management Agreement. Any references to a Treasury Management Agreement in any reference materials or instruments related to your accounts, Services, or transactions will be deemed to refer to this Agreement. This Agreement and the CBSA contain the entire understanding of the parties and supersede any previous discussions, proposals, or agreements, whether oral or written, with respect to the Services or the subject matter referred to herein. This Agreement will not supersede or govern any lending relationship between the parties or any banking services other than the Services and demand deposit accounts associated with the Services.

3. Reference Materials. The "reference materials" for a Service consist of documents that provide details regarding the functionality of that service, as well as certain formatting and other technical requirements for the Service. Reference materials may include, without limitation, user and administrator manual, quick reference guides, FAQs, and/or file formats and specifications; reference materials may be separate documents or may be instructions contained or available within a Service. Bank may update, modify, or create new reference materials for a Service without notice to Client. Client may obtain current reference materials at any time upon request to Bank, or at the website or other online location as specified by Bank. In the event of any conflict between this Agreement and the reference materials, this Agreement will control.

4. Amendment. Bank may amend this Agreement, including the CBSA and the pricing applicable to any Service, by giving Client prior written notice of the amendment. Notwithstanding the foregoing, an amendment by Bank may become effective immediately if: (i) Bank reasonably determines that the amendment will not have a material adverse effect on Client's use of any Service, or (ii) the amendment is required for security reasons or by law. This Agreement may not otherwise be amended except in writing signed by both parties. If Client does not agree with any amendment, Client's sole recourse will be to cease using the applicable Service(s) prior to the effective date of the amendment.

5. Term and Termination. This Agreement will remain in full force and effect until it is terminated by either party as provided herein. Either party may terminate this Agreement or any Service by giving thirty (30) days prior written notice to the other party. The liabilities of the parties will cease on the effective date of termination, except as to events occurring or liabilities incurred prior to the effective date of termination. If Bank reasonably determines it is no longer able to provide a Service due to a change in laws or rules or if required by a regulatory authority, Bank may terminate this Agreement or a specific Service immediately upon written notice to Client. Without limiting any other available remedies, Bank may terminate this Agreement or any Service immediately upon written notice to Client if (i) Client fails to perform or to observe any of the conditions, covenants, or restrictions herein; (ii) in Bank's good faith opinion, Client is involved in potentially illegal or unethical business practices or is financially unstable; or (iii) in Bank's good faith opinion, the prospect of Client's payment or performance has been impaired.

6. Headings and Certain References. The headings used in this Agreement are for reference purposes only and should not be considered when interpreting this Agreement. Whenever the term "including" is used in this Agreement, it means "including, without limitation." Whenever the term "days" is used in this Agreement, it is a reference to calendar days unless that reference specifies it is either a business day or a banking day (as that term is defined in the CBSA).

Operational Matters

7. Fees. Bank will disclose the fees applicable to the Services, and any changes to those fees, via a fee schedule, pro forma, or other method. Client must designate a deposit account as its billing account. Bank will deduct applicable fees from that billing account. If Client closes the billing account without designating a replacement, Bank may select any other deposit account as the new billing account.

8. Accessing Services through Online Facilities. Certain Services may be accessed through an online or mobile application or facility, including but not limited to an online or mobile application providing single sign-on access to one or more Services. Terms and conditions for an online or mobile application or facility may be within this Agreement or may be within a separate agreement or set of terms. If Client accesses any Services through an online or mobile application or facility, the terms applicable to the online or mobile application or facility will govern Client's use of that online or mobile application or facility (including how users log-in to the online or mobile application or facility and how user and administrative entitlements are handled therein), and Part II of this Agreement will govern use of the Services being accessed via the online or mobile application or facility.

9. Proprietary Rights. Bank or Bank's vendors retain all ownership and other rights in the Services, related data, websites, documentation, mobile applications, and software, and in any related trade secrets, copyrights and other intellectual property and proprietary information. Client acknowledges that the Services (and related data, websites, documentation, mobile applications, and software) contain confidential and/or proprietary information that belongs to Bank or Bank's vendors. Client will not disclose or otherwise make such information available to any person other than Client's employees or agents who have a valid need to use the Services on behalf of Client. Client must require its employees and agents to comply with the restrictions on use in this Agreement. These obligations will continue after termination of this Agreement or termination of any Services. Client agrees that Bank may pursue any remedy available at law or in equity to protect its ownership and intellectual property rights and to preserve confidentiality of the Services, including any injunctive relief Bank deems necessary. Client may not take any action or engage in any conduct that violates Bank's rights or the rights of Bank's vendor with respect to the Services.

10. Limited License. Bank grants Client a limited, non-exclusive, and revocable license or sublicense to use the Services, and any related software, websites, or mobile applications, for business purpose activities pursuant to the terms of this Agreement. The Services, including all online services, websites, and mobile applications, and the entire contents, features and functionality (including but not limited to all information, software, text, displays, images, video and audio, and the design, selection and arrangement thereof) of the Services, are owned by Bank, Bank's licensors, or other vendors of such material and are protected by United States and international copyright, trademark, patent, trade secret and other intellectual property or proprietary rights laws. Client must not (a) copy, disassemble, decompile, or otherwise reverse engineer any part of the Services, or (b) remove, obscure, or modify any acknowledgments, credits or legal, intellectual property or proprietary notices, marks or logos contained in the Services or their content. Client may use the Services for Client's own benefit. Client may not copy, reproduce, distribute or create derivative works from the content and agree not to reverse engineer or reverse compile any of the technology used to provide the Services. In the event Client attempts to use, copy, license, sublicense, sell or otherwise convey or to disclose the Services in any manner contrary to the terms of this Agreement, Bank will have, in addition to any other remedies available, the right to injunctive relief enjoining such actions. A separate license agreement (in the form of a "shrink wrap" or "click wrap" agreement with Bank or Bank's vendor) may be required for Client to download or otherwise access the Services or any related websites, software, or mobile applications, and Client acknowledges and agrees that such license agreement will apply to use of the Service, regardless of whether the license agreement is agreed to by an Authorized Individual, a user of the Service, or an administrator of the Service.

11. Representations and Warranties Related to Trust Accounts, Political Organizations, and ERISA. Client acknowledges that inclusion of any account within a Service which is designated as a trust account, escrow account, "for the benefit of" account, political organization account (including, without limitation, a campaign committee account for a candidate for federal, state, or local office or a political action account) or account of similar designation, may result in access to such account (including use of the funds and access to information related to the beneficiaries of such account) by any user entitled to access the account within the applicable Service. To the extent Client requests this type of account to be included in a Service, Client represents and warrants that this inclusion is not prohibited by any agreement applicable to the account or Client, and does not violate any applicable law or any fiduciary or other duty that Client may have with respect to the account. Client assumes all risks associated with including this type of account in a Service, and Client will indemnify and hold Bank harmless from any claims, judgments, damages, costs, liabilities, losses or expenses, including reasonable attorneys' fees and court costs and expenses, that arise directly or indirectly from including this type of account in a Service. Client further represents and warrants that if any account that is subject to the Employee Retirement Income Security Act of 1974 ("ERISA) is included in a Service, Client will indemnify and hold Bank harmless from any liability for any loss of ERISA funds as a result of such inclusion.

12. Service Selections. During implementation of a new Service or modification of an existing Service, certain selections may be made including but not limited to security procedures, transaction limits, Primary Administrator(s), and other options or features relating to the Service. Selections made for a Service will be incorporated into this Agreement and will govern any use of that Service. Any election to use a new Service or modification of an existing Service, as well as certain information relating to Service selections, may be communicated in accordance with the Notice section herein. Client will be bound by the Service selections communicated in accordance with this Agreement and the corresponding fees unless Client notifies Bank of any errors before any subsequent use of the Service. Certain Services require testing, training, or additional documentation that

must be completed; however, Client will be bound by all terms and conditions of this Agreement during any use of a Service, regardless of whether testing, training, or additional documentation has been completed.

13. Equipment, Communications Capabilities and Software. Several of the Services require that Client have adequate, uncompromised, and properly working equipment (including mobile devices, to the extent mobile applications are used or mobile internet access is used), communications capabilities (including email addresses and an internet connection), connectivity, and software (collectively, "technology") in order to use the Service. Client is responsible for providing and maintaining any technology necessary to use a Service. It is Client's responsibility to ensure the integrity and security of the technology and that the technology remains functioning properly and is compatible with Bank's processing environment. Bank will have no responsibility if Client's technology is defective, compromised, or does not remain compatible with, or connected to, Bank's processing environment, even if Client has told Bank what technology Client intends to use or Bank has previously indicated Client's technology was compatible.

14. Electronic Communications. Client's consent to receive electronic communications in the CBSA will also apply to electronic communications related to the Services. By use of any Service on Client accounts, Client agrees to continue receiving such electronic communications; in the event Client wishes to withdraw consent to receive electronic communications, Client must cease use of the Services. It is Client's sole responsibility to provide accurate contact information to Bank (including email address, telephone, and mobile numbers) and promptly notify Bank in the event of any changes to Client's contact information. Client represents and warrants that to the extent Client provides any personal mobile device number to Bank for the purpose of notification relating to a Service, Client has obtained express consent from the owner of the mobile device for such purpose.

15. Alerts and Notifications. Certain Services may provide or allow Client to receive alerts or notifications through email, text message, and/or notifications to a mobile device or through a mobile application ("Alerts"). Client is responsible for providing accurate and up-to-date contact information and proper authority to Bank in order to receive Alerts, and for managing Alert settings within the applicable Service. Alerts are provided as a convenience only and may be subject to lag times, interruptions, or delays in transmission and Bank makes no representation or warranty concerning the availability, currency or accuracy of any Alert. Client remains obligated to review information available within the applicable Service or account statement per the terms of this Agreement, regardless of whether Alerts are received by Client. Message and data rates may apply. Bank is not liable for delayed or undelivered Alerts.

16. Notices. Any notice under this Agreement will be deemed given: (i) to Bank when such notice is received by Client's Treasury Sales Officer, or at such other location or address as Bank may hereafter provide to Client in writing; (ii) to Client when mailed or delivered to Client's current address as shown in Bank's records, emailed to Client at a current email address for Client as shown in Bank's records, or delivered to Client via a Service or through other electronic means, including mobile application messages, messages provided within a Service or posted to a website, and text messages. If Client needs assistance with contact information for a Treasury Sales Officer or does not have an assigned Treasury Sales Officer, Client can call Treasury Solutions Client Support at 800-774-8179 for assistance on sending notice to Bank. At Bank's discretion, communications with Client regarding operational, product-related, procedural, and technical matters relating to the Services may be provided orally and not subject to the notice requirements of this section. Bank may require written confirmation of any notices provided to Bank orally. Bank is authorized to rely on any instructions or information provided by Client until Bank receives notice from Client modifying any prior instructions or information, and Bank has had a reasonable time to act on such notice.

Representatives and Third Parties

17. Authorized Signers. Client will identify individuals with authority to conduct transactions on an account (e.g., issuing checks and payment orders) by executing and submitting signature cards in a form provided by Bank.

18. Designated Representatives. Client will identify individuals with authority to enter into agreements and provide instructions on behalf of Client and delegate any authority regarding the Services through a designation, delegation, or other document provided by Client and acceptable to Bank. Those individuals will be referred to as "Designated Representatives." Bank may act upon any oral or written instruction that the Bank in good faith believes has come from a Designated Representative including any instruction via telephone call, facsimile, e-mail, text message, instant message, or other electronic method. Client will be bound by, and Bank will be deemed to have acted in good faith in accepting, any instruction from a Designated Representative when Bank has authenticated such instruction in accordance with Bank's authentication procedures, using information provided by Client and contained in Bank's records, or when Bank accepts an instruction in reliance on a designated security procedure in accordance with this Agreement.

19. Administrators. Some Services require designation of a "Primary Administrator." A Primary Administrator for a Service has the ability to make certain selections for the Service and to assign and modify entitlements and authorizations for a Service, including creating additional users and users with administrative entitlements ("administrators"), all as more specifically described in Part II of this Agreement with respect to the applicable Service. Primary Administrators may grant entitlements to

additional administrators up to and including all of the entitlements held by the Primary Administrator, meaning that those additional administrators may have the ability to make selections for a Service, create additional administrators, or modify the entitlements of the Primary Administrator. Primary Administrators must initially be designated by an Authorized Individual but given the ability of additional administrators to modify entitlements of the Primary Administrator, the individual designated by Client as Primary Administrator may not retain all of their original administrative entitlements in the Service. Client is bound by any actions of a user who has been granted entitlements within a Service by an administrator, and Client is bound by any actions of users with administrative entitlements that enable them to perform administrative actions including but not limited to acceptance or modification of security procedures, selection of Service-specific dual administration, dual control, or other Service-specific selections, acceptance of additional terms or licenses (such as click-wrap terms) relating to a Service, and granting of access and entitlements to the Service. Client is responsible at all times for ensuring that Client's current administrators review and modify the entitlements and access of any previously designated user or administrator as necessary. Removal or replacement of a user or administrator in any agreement or other documentation provided to Bank may not result in automatic removal of the user or administrator's entitlements within a Service. Refer to applicable reference materials for details regarding the Primary Administrator role, other authorized user roles, and the entitlements that different roles may include.

20. Third Parties. Client may authorize third party processors and other agents ("Third Parties") to issue instructions to Bank, provide information to be used relating to Services, or use the Services on the Client's behalf. Bank may in its sole discretion require documentation from Client, the Third Party, or both, to evidence the Third Party's authority with respect to Client's accounts and Services. Client remains responsible for any actions of its Third Parties, whether or not Client has provided notice to Bank of Client's use of such Third Parties. In addition, some Services may provide access to information about Client's accounts at other financial institutions or entities ("Other FIs") or may allow reporting of information about Client's accounts with Bank to an Other FI. Bank makes no representations and assumes no liability with respect to the correctness, accuracy, completeness, integrity, or timeliness of any information (i) received from any Third Party or Other FI or (ii) any use or disclosure of information provided to a Third Party or Other FI. Bank is not responsible for any Service errors or delays caused by Third Parties or Other FIs.

21. Authority for Other Entities. If Client requests accounts owned by another entity to be associated with or accessed in connection with Client's Services, Client represents and warrants that Client has authority (granted by a duly authorized representative of the owner of the account(s)) to access the accounts and perform transfers of the funds contained therein, regardless of whether Bank requires further proof of, confirmation, or documentation relating to Client's authority with respect to the accounts of the other entity. Client further agrees that the provisions of this Agreement will apply to those accounts accessed by or associated with the Services to the same extent as if Client owned the accounts. Client agrees to indemnify and hold Bank harmless from any and all claims or losses that arise as a result of Bank complying with Client's request to add or associate accounts to Client's Services.

22. Bank's Vendors. Bank may delegate any duties under this Agreement to one or more affiliates, agents or vendors of Bank without notice to or consent of Client. Bank will be responsible for the performance of such providers to the same extent as if Bank were providing the applicable Service(s) directly.

23. Client's Vendors. Any third party servicer or vendor used by Client in connection with any Service will be deemed Client's agent. Client will be liable for (i) such vendor's failure to comply with requirements of this Agreement, (ii) all fees, costs and expenses of such vendor, and (iii) any claims, damages, costs and expenses incurred as a result of such vendor's performance or non-performance.

24. Courier or Messenger Services. For any courier or messenger services Bank provides to Client, Client understands and agrees that (a) the courier is Client's agent and not an agent of Bank; (b) deposits collected by the courier or messenger are received by Bank when the deposits have been delivered to a teller at Bank's premises or a location that is eligible and designated by Bank to receive deposits; (c) negotiable instruments collected by the courier or messenger are paid at Bank when delivered to the courier or messenger; and (d) transactions conducted by a courier service are not insured by the FDIC.

25. Assignment. Client may not assign this Agreement or any Services to a third party without Bank's prior written consent, which will not be unreasonably withheld, provided that Client and/or third party may be required to execute any documentation deemed necessary by Bank as a condition of the written consent of Bank. Bank may assign this Agreement to any of Bank's affiliates or successors in interest, without notice to or consent from Client. In the event Client objects to any such assignment, Client may terminate this Agreement or any Services immediately upon written notice to Bank.

26. Hardware and Security Credentials. Client is responsible for maintaining the confidentiality and security of Client's computer or mobile device, as well as access passwords, account numbers, log-in information, and any other security or access credentials or information used to access or related to the Services (the "security credentials"). Client is also responsible for preventing unauthorized access to computers or mobile devices used to access the Services. **Bank strongly recommends that Client use secure encryption, secure browsing software, and other available security technology to protect Client's computer and mobile environments.** Bank will not be responsible for any errors, deletions, or failures that occur as a result of any malfunction of Client's computer or mobile device, nor will Bank be responsible for any computer virus or malware that affects Client's computer or mobile device while using a Service.

27. Security Procedures. The security procedures Bank offers to Client are designed to control access to the Services and verify the authenticity of instructions provided to the Bank. The security procedures are not designed to detect errors in the content of instructions or information transmitted to the Bank, including but not limited to intended account numbers of Client, account numbers not belonging to name of recipient, and erroneous or fraudulent instructions provided to Client by another party. Security procedures may include, but are not limited to, access credentials (including username, user ID, password, or other log-in information); authorization codes or tokens used to log in to a Service or initiate or approve any transactions initiated within a Service; and procedures to verify or authenticate transactions (including dual control requirements). Client agrees that use of any Service constitutes acceptance of the security procedures for that Service, as described in Part II of this Agreement with respect to that Service, and agrees that the security procedures are commercially reasonable for Client's use of the Service, including the size, type, and frequency of any possible transactions that may be initiated from Client's accounts that may be associated with the Service now or in the future. Client agrees to be bound by, and Bank is authorized to rely and act upon, all Service initiation, access, and instructions accepted by Bank in good faith and in compliance with the applicable security procedures, whether or not Client (or a user, administrator, or Designated Representative of Client) actually gave Bank those instructions. If Client believes any security procedure is inadequate, Client may terminate the Service immediately upon notice to Bank. Client agrees to comply with additional security procedures that may be implemented by Bank for a particular Service from time to time. Client is responsible for controlling access to and maintaining the confidentiality of the details related to the security procedures and Client must immediately report to Bank as soon as Client becomes aware of any (i) suspected breach of that confidentiality, (ii) compromise of any security procedure, or (iii) need to revoke any access credentials or authorization codes. Client's failure to control access to and maintain confidentiality of the security procedures, or failure to notify Bank as required herein, may result in improper use of the security procedures to access a Service or initiate transactions. Subject to applicable law, Client will be responsible for any transaction or losses relating to access to a Service resulting from such improper use of security procedures, provided Bank has complied with its obligations herein, and Client agrees that Bank will have no liability for any loss, claim, or damage Client sustains as a result of the improper use of the security procedures.

28. Bank's Policies and Procedures. Client agrees that Bank's internal policies or procedures are for Bank's sole benefit and do not impose any higher standard of care or duty upon Bank. Client cannot claim any reliance on any such policies or procedures.

29. Liability. To the extent permitted by law, Bank's liability under this Agreement will be limited to direct losses suffered by Client caused directly by Bank's gross negligence or willful misconduct in performing its obligations under this Agreement, which liability will not exceed the sum of fees and charges imposed for Services provided to Client for a period of one year. Notwithstanding the foregoing, if Bank's failure to exercise ordinary care results in an unauthorized, delayed, or erroneous Payment Order, as defined in Article 4A of the Uniform Commercial Code of the state whose law is applicable to this Agreement (the "UCC"), Bank will be required to reimburse Client the amount of the loss of funds relating to Bank's failure, plus the amount of interest losses (calculated using the daily Federal Funds rate published by the Federal Reserve Bank of New York) attributable to such failure, according to the terms of the UCC. Bank's liability for Client's direct losses will be reduced to the extent any losses are the result of Client's failure or breach of Client's obligations under this Agreement, including any failure to mitigate damages. If Bank reimburses Client for any losses or damages, Client agrees to transfer all rights relating to the transactions in question to Bank and to reasonably assist Bank in any efforts or legal actions that Bank may take to recover those amounts from any third party.

30. Indemnification. Client will indemnify and hold Bank and its affiliates, subsidiaries, officers, directors, and employees harmless against any claim, loss, damage, deficiency, penalty, cost, or expense, including litigation expenses, other costs of investigation or defense, and reasonable attorney's fees resulting from: (a) any breach or default by Client in the performance of this Agreement; (b) any negligence or willful misconduct of Client; (c) incorrect, incomplete, or inaccurate data or information furnished by Client to Bank; and (d) any action taken by Bank (i) at the direction of Client or a Third Party or other agent of Client, or (ii) per any instruction authenticated in accordance with the requirements for that instruction or the Service to which the instruction relates. Client's duty to indemnify and hold Bank harmless will be reduced by the extent to which Bank's breach of this Agreement, gross negligence, or willful misconduct contributed to any losses.

31. Disclaimer of Warranties. The Services are provided "as is", and Bank makes no representations or warranties of any kind (i) that the operation of any Service will be continuous, uninterrupted, or error-free, (ii) that the Services are free of defects, (iii) that the Services or any associated websites, mobile applications, or software are free of viruses, disabling devices or other harmful components, or (iv) that any information or reports that are transmitted over the internet, a wireless network, or sent by e-mail or other electronic method will remain confidential or remain accurate and unaltered when received or accessed by Client. **To the maximum extent permitted by law, Bank also disclaims all representations and warranties of any kind, whether express, implied or statutory, in connection with the Services and any related websites, software, or other equipment Bank may provide, including implied warranties of merchantability, fitness for a particular purpose, title and non-infringement.**

32. Liability Provisions Related to Government Entities. Any indemnification obligation in this Agreement will not apply to a government entity Client to the extent such obligation is limited or prohibited by applicable law. Notwithstanding the foregoing, a government entity Client will otherwise remain financially and legally responsible and liable to Bank for all obligations it incurs under this Agreement, including but not limited to any overdrafts in an account, and Bank specifically reserves all other rights with respect to the government entity Client.

33. Remedies. The rights, powers, remedies and privileges provided in this Agreement are the sole and exclusive rights, powers, remedies and privileges of both parties with respect to the Services.

34. Force Majeure. Client agrees that Bank will not be liable with respect to any error, delay or failure to perform caused by (i) fire, flood, natural disaster, strike, civil unrest, terrorism, failure of computer or communications facilities that Bank does not control, (ii) acts or omissions of any third party including any Federal Reserve Bank, clearing house or funds transfer system, or (iii) any other circumstance beyond Bank's reasonable control, or with respect to matters for which Bank has not specifically assumed responsibility under this Agreement.

35. Fraud Detection/Deterrence. Bank may recommend certain Services to Client that are designed to detect/deter fraud, help Client to identify and reject potentially fraudulent transactions, or generally reduce the likelihood that certain types of fraudulent transactions will occur. Client agrees that if Client fails to implement any of these Services which are recommended by Bank (whether before or after Client suffers a loss of the type that could be prevented by the Service), Client will be precluded, from and after the date that Client declines the Service, from asserting any claims against Bank with respect to any losses for any unauthorized, altered, counterfeit, or other fraudulent transactions that the rejected Service was designed to detect or deter. In addition, Bank will not be required to re-credit Client's account or otherwise have any liability for such transactions as long as Bank has otherwise satisfied its duty of care with respect to the transactions and Services.

Part II: Service-Specific Terms and Conditions

ACH Fraud Control Service

1. Description of ACH Fraud Control Service. The ACH Fraud Control service is an internet-based solution with the following components: ACH Positive Pay, ACH File Control Totals, ACH Warehouse Search, ACH Blanket Block Option, Standing Order Option, and Single Entry Option. ACH Positive Pay enables clients to authorize which received Automated Clearing House (ACH) transactions post to Client's Truist deposit account. ACH File Control Totals enables Clients using ACH Origination via file transfer to input file control totals online and receive real time file processing status notifications. ACH Warehouse Search enables Clients to inquire on received or originated ACH transactions. The ACH Blanket Block, Standing Order, and Single Entry Options restrict ACH transactions from posting to the applicable account as described below. Client's use of services relating to receipt or origination of ACH debits or credits ("ACH entries") is subject to these terms and conditions, the ACH Origination terms and conditions (as applicable), and the Nacha Operating Rules ("Rules") governing the ACH Network. **The Nacha Operating Rules may be obtained through www.nacha.org.**

2. Designation of Primary Administrator. Client must designate a Primary Administrator for the ACH Fraud Control service.

3. Selection of ACH Fraud Control Service Options. Client may select various service options for each account in the ACH Fraud Control service setup. The options available are as follows:

    a. ACH Positive Pay.

        i. The ACH Positive Pay feature allows Client to create authorizations to allow particular ACH debit and credit entries to post to an account, and to review ACH entries received that are initially blocked and make a decision to post or return the entries.

ii. Client shall establish ACH authorization criteria (in a manner and format, and containing such information, as required by Bank) for ACH debit or credit entries that Client intends to be received for each deposit account. When an ACH entry is received that matches an authorization, the entry will post to the account in accordance with Bank's current processing procedures and in accordance with the Rules. When an ACH debit or credit entry is received that does not match an ACH authorization, that entry will initially reject, as a "rejected entry." Each rejected entry will be suspended for a period of time for Client to review and decide whether to return that entry or to allow that entry to post to the account.

iii. Until the applicable decision deadline, entitled users may either authorize the rejected entry to post or return the entry to the originator. If Client fails to notify Bank by the decision deadline of its decision concerning a rejected entry, Bank will not post the entry to Client's account and will return the entry.

iv. Client is responsible for having up-to-date and accurate authorizations in effect at all times for all ACH entries that Client intends to allow to post to Client's accounts. Bank shall have no liability for posting ACH entries which match a current authorization, or for any rejected entries that are returned to the originator, so long as Bank otherwise processes the ACH entries in accordance with these terms and conditions and Bank's current processing procedures.

v. In the event the ACH Positive Pay feature is unavailable, Bank will use reasonable efforts to provide information to Client with respect to rejected entries, and to allow Client to provide authorization or return decisions to Bank. Client acknowledges that when the ACH Positive Pay feature is unavailable, an entry that Client has not previously authorized, but that Client may have otherwise approved through the service, may be rejected.

vi. When an ACH authorization expires or service is terminated for any reason, Bank will no longer be obligated to monitor entries against such authorization criteria provided by Client and Bank will receive and accept or return ACH entries to Client's account in accordance with Bank's current procedures and the Rules.

b. Verification. If Client elects to use the verification feature (which may also be referred to as dual approval or dual administration in applicable reference materials) for requests to create, modify, or delete an authorization or to make decisions pertaining to a rejected transaction, a second user with sufficient entitlements must approve these actions. In order to use the verification feature, an ACH Fraud Control administrator must set up a user with the appropriate "verification" permission in ACH Fraud Control. **Bank strongly recommends that Client use the verification feature.**

c. Alerts. Certain alerts are available within the ACH Fraud Control service, including alerts when an ACH entry received for posting was rejected; when an ACH entry posted because it matched an authorization; when a decision for a rejected entry or an authorization maintenance request needs to be approved; and when a decision has been made or modified, or an authorization has been created, deleted or changed. The Primary Administrator of the service will designate which users are to be sent an alert and which alert(s) each user is to be sent. Client is responsible for establishing alert notification preferences for users, and for users' monitoring of alerts and taking action as necessary.

d. ACH File Control Total.

i. The ACH File Control Total feature allows Client to submit control totals to Bank in order to release ACH files for processing, when Client uses Bank's ACH Origination service and submits ACH files to Bank via file transfer.

ii. Client is responsible for submitting valid ACH control totals via the ACH File Control Total feature in a manner and format acceptable to Bank when submitting ACH files to Bank for processing.

iii. Client is responsible for establishing email notification preferences and monitoring notifications which provide file processing acceptance, suspension, and user statuses for the ACH File Control Total feature.

e. ACH Warehouse Search.

i. The ACH Warehouse Search feature allows a user to view ACH transaction entries that have been received and posted to a deposit account and to view ACH file, batch and transaction details that Client has originated through Bank's ACH Origination service.

ii. ACH received transaction information and ACH Origination file, batch and transaction information will be maintained and made available for view through ACH Warehouse Search in accordance with Bank's applicable retention schedules.

f. ACH Blanket Block Option. This option allows Client to block the posting of all incoming ACH debit and/or credit entries to a designated account. Client can opt to block only incoming ACH debit entries, only incoming ACH credit entries, or both

incoming ACH debit and credit entries. Client will not have the opportunity to decision rejected entries; instead, any entries which are blocked by this option will be returned automatically.

g. Standing Order Option. This option allows Client to generally block all incoming ACH debit entries from posting to a designated account, but allows Client to authorize one or more incoming ACH debit entries from a known source/originator(s) to post to the account on a repetitive or "standing" basis. Client will not have the opportunity to decision rejected entries; instead, any entries which do not match an authorization will be returned automatically.

h. Single Entry Option. This option allows Client to generally block all incoming ACH debit entries from posting to a designated account, but allows Client to authorize particular ACH debit entries from a known source/originator to post to the account on a one-time or "single entry" basis. Once the Bank has posted an entry to which a single entry authorization applies, that authorization will expire and the Bank will block any future instance of that entry unless Client establishes a new authorization to allow that future instance. Client will not have the opportunity to decision blocked or rejected entries; instead, any entries which do not match an authorization will be returned automatically.

4. ACH Debit Entries Sent by Bank or Bank's Vendors. If Client uses an account setup for the ACH Fraud Control service to settle incoming ACH debit entries for certain transactions with Bank or with certain of Bank's third party vendors, then Client must specifically authorize those entries through the service. Examples of these ACH debit entries include Cash Concentration service debits, automated loan and lease payments, check order payments, merchant card settlements, collections, and transfers. Client is responsible for having up-to-date and accurate authorizations in effect for all ACH entries Client intends to post to Client's accounts, including incoming ACH debit entries for transactions with Bank or Bank's vendors. If Client fails to authorize entries for these transactions, then such entries may be blocked and Client may incur additional fees, interest and charges. Note that in some cases, due to Bank's system configurations, incoming ACH debit entries for certain transactions with Bank or Bank's vendors may still post to Client's account, even if Client has not authorized those entries through the service**.**

5. Reversals, Returns and Adjustments. In accordance with the Rules, ACH reversals will automatically post to Client's account regardless of any options or blocks on the account. Bank may also return an ACH entry for any reason that an entry may be returned under the Rules or under this Agreement, and Bank may post any entry, reversal or adjustment to the applicable account which Bank is required to accept under the Rules or any other applicable rule, guideline or regulation.

ACH Origination Service

1. Description of ACH Origination Service. The Automated Clearing House ("ACH") Origination service allows Client to initiate debit and/or credit entries through the ACH network, a funds transfer system for sending and settling electronic entries among participating financial institutions. Details regarding functionality, formatting, and other technical requirements that Client must follow when using the service are provided in the ACH Origination reference materials.

2. Functioning of the ACH Origination Service. Under the ACH Origination service, Bank acts as the originating depository financial institution ("ODFI") with respect to entries that Client sends Bank, or entries that are sent to Bank for processing on Client's behalf. Client is the "originator" for these entries. Client agrees to comply with and be bound by all current Nacha Operating Rules & Guidelines ("Rules") which govern the ACH network, including without limitation, Client's obligation under the Rules to establish, implement, and annually review risk-based processes and procedures designed to identify and prevent fraudulent entries such as those induced by impersonation or under false pretenses (e.g., business email compromise). **The Nacha Operating Rules may be obtained at www.nacha.org.** If Client fails to comply with the Rules, certain fines or penalties may be imposed by Nacha; Client authorizes Bank to debit Client's designated account for any such fines or penalties without prior notice. In the event of any conflict between any term used or defined in both these ACH Origination terms and conditions and the Rules, the definition in the Rules shall apply. Client's use of a third-party service provider or processor with respect to Client's ACH Origination service is subject to Bank's prior approval and any additional documentation required by Bank. If Bank permits Client to use a third-party service provider or processor, then each reference in these ACH Origination terms and conditions to "Client" includes such third-party service provider as appropriate. Client is solely responsible for its third-party service provider's compliance with these terms and conditions.

3. Definitions. Terms that are defined in the Rules have the meanings given to those terms in the Rules. The following terms have the specified meanings for purpose of these ACH Origination terms and conditions:

a. "Authorized representative" means an individual that may be designated by Client to provide instructions (including but not limited to control totals) to Bank relating to Client's ACH Origination service.

b. "Batch" means entries that have been grouped together and that have the same effective entry date, the same Standard Entry Class (SEC) Code, and that settle to the same designated account.

c. "Cut-off deadline" means the time on a banking day by which Bank must receive an entry in order for it to process on that day. The cut-off deadline is established by Bank and may be changed at Bank's discretion.

d. "Designated account" means the account(s) designated by Client for settlement of ACH Origination activity.

e. "File Transfer" means the secure transmission of files to and from Bank using an internet browser or a secure FTP (File Transfer Protocol). The File Transfer method of transmission of ACH Origination entries to Bank may also be referred to elsewhere as ACH Origination by "direct transmission."

f. "Instruction" means any direction relating to an entry that Bank receives from an authorized representative, including requests to cancel an entry.

g. "Nacha" means the National Automated Clearing House Association.

h. "On-us entry" means an entry originated by Client to credit or debit an account maintained with Bank, which Bank elects to process as an on-us entry (as described in Section 6 below) rather than processing via the ACH network.

4. Transmitting Entries to Us. Client may transmit ACH credit and/or debit entries and instructions to Bank through one of Bank's online services which allows for ACH Origination, or by File Transfer to Bank (each method an "ACH Origination channel"). All entries must comply with (i) the requirements of the applicable ACH Origination channel, (ii) the requirements of, and be identified by the appropriate SEC Code, and (iii) applicable Nacha record format specifications and any requirements set forth in the ACH Origination reference materials. Client agrees that it is solely responsible for the accuracy and authorization of all entries submitted to Bank and will verify all entries through Client's internal fraud monitoring procedures. Bank may at any time prohibit Client from originating certain types of ACH entries or may restrict origination of certain entries via ACH Origination channels. Client must, for at least three (3) banking days after the effective entry date of an entry, retain all data on any file transmitted to Bank that would be required to reprocess an entry.

5. Obligations of a Third-Party Sender or Third Party Service Provider. Client must obtain Bank's approval, and execute any additional documentation or provide any additional documentation that Bank may require, before acting as a third-party sender or third-party service provider for ACH Origination, as such terms are defined in the Rules. If Client sends Bank any entries as a third-party sender or third-party service provider, Client automatically makes the additional representations and agrees to requirements for third-party senders specified in the Rules, and agrees to provide the Bank any information required to comply with the Rules. In addition to all other requirements for ACH Origination contained within these terms and conditions, the following requirements apply to Client to the extent Client sends any entries to Bank as a third-party sender or third-party service provider:

a. Client will not transmit entries on behalf of any originator until (1) Client has obtained Bank's approval of such originator, which approval is subject to Bank's policies and procedures, and either (2) such originator and Bank have entered into an agreement for Bank to provide ACH Origination service to the originator and the originator agrees to be bound by the Rules, or such originator has entered into an appropriate agreement with Client containing such provisions as may be required by the Rules and/or Bank, and under which such originator is bound by the Rules.

b. Bank may impose additional risk exposure limits for a Client acting as a third-party sender or third-party service provider and may monitor entries transmitted to Bank relative to the applicable exposure limits, across multiple settlement dates.

6. Bank's Processing of Entries. Except as provided later in this section with respect to on-us entries, Bank will process entries and instructions Bank receives from Client and then transmit those entries as the ODFI to an ACH operator in accordance with the terms herein. Bank will only accept entry files that pass Bank's system edit. Bank will transmit the entries to the ACH operator by its deadline prior to the effective entry date shown in the entries as long as the ACH operator is open for business on that day and Bank receives the entries (a) prior to Bank's cut-off deadline and (b) with a sufficient number of days (as specified in the ACH origination reference materials) to meet the effective entry date shown in the entries. For entries that Bank receives after those times, Bank will use reasonable efforts to transmit such entries by the ACH operator's next deadline on a banking day on which the ACH operator is open for business. If Bank chooses to process an entry as an "on-us" entry, then Bank will credit or debit the receiver's account subject to the same cut-offs and conditions stated above. For an entry that Bank chooses to process as an "on-us" entry that Bank receives after those cut-off times and deadlines, Bank will use reasonable efforts to credit or debit the receiver's account on the banking day following such effective entry date. If the effective entry date of any entry Bank receives from Client is not a banking day, Bank will process that entry on the banking day following the requested effective entry date. In Bank's sole discretion, Bank may verify or authenticate any entry or file by any method chosen by Bank, but Bank is under no obligation to do so. If Bank is unable to verify or authenticate an entry or file, then Bank may refuse to process such entry or file.

7. Exposure Limits and Pre-Funding. Bank reserves the right to establish and change aggregate and individual dollar limits or "exposure limits" for Client's ACH Origination service entries and files. Such limits are internal limits established to monitor Bank's risk exposure to Client, and Bank may in its sole discretion, but is not required to, share such limits with Client. Bank may refuse to process entries or files that exceed the applicable exposure limits or may, in Bank's sole discretion, process such entries or files. Bank also reserves the right to change the terms upon which Bank provides ACH Origination service to Client at any time if Bank believes Client's financial condition or usage of the ACH Origination service warrants such a change, including requiring that Client pre- fund all ACH credit entries. Pre-funding means that Client must have available, collected funds in Client's designated account in an amount equal to all credit entries Client has submitted to Bank. Bank will place a hold upon the funds in the amount of all credit entries when Bank receives Client's file containing ACH credit entries. The held funds will then be withdrawn from Client's account and used to fund the ACH credits.

8. Suspension and Rejection of Entries. Bank may suspend processing of and/or reject an entry, batch or file that (a) does not comply with the Rules or these ACH origination terms and conditions, or any applicable formatting requirements; or (b) contains an effective entry date more than 45 calendar days after the day Bank receives such entry, batch or file. Bank may suspend processing of and/or reject an "on-us" entry for any reason that would allow that entry to be returned under the Rules or these terms and conditions. Bank may also suspend processing of and/or reject an entry, batch, or file if Client fails to comply with any of Client's obligations under these ACH Origination terms and conditions, including Client's obligation to maintain sufficient balances in the designated account(s). Bank may suspend processing of and/or reject an entry, batch or file without giving notice to Client.

9. Cancellation and Amendment of Entries. Client may request cancellation of an entry through certain online services or by another method as communicated to Client by Bank. In Bank's sole discretion, Bank may verify or authenticate cancellation instructions by any method chosen by Bank, but Bank is not obligated to do so. If Bank is unable to verify or authenticate a cancellation instruction, Bank may refuse to act upon such instruction. Bank has no obligation to honor or process any instructions from Client to cancel or amend an entry once Bank has received that entry. However, as an accommodation to Client, Bank will use good faith efforts to attempt to honor Client's instruction to cancel (but not to amend) an entry if (a) the instruction complies with any applicable requirements Bank may impose and (b) Bank receives such instruction at a time and in a manner that gives Bank a reasonable opportunity to act on it prior to transmitting the entry to the ACH operator or, in the case of an "on- us" entry, prior to crediting or debiting the entry to the receiver's account. Bank is not liable if a request or any attempt to cancel an entry is not successful. Client agrees to reimburse Bank for any expenses Bank may incur in attempting to honor Client's cancellation instruction.

10. Name and Account Number Inconsistency. Client must ensure the accuracy of Client's entries and instructions. If an entry describes the receiver inconsistently by name and account number, payment may be made by the RDFI (or, for an on-us entry, by Bank) solely on the basis of the account number, even if that number is associated with an account owned by a person other than the named receiver according to the RDFI's records. Bank shall have no liability for any losses associated with such inconsistency. Client is responsible for any loss associated with such inconsistency and Client's obligation to pay Bank the amount of the entry is not excused in such circumstances.

11. Notice of Returned Entries. Bank will give Client notice via the online service Client uses, or by another means, promptly after Bank receives a returned entry from the ACH operator, and Client may be charged a fee for these notices. The type of notice used will be selected during implementation of the service, or in some cases, the type of notice may be dependent upon Client's ACH Origination channel. If Client elects the Representment option of the ACH Origination service, Bank will retransmit certain types of returned entries in accordance with the Rules. Except in the case of entries retransmitted under the Representment option, Bank is not obligated to retransmit any returned entry that Bank originally transmitted in compliance with these ACH Origination terms and conditions, and if Client wants Bank to retransmit any such entry to the ACH Operator, Client must retransmit the entry to Bank.

12. Notifications of Change. Promptly after Bank receives a notification of change relating to one of Client's entries, Bank will give Client notice of the notification of change via the online service Client uses, or by another means; Client may be charged a fee for these notices. The type of notice used will be selected during implementation of the service, or in some cases, the type of notice may be dependent upon Client's ACH Origination channel. Client agrees to make the required change(s) prior to submitting any further entries to the applicable receiver's account.

13. Security Procedures. The security procedures for the ACH Origination service are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.

    a. Control Totals. For ACH entries sent to Bank via File Transfer, Client is required to verify the total dollar amounts for all debit entries and, separately, for all credit entries contained in each file by submitting to Bank the total dollar amount for each, or the "control totals." The file will not be released for processing until an accurate control total is submitted. Except for files transmitted in or to be converted into an EDI format, Client must submit control totals through either the

ACH File Control Total feature of the ACH Fraud Control service, or Bank's ACH Control Total Verification ("ACTV") system. Control totals submitted via ACH File Control Total or ACTV must comply with the requirements of the respective method of submission. If Client's file is transmitted in or to be converted into an EDI format, Client's authorized representative will be required to provide control totals to Bank according to the method required by Bank. If Client uses a third-party service provider or processor to send entries to Bank via File Transfer in a file that also contains entries being initiated on behalf of other clients of the third-party service provider, then Client's third-party service provider may provide Bank control totals on an aggregate basis for all entries contained in that file.

b. Online Services. For ACH entries that are transmitted to Bank through one of Bank's online services, Client is required to comply with the applicable security procedures for that online service, as set forth in the terms and conditions for the online service.

c. File Transfer. For entries transmitted by File Transfer, a logon record with a unique ID and password is required. The ID and password are provided to Client at the time of establishment of the File Transfer application. If Client uses a third-party payment provider or processor that sends Client's entries to Bank via File Transfer in a file that also contains entries being initiated on behalf of other clients, then Client's third- party service provider will use the ID and password that Bank issues directly to the provider.

14. Security Requirements. Client is required to establish, implement, and, as appropriate, update security policies, procedures, and systems related to the initiation, processing, and storage of entries. These policies, procedures and systems must:

    a. protect the confidentiality and integrity of Protected Information (as defined in the Rules) until its destruction;

    b. protect against anticipated threats or hazards to the security or integrity of Protected Information until its destruction; and

    c. protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

    Such policies, procedures and systems must include controls that comply with applicable regulatory guidelines on access to all systems used by Client to initiate, process and store entries.

    In addition, if Client's total ACH origination or transmission volume (including Client's volume through Bank as well as any other financial institution) exceeds the applicable threshold in the Rules, Client must protect depository financial institution account numbers used in the initiation of entries by rendering them unreadable when stored electronically, as more specifically described in the Rules.

15. Payment for Entries. Client must pay Bank the amount of each credit entry Bank originates on Client's behalf and Bank will pay Client the amount of each debit entry that Bank has originated on Client's behalf, all at such times as Bank may determine and in accordance with the Rules. Client must also pay Bank (at such time as Bank may determine) the amount of each debit entry Bank has originated on Client's behalf that is returned by the RDFI. Bank may, without notice or demand, and Client authorizes Bank to, (a) debit any designated account for amounts that Client owes Bank under these ACH Origination terms and conditions and (b) credit any designated account for the amount of (i) originated debit entries and (ii) returned entries previously debited from any designated account. Client must at all times maintain sufficient collected funds in the designated account(s) to cover Client's payment obligations to Bank. If Client's obligations to Bank at any time exceed such funds in the designated account(s), Bank may refuse to process entries and suspend the ACH Origination service until Client deposits sufficient funds and/or Bank may debit or place a hold on funds in any account Client maintains with Bank. Bank has the right to net any amount Bank owes Client against obligations Client owes to Bank.

16. Representations for all Entries. Client makes the following representations to Bank with respect to each entry Client sends Bank:

    a. the receiver designated in the entry authorized Client to initiate the entry to credit or debit its account in the amount and on the effective entry date of the entry,

    b. the receiver's authorization is and will remain effective until the receiver's account is debited or credited,

    c. the entry conforms to Client's obligations under the Agreement, these ACH Origination terms and conditions, the Rules, and the ACH Origination reference materials,

    d. the entry complies with and does not violate applicable laws and regulations (including those relating to sanctions programs), and

    e. Client has performed a reasonable examination of Client's receiver relationships to identify transactions with those receivers which must be originated using the IAT SEC Code.

Client agrees to be bound by the Rules and acknowledges that payment of an entry by the RDFI to the receiver is provisional until the RDFI receives final settlement for such entry and that, if such settlement is not received, the RDFI will be entitled to a refund from the receiver of the amount credited and, in such case, Client will not be deemed to have paid the receiver the amount of the entry.

For each entry that Client sends Bank, Client warrants that the entry uses the appropriate SEC Code, and meets all requirements for that SEC Code as set forth in the Rules, including but not limited to the following: (i) the entry was properly authorized per the requirements for the applicable SEC Code, (ii) Client will retain a copy or evidence of the authorization as required by the Rules for the applicable SEC Code, (iii) Client will verify any information relating to the entry and perform any fraud prevention or other obligations as required by the Rules for the applicable SEC Code, and (iv) Client makes any representations or warranties relating to the entry as required by the Rules.

17. International ACH Transaction (IAT) Entries. If Client sends Bank an IAT entry, Client represents and warrants to Bank and agrees:

    a. The entry will be identified by, and will comply with the requirements of, the IAT SEC Code, including complying with all Nacha record format specifications for the IAT entry.

    b. If Client originates an entry using another SEC Code and Bank determines in good faith the entry should have been originated using the IAT SEC Code, in addition to any other rights Bank may have, Bank may suspend the processing of and/or reject the entry (or batch or file containing the entry) and Bank may also suspend and/or terminate Client's ACH Origination service immediately without prior notice. Similarly, a gateway operator or ACH operator may suspend the processing of and/or reject an entry that it determines should have been originated as an IAT entry.

    c. Client is in compliance with, and the entry complies with, all applicable United States laws and regulations, including sanctions and other programs administered by the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC) and Financial Crimes Enforcement Network (FinCEN).

    d. Client is in compliance with, and the entry complies with, the laws, regulations, and payment system rules of the receiving country, including any requirement to obtain the receiver's written, oral, or electronic authorization, for the receiver's authorization to be validly signed, for the receiver's authorization to be in proper form to authorize the foreign RDFI to debit the receiver's account, to provide notice of the entry prior to it settling in the receiver's account, to provide notice to the receiver of the receiver's recourse and other provisions relevant to the receiver, and to obtain a separate authorization from the receiver for each debit entry initiated at sporadic times, instead of set intervals.

    e. In addition to any other rights Bank has, if Bank suspects or determines that the entry does not comply with any applicable laws or regulations, the Rules, or any other payment system rules (including those laws and regulations relating to sanctions programs), Bank may suspend processing of and/or reject the entry and hold funds debited from or to be credited to Client's account for the entry.

    f. Client will maintain either the original or a copy of any authorization required from the receiver for the entry for the longest period of time Bank may be required to produce that authorization under any of the Rules, the laws and regulations of the U.S., and the laws, regulations, and payment system rules of the receiving country. Client will provide a copy or evidence of the authorization required from the receiver of the entry within a reasonable time upon Bank's request.

    g. If the entry is an outbound IAT entry, Client authorizes the gateway operator to transmit the entry to the foreign gateway operator and to arrange for the settlement of the entry with the foreign gateway operator, for further transmission to, and settlement with, the foreign RDFI for credit or debit of the amount to or from the receiver's account.

    h. If the entry is an outbound IAT entry and Bank does not have an agreement for processing IAT entries with the domestic RDFI that serves as the gateway operator for the entry, it may result in either Bank or the gateway operator suspending the processing of and/or rejecting the entry or the batch or file in which the entry is contained.

    i. Client bears sole responsibility for all losses and other risks relating to foreign exchange conversion with respect to the entry.

    j. In addition to any other indemnity obligations Client has under this Agreement or these ACH Origination terms and conditions, Client will defend, indemnify, protect and hold Bank, Bank's affiliates, and Bank's officers, directors, employees, attorneys, agents, and representatives harmless from and against any and all liabilities, claims, damages, losses, demands, fines, judgments, disputes, costs, charges, and expenses which relate in any way to (i) any IAT entry (or requests or instructions related to an IAT entry) Client sends to Bank that does not comply with all applicable laws and regulations, the Rules, and the payment system rules of the receiving country, or (ii) any breach of any representation, warranty, or agreement Client has made related to an IAT entry. Without limiting the foregoing, Client agrees that Client

is liable for and will reimburse Bank for all amounts that may be erroneously paid by Bank or any receiving bank in respect of any entry erroneously credited or debited by Bank or any receiving bank pursuant to any IAT entry Client originated, or related instructions of Client and any claim paid by Bank (including any claim for interest) as a result of a declaration of a receiver or other person alleging that an IAT entry was not originated in accordance with the receiver's authorization, the receiver's authorization was revoked, a required notification was not given in sufficient time before the entry was processed to the account of the receiver, or no valid authorization ever existed between the receiver and Client.

k. Due to IAT entry processing requirements, processing of an IAT entry may be delayed or suspended. Any such delay or suspension may affect the settlement of and availability of funds for an IAT entry. Client must transmit IAT entries to Bank in files comprised solely of IAT entries. In addition to any other limits on Bank's liability, Bank will not have any liability for any delay in or suspension of processing or rejection of an IAT entry or file containing an IAT entry, in accordance with Bank's processing requirements for IAT entries or applicable law, or for the actions of any third parties (including any gateway operator or ACH operator) resulting in the delay in or suspension of processing or rejection of an IAT entry.

l. A gateway operator may return the entry after the period of time for the return of an IAT entry provided in the Rules, and Client agrees Bank may settle that return to Client's designated account.

18. Proof of Authorization. Within five (5) days of Bank's request, Client will provide Bank with an accurate record evidencing the receiver's authorization (or in the alternative, Client's contact information, when permitted by the Rules).

19. Audit Rights. At any time, upon two days' prior notice, Bank may perform a remote or onsite audit of Client's systems, procedures, controls, and records as Bank deem necessary to determine Client's compliance with the Rules and these ACH Origination service terms and conditions. Client will provide Bank with reasonable assistance and information to conduct such audit, including reasonable access to operating systems, policies, procedures, records, and other materials.

20. Same Day ACH Option.

a. Description of the Same Day ACH Option. "Same Day ACH" is an option of the ACH Origination service that allows the Client to submit ACH credit and/or debit entries for same-day processing. Upon approval by Bank, Client may elect to use Same Day ACH for ACH Origination channels and/or accounts as designated to Bank. Client's election to use Same Day ACH may apply to all accounts within a designated ACH Origination channel, or Bank may allow Client to select specific accounts for Same Day ACH. Same Day ACH may not be available for all ACH Origination channels.

b. Requirements. In order for an ACH entry to be processed as a Same Day ACH entry, (i) Client must have elected Same Day ACH for the applicable ACH Origination channel and designated account; (ii) the effective entry date must be the same date (or earlier date, also known as a "stale-dated" entry) as the banking day that Client submits the entry to Bank; (iii) Client must submit the entry to Bank before the cut-off deadline for Same Day ACH processing as specified in the reference materials; and (iv) Client must meet all requirements for Same Day ACH set forth in the Rules (including but not limited to any transaction limits or restrictions on particular SEC Codes), these terms and conditions, and the applicable reference materials. In the event an ACH entry submitted by Client that is intended for same-day processing does not meet these requirements, but otherwise meets applicable requirements in these terms and conditions for ACH Origination, the entry will be processed by Bank, but not on a same-day basis. Same Day ACH can only be transmitted in a batch containing only Same Day ACH entries.

c. Same Day ACH Fees. In the event that an entry that Client submits as a Same Day ACH entry is not processed on a same-day basis as a result of Client's failure to meet applicable requirements for Same Day ACH, or the file suspending due to errors on Client's part (e.g., control total missing or incorrect, or insufficient funds in Client's account), then Client may be charged the applicable Same Day ACH fee for the entry, regardless of whether the entry is processed the same day Client submitted it to Bank or not.

d. Processing.

i. If Client submits a Same Day ACH entry to Bank according to the requirements set forth herein, Bank will use commercially reasonable efforts to transmit the entry to the ACH operator by deadline for same- day processing and settlement. However, certain delays or suspensions (including but not limited to system outages, delays due to reasonable internal Bank review for suspected fraud, anti-money laundering or other review) may prevent entries from being processed on a same-day basis. Accordingly, Client acknowledges and agrees that same-day processing is not guaranteed. Client agrees that Bank will have no liability due to the fact that such entry was not processed on a same-day basis for any reason, provided that Bank otherwise processes the entry according to these terms and conditions.

ii. If the Client has opted in to the Same Day ACH option for a designated account, any entry with a same- day or stale-dated effective entry date that is processed by Bank during a Same Day ACH processing window (A) will be considered a Same Day ACH entry; and (B) will be assessed the applicable Same Day ACH fee. Client must ensure that accurate effective entry dates are used for all of Client's ACH entries, as the effective entry date is used to determine whether an entry will be processed on a same- day basis.

iii. If Client has opted to use Same Day ACH for a designated account but wishes to submit an entry to be processed on a next-day (or later) basis, then Client must ensure that the effective entry date for such entry corresponds with the intended settlement date.

Account Reconciliation Plan Service

1. Description of Account Reconciliation Plan Service. The Account Reconciliation Plan ("ARP") service (full reconciliation, partial reconciliation or deposit reconciliation) assists Client in reconciling accounts by exchanging information with Bank regarding checks that Client has issued against Client's accounts and checks deposited into Client's accounts. Details regarding the functionality of the ARP service and formatting and other technical requirements for the service are provided in the ARP reference materials.

2. Operations of the Service. Client will designate the ARP service options for each account included in the service. All check, deposit or other information exchanged between Client and Bank in connection with the service must be transmitted electronically in the format specified by Bank. Check, deposit and other information Client sends must be received by Bank no later than the cutoff time for such information reflected in the ARP reference materials. Client may select a monthly, weekly or bi-weekly statement cycle for each account included in the service. If Client fails to designate a statement cutoff on Bank's ARP calendar, the default statement cycle will be monthly with a cutoff at the end of each calendar month.

BAI Transmission Service

1. Description of BAI Transmission Service. The BAI Transmission service is a Machine-to-Machine (M2M) information reporting service that provides Client balance, summary, and high-level transaction detail for posted account activity via BAI2 (BAI version 2) files. BAI2 is a file format developed by the Bank Administration Institute (BAI) as a common format for exchanging data. Bank supports the BAI2 standards for balance, summary, and detail information. BAI2 files are delivered over the internet by direct transmission of Client's formatted files into Client's accounting, treasury management workstation or Enterprise Resource Planning ("ERP") system.

   Client may elect Previous Day and/or Current Day BAI2 data files. The daily Previous Day BAI2 data file includes balance, summary and high-level transaction details for posted account activity. Current Day BAI2 data files include data sets as described in the File Delivery section below. Details regarding functionality and formatting of the service are provided in the BAI Transmission reference materials.

2. Use of the BAI Transmission Service. Client may use the BAI Transmission service with respect to the accounts that are identified during implementation of the service. BAI Transmission is a separate and distinct reporting channel from other BAI reporting services offered by Bank through online or digital services, and BAI Transmission is not intended as replacement functionality for those other, non-M2M BAI reporting services.

3. File Delivery. Previous Day files are created and distributed to via direct transmission Tuesday through Saturday mornings. Files are not provided on days following a non-banking day.

   Current Day BAI2 file content may be based on cumulative or incremental data sets. If Client elects to receive cumulative data, Bank offers multiple release windows from which to choose a custom schedule. Files are available Monday through Friday (excluding non-banking days) between 8 a.m. ET and 11:45 p.m. ET. If Client requires incremental data or net-new transactions since the time of last transmission, file delivery must start at the opening of the banking day and will be refreshed through predefined intervals through the day. Files are available Monday through Friday (excluding non-banking days) between 8 a.m. ET and 11:45 p.m. ET. Based on the selected file delivery schedule, actual transaction data contained in each Current Day BAI2 file transmitted may vary due to timing differences in comparison with current day reporting via Bank's online or digital channels. Client should use final posted transaction details from the Previous Day BAI2 data file for official posting to the Client's accounting, treasury management workstation, or ERP system.

Business Associate Agreement

1. Business Associate Agreement. This Business Associate Agreement ("BAA") is incorporated into this Agreement. This BAA applies to Client only if Client is a Covered Entity, and applies only to the treasury management services that, when provided to Client by Bank, result in Bank's classification as a Business Associate. Such treasury management services are referred to in this BAA as covered services. This BAA does not apply to any Client that is not a Covered Entity and does not apply to any services Bank provides to a Covered Entity that are not considered covered services. This BAA shall be effective as of the date that Bank provides any covered services to Client, if Client is a Covered Entity. Certain definitions for terms used in this BAA are included at the end of the BAA.

2. Introduction.

   a. In connection with the covered services, Covered Entity anticipates that Business Associate may receive PHI from or on behalf of the Covered Entity that is subject to protection under the Act.

   b. The purpose of this BAA is to establish protections for the privacy and security of PHI that is used by and/or disclosed to the Business Associate in connection with the covered services.

   c. If the parties previously entered into any business associate agreement, then this BAA shall not apply to any covered services which are governed by such previous business associate agreement, unless such existing business associate agreement is terminated by the parties or is amended to incorporate the terms herein. To the extent Business Associate provides covered services to Covered Entity which are not governed by a previous business associate agreement, then this BAA shall apply as of the date Business Associate provides such covered services to Covered Entity.

3. Privacy & Security of Protected Health Information.

   a. Permitted Uses and Disclosures. Business Associate is permitted or required to Use and Disclose PHI it receives from or on behalf of Covered Entity, or requests on Covered Entity's behalf only as follows:

      i. Functions and Activities on Covered Entity's Behalf. Covered Entity has requested that Business Associate perform the covered services associated with a banking or treasury management relationship. However, Business Associate may perform other activity for that relationship where PHI is incidentally provided to Business Associate or is excepted by the Act ("Exclusions"). The Exclusions are agreed to be Incidental Use and Disclosures, not subject to the terms of this BAA.

      ii. Business Associate's Operations. Business Associate may Use and Disclose PHI for all reasonable activity associated with Business Associate's performance of the covered services, proper management and administration, or to carry out Business Associate's legal responsibilities. Additionally, Disclosure is permitted only if:

         1) the Disclosure is Required by Law; or

         2) Business Associate obtains reasonable written assurance that:

            a) the PHI will be held in confidence and further Use or Disclosure will be only for the original purpose for which the PHI was Disclosed to Business Associate or as Required by Law;

            b) Business Associate will be promptly notified in the event the confidentiality of the PHI is breached; and

            c) to the extent for any purpose authorized by an Individual under 45 C.F.R. § 164.508.

   b. Receipt of PHI. Covered Entity will limit Disclosure of PHI to Business Associate to only the Minimum Necessary amount of PHI required or requested by Business Associate in providing the covered services. Upon termination of this BAA, the covered services, or Agreement, Covered Entity shall take all necessary steps to ensure that PHI is no longer provided, sent, or accessible to Business Associate.

   c. Prohibition on Unauthorized Use or Disclosure. Business Associate will not Use or Disclose PHI except as permitted or Required by Law, this BAA, or as otherwise permitted in writing by Covered Entity.

   d. Information Safeguards. Business Associate will use commercially reasonable efforts to implement and maintain administrative, technical, and physical safeguards ("Safeguards") designed to achieve compliance with 45 C.F.R. Part 164, Subparts C & E, and the HITECH Rules.

   e. Subcontractors and Agents. Business Associate will require its subcontractors and agents to provide reasonable written assurance that the subcontractor or agent will comply with the same restrictions and conditions that apply to Business

Associate with respect to the PHI as required by 45 C.F.R. § 164.504. Business Associate shall enter into a Business Associate Agreement with each of its Subcontractors, which meets these requirements.

f. Inspection of Books and Records. To the extent available according to Business Associate's retention schedule, Business Associate will allow DHHS to access its internal practices, books, and records, relating to its Use and Disclosure of PHI received from, or created or received by Business Associated on behalf of, Covered Entity, for the purpose of determining Covered Entity's and Business Associate's respective compliance with HIPAA. Business Associate will retain records according to its standard retention schedule and according to applicable regulatory requirements.

4. Individual Rights Requests.

a. Access. Business Associate shall, within thirty (30) calendar days after Covered Entity's request, make available in a mutually agreed upon format for inspection and copying, any PHI maintained in a Designated Record Set in the Business Associate's custody or control, that will enable Covered Entity to meet its access obligations under 45 C.F.R. § 164.524.

b. Amendment. Business Associate shall, within thirty (30) calendar days after receipt of notice from Covered Entity, promptly amend or permit Covered Entity access to amend any portion of the PHI maintained in a Designated Record Set in Business Associate's custody or control that will enable Covered Entity to meet its amendment obligations under 45 C.F.R. § 164.526.

c. Disclosure Accounting. Business Associate will maintain a process to provide Covered Entity an accounting of Disclosures that will enable Covered Entity to meet its disclosure accounting obligations under 45 C.F.R. § 164.528. Except for Disclosures that are exempted from the disclosure accounting requirements under HIPAA, Business Associate will make the legally required disclosure accounting information available as soon as possible, but not later than thirty (30) days after Covered Entity's written request.

d. Restriction Requests; Confidential Communications. Business Associate will comply with any Individuals' requests for restrictions and confidential communications to which Covered Entity has agreed pursuant to 45 C.F.R. § 164.522 (a) and (b), and of which Covered Entity has notified Business Associate in writing.

e. Responses to Individual Rights Requests. Covered Entity shall be solely responsible for responding to all Individual Rights Requests and communication regarding PHI, unless agreed to otherwise in writing between the parties. Covered Entity will not refer any Individuals directly to Business Associate. If Business Associate receives any Individual Rights Requests directly from an Individual, Business Associate may refer such Individual to the Covered Entity, but shall have no liability for the failure to do so.

f. Fees. Business Associate may charge a reasonable fee to cover the costs of fulfilling Covered Entity's requests under this Section 4, Individual Rights Requests.

5. Breach of Unsecured PHI.

a. Breach. In the event of a Breach of Unsecured PHI, Business Associate shall pursuant to the requirements set forth in subsection 2 below, provide written notice of the Breach to Covered Entity.

b. Notice Requirements. In the event of a Breach, written notice shall be sent to Covered Entity within thirty (30) calendar days of discovering such Breach (even if at such time Business Associate does not have all the details concerning the Breach). The notice shall contain the information required by 45 C.F.R. § 164.404(c), and any other additional and relevant information reasonably requested by Covered Entity so Business Associate and Covered Entity can comply in all respects with the Breach Notification Rule. The notice shall contain:

i. the date that a Breach was discovered, as determined by Business Associate in its reasonable discretion in accordance with the provisions of the Breach Notification Rule;

ii. a brief background and description of the Breach. Thereafter, Business Associate may follow up with additional information required under this subsection when such information becomes available;

iii. the nature of the PHI involved in the Breach; and

iv. a brief description of the mitigation and remediation efforts.

c. Security Incident. Upon written request, Business Associate shall, within thirty (30) calendar days, report to the Covered Entity any attempted or successful event Business Associate has become aware of for the time period specified in Covered Entity's request involving (a) unauthorized access, Use, Disclosure, modification, or destruction of PHI associated with Covered Entity, or (b) any interference with system operations in Business Associate's Information System containing PHI associated with Covered Entity, collectively a Security Incident as defined herein. The report provided by

Business Associate shall include any Security Incidents relating to PHI associated with Covered Entity for the time period requested by Covered Entity, up to (but not beyond) the date the request is made. If the Security Incident resulted in a Breach, then notice shall be provided in accordance with Section C.2 above. Covered Entity acknowledges that this Section C.3 constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents. Notwithstanding any of the foregoing provisions, Covered Entity agrees that Business Associate shall not be required to provide any additional reports of Unsuccessful Security Incidents to Covered Entity.

d. Mitigation. Business Associate agrees to take reasonable steps to mitigate, at its expense and to the extent practicable, any known harmful effects resulting from a Breach or Security Incident made known to Business Associate, not to exceed (6) six months of fees paid to Business Associate for the covered service associated with the Breach or Security Incident.

e. Reporting Obligations. Business Associate's only notification obligation under this Section C is to report Breaches and Security Incident as required herein to Covered Entity. Covered Entity shall be solely responsible to report a Breach or Security Incident to the affected Individuals, media outlets, DHHS, and other federal and state agencies if required by applicable law. If Covered Entity refers to or names Business Associate in any public notice or report, Covered Entity shall provide a copy of such notice or report to Business Associate prior to its release or publication.

6. General.

a. Termination of Agreement. Either party may terminate this BAA by terminating this Agreement per the applicable termination provisions within this Agreement. This BAA will also be deemed terminated if Business Associate ceases to provide any covered services to Covered Entity.

b. Obligations upon Termination.

i. Return or Destruction. Subject to Business Associate's standard record retention policies, upon any termination of this BAA, Business Associate will, if feasible, return or destroy all PHI in whatever form or medium (including any electronic medium) and all copies thereof upon request of Covered Entity. Business Associate and Covered Entity will mutually agree upon a reasonable time frame for the return or destruction of the PHI, which time period will not exceed one hundred and twenty (120) calendar days from date of termination effectiveness.

ii. Return/Destruction Not Feasible. To the extent Business Associate determines in its reasonable discretion that the return or destruction of PHI is not feasible, Business Associate will limit its further Use or Disclosure of PHI to those purposes that make return or destruction of the PHI infeasible.

iii. Continuing Privacy Obligation. Business Associate's obligation to protect the privacy of the PHI that was provided to Business Associate prior to any termination of this BAA shall survive such termination, for so long as Business Associate possesses the PHI. However, Business Associate shall have no obligations with respect to PHI disclosed to it after termination of this BAA, the covered services, or this Agreement.

c. Liability. Liability of Business Associate and Covered Entity under this BAA shall be governed by the applicable terms of this Agreement. This BAA shall not expand or limit the liability of either Covered Entity or Business Associate beyond the liability set forth in this Agreement, except as specifically stated otherwise herein.

d. Amendment to Agreement. Upon the effective date of any final regulation or amendment to the Act that would change the terms of this BAA with respect to PHI, this BAA shall be automatically amended to incorporate any regulations or amendment that relate to the obligations of Business Associate.

e. No Third Party Beneficiaries. There are no intended third party beneficiaries under this BAA.

f. Notices. Any notice required or permitted to be given by this BAA, must be in writing and must be provided per the notice terms of this Agreement. Business Associate shall use reasonable efforts to provide a copy of any such notices to the Privacy Official of Covered Entity, if Business Associate has been provided contact information for such individual by Covered Entity, but Business Associate shall have no liability for failure to provide notice to the Privacy Official if Business Associate has otherwise complied with its notice obligations herein.

g. Record Retention. Business Associate shall not be obligated to maintain any records containing PHI received from Covered Entity for longer than is required by Business Associate's record retention policies, which shall comply with applicable regulatory requirements. Business Associate's failure to comply with its obligations under this BAA due to the fact that a record or the PHI contained within a record has been destroyed in accordance with the Business Associate's normal record retention practices shall not be considered a breach of this BAA.

h. Entire Agreement. This BAA, as incorporated into this Agreement, is the entire agreement between the parties with respect to the parties' obligations to protect PHI under the Act.

i. Relationship to this Agreement and Confidentiality Agreement. This BAA is intended to address only the privacy and security of PHI. The parties may have entered a separate confidentiality agreement with respect to the Disclosure, receipt and Use of other Confidential Information (as defined in the applicable confidentiality agreement). To the extent there is a conflict between this BAA and the provisions of this Agreement, or between this BAA and any separate confidentiality agreement, this BAA shall control with respect to the protection of PHI and the obligations of HIPAA which may be applicable to the covered services. The terms of this BAA, this Agreement, and any separate confidentiality agreement shall be construed in a manner to achieve compliance with HIPAA and any applicable state privacy laws governing the protection of medical information that are not pre-empted by HIPAA.

j. Applicable Law. The provisions of this BAA shall be construed under the Act. To the extent the Act is not applicable, the applicable laws provisions of this Agreement shall govern.

7. Definitions. Capitalized terms used in this Agreement shall have the following meanings. Any other capitalized terms not identified here shall have the meaning as set forth in the Act as may be amended or revised from time to time, including amendments by the Secretary.

a. "Act" shall mean collectively HIPAA, HITECH Act, HIPAA Regulations, and HITECH Rules.

b. "Breach" shall have the meaning given to it by 45 C.F.R. § 164.402.

c. "Breach Notification Rule" shall mean the "Standards for Breach Notification for Unsecured Protected Health Information," 45 C.F.R. Part 164, Subpart D.

d. "Business Associate" shall have the meaning given to it by 45 C.F.R. § 160.103.

e. "Covered Entity" shall have the meaning set out in 45 C.F.R. § 160.103.

f. "DHHS" means the United States Department of Health & Human Services.

g. "Disclose" and "Disclosure" mean, with respect to PHI, release, transfer, providing access to, or divulging to a person or entity not within Business Associate.

h. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996.

i. "HIPAA Regulations" shall mean the HIPAA implementing regulations in 45 C.F.R. Parts 160-64.

j. "HITECH Act" shall mean the provisions of the Health Information Technology for Economic and Clinical Health Act contained in Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009. A reference to the HITECH Act shall also include any HITECH Rules related thereto.

k. "HITECH Rules" shall mean any regulations issued pursuant to the HITECH Act by DHHS, including the Breach Notification Rule.

l. "Incidental Use and Disclosure" shall meaning set out in 45 CFR § 164.502(a)(1)(iii).

m. "Individual" shall mean the person who is the subject of PHI and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

n. "Individual Rights Requests" shall mean requests by individuals for Access, Amendment, Disclosure Accounting, and Restriction as permitted by 45 C.F.R. § 164.500, et seq.

o. "Minimum Necessary" shall have the meaning set out in 45 C.F.R. § 164.502.

p. "PHI" or "Protected Health Information" shall have the meaning provided by HIPAA, 45 C.F.R. s. 160.103, but limited to that information received, maintained, transmitted or created by Business Associate from or on behalf of Covered Entity.

q. "Privacy Official" shall mean the person designated by the Covered Entity or Business Associate to serve as its Privacy Official within the meaning of 45 C.F.R. § 164.530(a), and any person to whom the Privacy Official has delegated any of his or her duties or responsibilities.

r. "Privacy Rule" shall mean the "Standards for Privacy of Individually Identifiable Health Information," 45 CFR Part 160 and Part 164, Subparts A and E.

s. "Required by Law" shall have the same meaning given to it in 45 C.F.R. § 164.103.

t. "Secretary" shall mean the Secretary of DHHS.

u. "Security Incident" shall have the meaning in 45 C.F.R. § 164.304.

v. "Security Rule" shall mean the "Security Standards for the Protection of Electronic Protected Health Information," 45 CFR Part 160, Subpart A, and Part 164, Subparts A and C.

w. "Covered Services" shall mean the activities, functions and/or services that Business Associate from time to time renders to or on behalf of Covered Entity to the extent that those activities, functions and/or services are covered by HIPAA.

x. "Unsecured PHI" shall mean PHI that is not secured through the use of a technology or methodology that renders such PHI unusable, unreadable or indecipherable to unauthorized individuals as specified in guidance issued pursuant to Section 13402(h) of the HITECH Act, including the Breach Notification Rule.

y. "Unsuccessful Security Incident" shall mean a ping or other broadcast attack on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as any such incident does not result in unauthorized access, use, or disclosure of PHI.

z. "Use" shall mean, with respect to PHI, utilization, employment, examination, analysis or application by Business Associate.

Cash Concentration Service

1. Description of Cash Concentration Service. The Cash Concentration service or "CashCon" service allows the Client to manage balances in accounts at other financial institutions by sending debit entries to those accounts through the automated clearing house ("ACH") network. Details regarding CashCon's functionality and service requirements are provided in the CashCon reference materials.

2. Functioning of the CashCon Service. Under the CashCon Service, the Bank originates ACH debit entries on behalf of Client that are directed to accounts designated by Client to be included in the service, each a "reporting location account". Debit entries directed to a reporting location account are "concentration" entries. The destination of any concentration entry (the account used as the settlement account for such entries) is the Truist account designated by Client and referred to as the "designated account." The Client will be the "originator" and Bank will be originating depository financial institution or "ODFI" for each of the concentration entries. Client's use of the CashCon service is subject to the terms and conditions for the ACH Origination service.

3. Implementation of CashCon Setup. A single reporting location account must use only one designated account to settle concentration entries. However, if Client has more than one reporting location account, each reporting location account may use a different designated account or a single designated account to settle concentration entries for those reporting locating accounts.

4. Origination and Processing of Entries. Client must send all concentration entries to the Bank by using one of the delivery methods offered by Bank, as described in the reference materials. Any concentration entries received after the daily cut-off time set forth in the CashCon reference materials will be treated as received on the next business day. Bank will format, process and settle to the relevant designated account all concentration entries that Bank receives from the Client in accordance with these CashCon terms and conditions and the terms and conditions for the ACH Origination service, including the Nacha rules referenced therein.

5. Security Procedures. The security procedures for the CashCon service require that Client's users use the authorization codes provided to Client to send concentration entries through any delivery method for the applicable reporting location account. Certain authorization codes may not be unique to Client, but the combination of authorization codes is unique to each Client. The authorization codes are not user-specific; this means that all of Client's users will use the same set of authorization codes to initiate a concentration entry for a particular reporting location account. Bank will send the authorization codes to the individual designated by Client. Client agrees that use of the service constitutes acceptance of the below security procedures.

6. ACH Origination Service. These CashCon terms and conditions are expressly made a part of the terms and conditions for the ACH Origination service and are subject to the terms and conditions thereof. Terms defined in the ACH origination terms and conditions have the same meanings when used herein. Any inconsistency on a particular issue between these CashCon terms and conditions and the terms and conditions for the ACH Origination service shall be resolved in favor of the CashCon terms and conditions.

1. Description of Cash Vault Service. The Cash Vault service is designed to facilitate Client's cash and deposit needs. Details regarding the Cash Vault service's functionality and certain requirements that Client must follow when using the Cash Vault service are provided in the Cash Vault reference materials.

2. Definitions. The following terms have the specified meanings for the purposes of these Cash Vault terms and conditions:

   a. "Account" means the account(s) designated by Client to which deposits will be made and from which cash orders will be funded.

   b. "Armored courier" means the armored courier selected by Client who acts as Client's agent and transports deposit bags and cash orders for deposit to Bank.

   c. "Authorized user" means any person that Client is deemed to have authorized to place cash orders up to the applicable order limit

   d. "Change orders" means those orders Client gives Bank for the delivery of U.S. coins or currency by armored courier.

   e. "Cash vault(s)" means the cash vault(s) that Bank has designated as serving Client's business location(s).

   f. "Contaminated currency" means any currency which the Federal Reserve Bank classifies as contaminated, including any currency damaged by or exposed to a contaminant hazard (including any chemical, radioactive or biological substances) that may present a health or safety risk, or that cannot be processed under normal operating procedures.

   g. "Deposits" means the funds that Client delivers to the cash vault that are to be processed for deposit in accordance with these Cash Vault terms and conditions.

   h. "Funds" means U.S. coins, currency, checks and other negotiable items.

   i. "Mutilated coins" means any coins that have been bent or twisted out of shape, punched, clipped, plugged, fused or defaced but that can be identified as to genuineness and denomination.

   j. "Mutilated currency" means any currency that has been damaged to the extent that one-half or less of the note remains, or its condition is such that its value is questionable and special examination is required before any exchange is made.

   k. "Order limit" means the maximum dollar value of change orders that may be requested on any business day for each of Client's locations.

3. Client's Obligations Related to Deposits.

   a. Client must collect and count funds and place them in a sealed, disposable deposit bag(s) or similarly designed tamper-proof bag(s) (each such bag is referred to in these terms and conditions as a "sealed deposit bag") clearly marked with Client's name or identification number. Each sealed deposit bag must be prepared in accordance with the requirements set forth in the Cash Vault reference materials. A deposit ticket listing Client's name, deposit account number and the amount of funds must be included in each sealed deposit bag.

   b. Client must cause sealed deposit bags to be delivered by the armored courier to the appropriate cash vault for each of Client's locations. Bank may reject, impose a special fee on, and/or delay processing of any sealed deposit bag if (i) the deposit ticket does not match the amount contained in the sealed deposit bag, (ii) the sealed deposit bag was not prepared in accordance with the requirements set forth in the Cash Vault reference materials, (iii) the sealed deposit bag is delivered to the wrong cash vault, (iv) the sealed deposit bag is delivered by anyone other than the Client's designated armored courier or (v) any sealed deposit bag appears to be unsealed or to have been tampered with.

   c. In the event that Bank accepts delivery of an unsealed deposit bag or a sealed deposit bag that appears to have been tampered with (each such bag is referred to in these terms and conditions as an "unsealed deposit bag"), and unless Client has previously given Bank instructions on how to process unsealed deposit bags, Bank will not process or take any action regarding an unsealed deposit bag until Client gives Bank an instruction regarding processing of the unsealed deposit bag.

4. Bank's Obligations for Processing Deposits.

   a. Bank will process each sealed deposit bag after delivery to the cash vault. Bank will open each sealed deposit bag, verify the contents against the deposit ticket and deposit from the bag the funds that qualify for deposit into the relevant account. Client's actual deposit is not made until such verification is completed at the cash vault and the deposit is posted to Client's account. If there is any discrepancy between the amount reflected on the deposit ticket and the

amount counted by Bank, or any discrepancy between the contents of the bag and information that is otherwise reported to or made available to Bank, Bank's count will be final. Without limiting the generality of the foregoing sentence, in certain situations, based upon data that Client (or a third party) has provided to Bank with respect to Client's cash to be deposited via the Cash Vault service, Bank may provide Client with provisional credit for such cash. However, Client's actual deposit shall not be deemed made and deposit credit shall not be given until such cash deposits are actually received by Bank, and are counted and verified. Client agrees that Client's actual deposit is based solely upon the physical verification and count performed by Bank and that Bank is not bound by any other information reported by Client or by a third party, and Bank may reverse or adjust any provisional credit that may have been given based upon such information.

b. Deposits collected by the armored courier are not deemed to be received by Bank until the deposits have been delivered to a cash vault, and such deposits are not insured by the FDIC during transit.

5. Change Orders. Client acknowledges that each authorized user has authority to place change orders up to the order limits for delivery to Client's location. Bank may place a "hold" on Client's account for the amount of a change order, and Bank will charge Client's account for the change order when Bank delivers the order to Client's armored courier. Bank reserves the right to reduce change orders to maintain Bank's inventory of coins and currency.

6. Authorization Codes. If required, Bank will provide authorization codes for placing change orders to Client's designated contact or to Client's designated authorized users.

7. Risk of Delivery. Client is solely responsible for engaging the armored courier. The armored carrier acts as Client's agent, not an agent or subcontractor of Bank. Client assumes any and all risks incidental to or arising out of selection of the armored carrier, the delivery of deposit bags to Bank and the delivery of change orders to Client. Notwithstanding the foregoing, Bank may reject any armored courier Bank deems unacceptable. Bank has no responsibility or liability for a deposit bag until Bank accepts possession of the deposit bag from Client's armored courier (as evidenced by one of Bank's authorized representatives signing the armored courier's manifest acknowledging receipt of a designated number of deposit bags) or for cash orders after Bank delivers them to Client's armored courier.

8. Contaminated and Mutilated Coins or Currency.

a. Bank is not obligated to accept currency or coin that is contaminated. Contaminated currency must be delivered to Bank in a separate sealed, tamper-evident disposable deposit bag, clearly labeled as "Contaminated Currency." Client must provide documentation stating the type and extent of the contamination, a breakdown by denomination of the currency and a deposit slip for the declared value. The deposit bag and 2 copies of the required documentation must be placed in a second sealed, tamper-evident, disposable deposit bag with stated value recorded on the bag. If Bank accepts the contaminated currency, Bank will forward the deposit of contaminated currency to the Federal Reserve Bank for processing. Once the Federal Reserve Bank has provided confirmation of value, Bank will credit Client's account for the value assigned. Client should not deliver any contaminated coin to Bank, but should follow instructions in the Cash Vault reference materials or contact Bank for further instructions on handling contaminated coins.

b. Bank is not obligated to accept mutilated coin or currency. Mutilated coins or currency must be delivered to Bank in a separate sealed, tamper-evident disposable deposit bag, clearly labeled as "mutilated coins" or "mutilated currency" as appropriate in accordance with the Federal Reserve's guidelines. Client must provide documentation stating the estimated value of the mutilated coins or currency, a breakdown by denomination of the coins or currency, an explanation of how the coins or currency became mutilated, and a deposit slip for the estimated value of the deposit. The deposit bag and 2 copies of the required documentation must be placed in a second sealed, tamper-evident, disposable deposit bag with stated value recorded on the bag. If Bank accepts the mutilated coin or currency, Bank will forward the deposit of mutilated coins to the U.S. Mint and the deposit of mutilated currency to the U.S. Department of the Treasury. Once the U.S. Mint or the U.S. Department of the Treasury has provided confirmation of the value of the mutilated coins or currency, Bank will credit Client's account for the value assigned.

c. If there is any discrepancy between the value of the contaminated currency or mutilated coins or currency assigned by Client and the amount counted by Bank or by the Federal Reserve Bank, U.S. Department of the Treasury or the U.S. Mint, Bank's count or the count of the Federal Reserve Bank, U.S. Mint or the U.S. Department of the Treasury will be final. Bank will charge Client for any additional fees charged by the Federal Reserve Bank for processing any contaminated currency, by the U.S. Mint for processing any mutilated coins or by the U.S. Department of the Treasury for processing any mutilated currency.

d. Bank may refuse to accept any contaminated or mutilated coins or currency unless Bank has provided Client with prior approval for the delivery of such coins or currency. If any contaminated currency or mutilated coins or currency is included in among deposit bags or comingled in any deposit bag and not contained in a separate marked deposit bag,

Bank may refuse to process all or part of the deposit bag containing such currency, may return the deposit bag or the contaminated currency or mutilated coins or currency contained in the deposit bag or may refuse to give credit for the contaminated currency or mutilated coins or currency, and Bank will charge Client for the amount of any currency or coins that were unable to be processed for which Client was given provisional credit. Bank has no liability for the amount of any contaminated currency or mutilated coins or currency included in any deposit bag and not contained in a separate marked deposit bag as required above.

Check Image Services

1. Description of Check Image Services. Check Image Services provides the ability to receive paid item and deposit ticket images via CD-ROM or Check Image Transmission for long term archival and storage. The Check Image Transmission option includes delivery of imaged items through direct transmission. The CD-ROM option includes delivery of imaged items (and in some cases when made available by Bank, account statements and Account Reconciliation Plan (ARP) reports) on a CD-ROM. Client must have required equipment and must download and install required software materials in order to access the CD-ROM. Details regarding the functionality and requirements that Client must follow when using the Check Image Services are provided in the Check Image Services reference materials.
2. Selection of Check Image Services. Client may select the Check Image Transmission and/or CD-ROM delivery method for imaged items or other available reports or statements designated by Client for the accounts included in the service. Client must specify a lead account for all accounts capturing the same types of images using the same delivery method.
3. Imaged Items. Client agrees that Bank will have no liability for any missing image or if any image Bank captures is not legible. In the event of any missing or illegible images, Bank will use reasonable efforts to provide a replacement image.

Controlled Disbursements Service

1. Description of Controlled Disbursements Service. The Controlled Disbursement Account ("CDA") service allows Client to manage daily cash requirements by allowing Client to defer funding of check disbursements until the day they are presented for payment.
2. Operation of the CDA Service.
    a. When Client requests the CDA service, Bank will provide Client with a set of specifications, including routing number and magnetic ink encoding requirements, that checks issued against a disbursement account must meet in order for the CDA service to operate correctly. Using checks that do not meet these specifications can result in daily out-of-balance situations in a disbursement account. Client must give Bank voided sample checks for each disbursement account so that Bank may test those checks for compliance with the specifications. Client may not issue checks against a disbursement account until Client has received a notice from Bank that Client's sample checks are acceptable.
    b. On each banking day, Bank will make information available to Client, through one of Bank's online services, regarding the total dollar amount of all checks that have been presented for payment against each disbursement account that day by the daily reporting deadlines disclosed to Client.
    c. Client understands that Bank provides presentment information to Client solely to assist Client in funding Client's disbursement accounts. The CDA service does not relieve Client of the obligation to fund Client's disbursement accounts appropriately. As a result, Client agrees to have sufficient funds on deposit in each disbursement account to pay all checks issued against that account, whether or not Bank has notified Client of the presentment of those checks. If the presentment information is not available by the daily reporting deadline, Client should consider using an estimate for funding the disbursement account based on historical information and/or Client's information on its issued checks. The disbursement account must be funded by the funding deadline(s) disclosed to Client. In the event a disbursement account is not adequately funded on the date of presentment, Bank may return items for which there are not sufficient funds.
    d. If any ACH or other electronic debits are presented against a disbursement account, those debits may not be included in the information Bank provides Client regarding daily presentments. In that event, Client must adjust Client's funding of the disbursement account to cover those ACH or other electronic debits.

e. Client agrees and understands that the purpose of the CDA service is to allow Client to manage daily cash requirements by allowing Client to defer funding of check disbursements until the day they are presented for payment. The service should not be used to delay payment to or collection of funds by any payees or the presenter of any check.

Controlled Payment Reconciliation Service

1. Description of Controlled Payment Reconciliation Service. The Controlled Payment Reconciliation ("CPR") service allows Client to provide Bank instructions regarding payment or return of certain checks Client believes are fraudulent or not validly issued, before the checks post to Client's account. CPR Payee Positive Pay is a version of the CPR service that includes payee name matching, as described herein. Client may select either CPR or CPR Payee Positive Pay. Each account enrolled in the respective service option is referred to herein as an "enrolled account". Details regarding the functionality, formatting and other technical requirements for the service are provided in the reference materials.

2. Operation of the CPR Service. CPR service helps Client detect unauthorized, counterfeit, altered or otherwise fraudulent checks on Client's enrolled account(s) by comparing issued check (and any voided check) information provided to Bank by Client against the checks presented to Bank against the enrolled account(s). CPR Payee Positive Pay provides stronger protection against fraudulent checks by comparing payee names from Client's issued check file with the payee name on the check, in addition to the standard check number and account fields that are compared with the CPR service. In order for the payee name verification process to function correctly, the payee name must be clearly displayed on Client's printed checks, and the payee name provided in the issued check file should exactly match the name printed on the check.

   a. Presentment Processing. Client must transmit an issue file to Bank on each day on which Client has issued any checks against an enrolled account. Bank must receive that issue file by the deadline set forth in the reference materials and the file must contain the information set forth in the reference materials with respect to each check listed in the file. Bank will compare the information in Client's issue file with the information in Bank's systems with respect to checks (i) that have been presented to Bank through normal check clearing channels for payment against the enrolled account, and (ii) for which Bank has provisionally settled but has not yet posted to the enrolled account. Client authorizes Bank to post, finally pay and charge against the enrolled account, each check that Bank reasonably determines matches the information in Client's issue file. Bank will notify Client of each presented check that is not included in the issue file or that reflects information that does not reasonably match the information in the issue file ("mismatched checks"). Client must instruct Bank to pay or return each mismatched check by the payment decision deadline set forth in the CPR reference materials; such instruction is a "decision".

   b. Mismatched Checks. Client may elect one of two ways for Bank to handle mismatched checks if Client fails to give Bank a pay or return decision by the payment decision deadline. Under the "return default" option, Client authorizes Bank to return unpaid each mismatched check unless Bank receive an instruction from Client to pay it before the payment decision deadline. Even if Client selects a return default option, Bank may post, finally pay and charge against the enrolled account a mismatched check Client hasn't decisioned (A) as otherwise provided below, for mismatched checks presented over the counter in one of Bank's branches and (B) mismatched checks that Bank believe in good faith result solely from encoding errors. Under the "pay default" option, Client authorizes Bank to post, finally pay and charge each mismatched check against the enrolled account unless Bank receives an instruction from Client to return it before the payment decision deadline. Bank will process and pay all exceptions according to Client's default settings.

   c. Client may opt not to provide information in Client's issue file (i) for one or more check attributes that the CPR service is capable of matching or (ii) certain items in situations where Client deems it necessary to avoid mismatch situations, such as instances where Client believes an item has already been legitimately paid. Client acknowledges that not providing information to allow for matching of all available check attributes or not including information for all items increases the risk that a fraudulent check will not be detected as a mismatched check. If Client fails to provide information in Client's issue file regarding all available check attributes that the service is capable of matching, or Client fails to provide an issue record for a check at all for any reason, then Bank will not be liable for paying any check that is fraudulent with respect to the attributes for which Client failed to provide the Bank information, provided Bank otherwise satisfied its duty of care with respect to the other aspects of the CPR service in processing that check.

3. Teller Access Service. As part of the CPR service, Bank will also make Client's issue files available to Bank's branches to assist Bank's tellers in cashing checks ("teller access"). If a check presented for payment against an enrolled account over the counter in one of Bank's branches (1) is presented before Bank has received and processed an issue file for such check, (2) is a mismatched check, or (3) is otherwise identified by Bank as suspect, then Bank will not pay the check and will refer the presenter back to Client. If a check that matches the issue file information in check number and amount is presented to Bank for cashing over the teller line and the payee name, if provided by Client, does not match the name viewed on the check by

the teller, then Bank may in its discretion decide to pay the check, or to not pay the check and refer the presenter back to Client.

4. Transmission of Information. Bank will transmit information regarding mismatched checks to Client by using certain of Bank's online services. Client must transmit Client's issue files and Client's pay or return decisions to Bank by using one of Bank's online services as designated in the reference materials. Client's issue files and pay or return decisions must be in a format acceptable to Bank. In the event the applicable online service is not available, then a mutually agreed-upon alternative delivery method and process will be established to provide the relevant information to Client and for Client to provide Client's issue files and/or Client's pay or return decisions to Bank. Client will designate one or more operational contacts for the CPR service. Bank may, in its sole discretion, contact these operational contacts in the event Bank has questions about Client's issue file, the relevant online service is not available, to set up an alternative delivery method, or for other operational issues with the service. These operational contacts are also authorized to instruct Bank to pay or return any mismatched check in the event that Bank, in its sole discretion, contacts an operational contact regarding such check.

5. Limits on Bank's Liability. Client acknowledges that Bank will rely on information and instructions Client gives Bank in providing the CPR service and that Bank is not required to inspect any attribute of a check (other than those included in the relevant issue file) that is processed through the CPR service. Bank will not have any liability for paying or returning any check in accordance with these CPR terms and conditions, including any check that (i) bears a forged or unauthorized signature, or is counterfeit, or otherwise not validly issued or (ii) is altered or otherwise fraudulent with respect to an attribute that the CPR service is not designed to match. Client will be precluded from asserting any claims against Bank with respect to losses for any fraudulent check that was paid or returned in accordance with these terms and conditions. Client also acknowledges that the CPR service is not a substitute for Bank's stop payment service, or a means to reject checks that were validly issued but for which there exists a dispute with respect to the underlying transaction. Client agrees not to report an item as "void" via this service if Client has released the item for payment.

Daily Liquidity Account and Corporate Premium Money Market Account

1. Description of Daily Liquidity Account ("DLA") and Corporate Premium Money Market Account ("CPMMA") Service. These terms describe the treasury management services associated with the DLA and CPMMA, which are account types intended to be used to hold balances for longer periods of time, with limited transactional capabilities. These terms apply only to new DLA or CPMMA account types opened with Truist Bank. If Client previously opened a DLA or CPMMA with SunTrust Bank, the terms of the existing agreement(s) (as amended) for the accounts that Client executed with SunTrust Bank continue to apply, as certain services implemented on such accounts differ from services implemented for Truist DLA or CPMMA. DLA is an interest-bearing demand deposit account as defined under Federal Reserve Regulation D, and there is no limit on the number of withdrawals or transfers an account holder may make CPMMA is an interest-bearing money market deposit account as defined under Federal Reserve Regulation D; Bank reserves the right at any time to require at least seven days' written notice of an intended withdrawal from the CPMMA, and account holders are limited to six withdrawals or transfers per calendar month or statement cycle. The DLA or CPMMA is opened with Bank using Bank's standard account opening documentation; then, the treasury management services indicated below will be implemented on the accounts. The addition of any other treasury services on DLA or CPMMA, or any modification of the services listed below for DLA or CPMMA, are subject to approval by Bank and may not be permitted, in Bank's sole discretion.

2. Services Implemented for DLA and CPMMA. The following services will be implemented for a Truist DLA or CPMMA, according to the terms and conditions herein: ACH Blanket Block, Check Block, and Digital Treasury. Client will have the option to enroll in Wire Service within Digital Treasury, as described in these terms and conditions. Any additional services used with respect to the DLA or CPMMA will be subject to applicable service terms and conditions.

3. ACH Blanket Block. ACH Blanket Block will be implemented for each DLA or CPMMA. This service blocks the posting of incoming automated clearing house, or "ACH," debit and/or credit entries against the account. Client acknowledges that any ACH debits attempted against the account or any ACH credits sent to the account will be returned automatically and will not be processed, so Client agrees to use alternate methods to transfer funds into or out of the account.

4. Check Block. Check Block will be implemented for each DLA or CPMMA. This service blocks any checks presented against the account. Client acknowledges that any checks presented against the account will be returned and will not be paid, so Client agrees to use alternate methods to transfer funds out of the account.

5. Digital Treasury. Digital Treasury will be implemented for each DLA or CPMMA. Digital Treasury terms and conditions are below; however, certain functions within Digital Treasury will not be available for DLA or CPMMA, including, but not limited to, ACH Origination and Real-Time Payment initiation.

a. Description of Digital Treasury Service. Digital Treasury service is an internet-based information reporting and transaction initiation system providing real-time access and functionality to Client deposit accounts, and certain functionality or information related to loans or commercial card accounts ("Digital Treasury"). Digital Treasury provides Client a single access point to access account information, place stop payments, initiate certain types of payments, transfer funds between accounts, provide decision instructions for certain services, and receive notifications for Client's accounts or services. The types of payments available to be initiated (e.g. Wire, ACH Origination, and Real-Time Payments) and services available for decision instructions (e.g. Positive Pay and Reverse Positive Pay), and other services and account functions available within Digital Treasury are subject to terms and conditions specific to those services and functions and may include additional fees.

b. Introduction. Certain services that are available through Digital Treasury require separate enrollment, and Client may not use such services until enrollment is completed. Client agrees that any use of any service through Digital Treasury is subject to the applicable fees and terms and conditions for that specific service as well as these Digital Treasury terms and conditions.

Certain access to Digital Treasury may require Client to download and agree to license agreements related to, and use certain software, including but not limited to Rapport (a secure browsing software provided by Trusteer Inc., an IBM company), as designated by Bank. Client's failure to use such software may limit Client's ability to access Digital Treasury.

c. Security Procedures. The security procedures for Digital Treasury are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.

i. Access Credentials. Access credentials, which may include User ID, initial Password and Security Token, will be provided to the Primary Administrator established during the Digital Treasury enrollment for each designated user. Upon initial log in to Digital Treasury, each user will be required to change their initial Password to a new personal password pursuant to the instructions provided. Valid access credentials are required to log in to the service and perform transactions within the service.

ii. Dual Payment Approval. Any ACH, wire, or RTP transaction initiated through the service requires dual payment approval, which means that one authorized user with sufficient entitlements must initiate the transaction and a different authorized user with sufficient entitlements must approve the transaction in order for the transaction to be released and processed. At Client's option, Client may require additional approvals (two or more users) for such transactions.

iii. Administrative Approval. Administrative actions initiated through the service such as, but not limited to, specifying the type of payments a user can initiate or limiting payment amount by payment type or source account, must be approved by a second user with the appropriate permissions. Administrative approval entitlements in Digital Treasury are the same as those established for Truist One View. If Client elects to opt out of the administrative approval security procedure for Truist One View/Digital Treasury, Client must document this decision in writing and in accordance with Bank procedures. **Bank strongly recommends that Client not opt out of the administrative approval security procedure**.

iv. Security Token. Transactions initiated within the service (including but not limited to Wire, ACH Origination, Real-Time Payments, account transfers, and loan payments or advances) require the approval of an authenticated user with appropriate entitlements in order for the transaction to be released and processed. Authentication methods and procedures may change from time to time and will always be stated in current reference materials.

d. Administrators and Operators. The two individuals designated as Truist One View Primary Administrators also become Digital Treasury Primary Administrators at enrollment. If Client has opted out of the Truist One View administrative approval security feature, the single individual designated as the Truist One View Primary Administrator is the Primary Administrator of the Digital Treasury service. A Primary Administrator may create additional users of the service and users with administrative entitlements, who may also be referred to as Company Operators and Administrators, respectively. Once entitlements are given to Administrators and Company Operators, each will have authority to perform all actions and transactions available through Digital Treasury as granted by the entitlements. Each Company Operator and Administrator may perform any entitled actions or transactions on Client's accounts regardless of whether they are otherwise a designated signer on any such accounts. Should Client request Bank to revoke or change a Primary Administrator, Client must notify Bank of such revocation or change as soon as possible in writing and in accordance with Bank procedures.

e. Account Information. Client can select from a variety of reporting formats that may include different combinations of account balances and activity information.

f. Account Transfers. Client may initiate current day and future dated transfers between its accounts at Bank, as may be subject to any applicable restrictions on the number of transfers governing such account(s). Bank will execute any transfer request on the value date for the transfer indicated within the service. By initiating any transfer, Client assumes full responsibility for verifying the availability of collected funds for the requested transfer date.

Bank is under no obligation to honor, either partially or entirely, any transfer request that exceeds the available funds in Client's account. If Bank in its sole discretion creates an overdraft to complete a transfer, Client agrees to repay Bank upon demand, together with any applicable interest or fees and if necessary, the costs of collection.

g. Stop Payments. Client may initiate stop payment requests or cancellations of a stop payment order in the form and manner specified in Digital Treasury. Client must provide the account number, check serial number, exact check amount, and stop payment reason in order for the stop payment instructions to be effective. Stop payments are subject to applicable terms within the Commercial Bank Services Agreement.

h. Images of Paid Checks, Deposits & Deposited Items, and Returned Deposited Items. Through Digital Treasury, Client may view digital images of cancelled (paid) checks, deposit slips and accompanying items, and returned deposited checks. Online images may be viewed only for such periods of time as Bank may establish and older images may be sent to Client via the method specified by Bank.

As is common industry practice with various check "truncation" or "safekeeping" services, Bank destroys the original checks but retains the images for at least the number of years required by law. If an image of a check is missing or is illegible, Bank will attempt to provide Client with a legible copy upon Client's request, if Client gives Bank adequate information to identify the specific item. However, Bank will have no liability to Client if Bank is unable to provide a copy within Client's requested timeframe, or at all, due to any reason other than Bank's gross negligence, willful misconduct or criminal conduct. Bank reserves the right to charge a fee for such requests in some circumstances, such as when the image is missing or illegible due to circumstances beyond Bank's control.

i. Alerts. With this service, Client may choose to receive alerts concerning selected types of events relating to Client's accounts or services. Client may then log on to Digital Treasury to obtain more details. Bank accepts no responsibility or liability if Client does not receive any alerts in a timely manner due to email outages or any other reason.

j. eStatements. With this service, Client may choose to receive images of Client's statements including bank statements, and other reports or information. Bank accepts no responsibility or liability if these statements or reports are not available in a timely manner due to outages or any other reason. When a deposit account is included within the service, paper statement delivery will be suppressed for such account, and the statements for such account will only be available within Digital Treasury to entitled users. **Bank strongly recommends that Client establish appropriate internal controls to monitor and review statements for deposit accounts, especially in the event that statements are only available through Digital Treasury.** If Client requires paper statement delivery for deposit accounts included within the service, Client must request paper statements from Bank and additional fees may apply.

k. Loan, Line of Credit, and Card Accounts. If any loan, line of credit, or credit, commercial, or purchasing card account types are included in Client's setup of the service, the term "account" when used in reference to the service includes these account types. By requesting the account to be included in the service, Client authorizes Bank to provide or display information relating to such loan, line of credit or card accounts within the service or to entitled users, and to provide any available functionality or service with respect to those accounts as may be requested or enabled by an entitled user, including, but not limited to, the ability to view account and transaction information, to make payments on the accounts, or to perform drawdowns, advances, or other transactions on the accounts. Client represents and warrants to Bank that inclusion of such accounts in Digital Treasury is in accordance with and does not violate any terms, resolutions, or agreements relating to the accounts. Client shall indemnify and hold Bank harmless against any claim, loss, damage, cost or expense including litigation expenses and reasonable attorney's fees resulting from a breach of the representation and warranty in this Section k or resulting in any way from the inclusion of the account in Digital Treasury.

l. Loan Payments & Advances. Client may have the opportunity to request access to loan accounts through Digital Treasury to perform the following functions:

i. apply a payment to their loan obligation via one of the accounts available from the Digital Treasury application; and/or

ii. loan advance service for loan eligible accounts to a deposit account established and entitled in the Digital Treasury application. Loan advances will be subject to applicable limits or availability per terms of the loan.

m. Commercial Card Accounts. If any commercial card, credit card, or purchasing card accounts are added to Digital Treasury, reporting and transaction information for such accounts will be available within Digital Treasury.

6. Wire Service. If Client enrolls a DLA or CPMMA for wire service within Digital Treasury, the Truist Wire Agreement, together with these terms and conditions and the Digital Treasury terms and conditions, will apply to wires initiated through Digital Treasury. The Truist Wire Agreement can be located within this Agreement via the Table of Contents under the Wire Service heading.

Digital Treasury Service

1. Description of Digital Treasury Service. Digital Treasury service is an internet-based information reporting and transaction initiation system providing real-time access and functionality to Client deposit accounts, and certain functionality or information related to loans or commercial card accounts ("Digital Treasury"). Digital Treasury provides Client a single access point to access account information, place stop payments, initiate certain types of payments, transfer funds between accounts, provide decision instructions for certain services, and receive notifications for Client's accounts or services. The types of payments available to be initiated (e.g. Wire, ACH Origination, and Real-Time Payments) and services available for decision instructions (e.g. Positive Pay and Reverse Positive Pay), and other services and account functions available within Digital Treasury are subject to terms and conditions specific to those services and functions and may include additional fees.
2. Introduction. Certain services that are available through Digital Treasury require separate enrollment, and Client may not use such services until enrollment is completed. Client agrees that any use of any service through Digital Treasury is subject to the applicable fees and terms and conditions for that specific service as well as these Digital Treasury terms and conditions.

   Certain access to Digital Treasury may require Client to download and agree to license agreements related to, and use certain software, including but not limited to Rapport (a secure browsing software provided by Trusteer Inc., an IBM company), as designated by Bank. Client's failure to use such software may limit Client's ability to access Digital Treasury.
3. Security Procedures. The security procedures for Digital Treasury are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.

   a. Access Credentials. Access credentials, which may include User ID, initial Password and Security Token, will be provided to the Primary Administrator established during the Digital Treasury enrollment for each designated user. Upon initial log in to Digital Treasury, each user will be required to change their initial Password to a new personal password pursuant to the instructions provided. Valid access credentials are required to log in to the service and perform transactions within the service.

   b. Dual Payment Approval. Any ACH, wire, or RTP transaction initiated through the service requires dual payment approval, which means that one authorized user with sufficient entitlements must initiate the transaction and a different authorized user with sufficient entitlements must approve the transaction in order for the transaction to be released and processed. At Client's option, Client may require additional approvals (two or more users) for such transactions.

   c. Administrative Approval. Administrative actions initiated through the service such as, but not limited to, specifying the type of payments a user can initiate or limiting payment amount by payment type or source account, must be approved by a second user with the appropriate permissions. Administrative approval entitlements in Digital Treasury are the same as those established for Truist One View. If Client elects to opt out of the administrative approval security procedure for Truist One View/Digital Treasury, Client must document this decision in writing and in accordance with Bank procedures. **Bank strongly recommends that Client not opt out of the administrative approval security procedure**.

   d. Security Token. Transactions initiated within the service (including but not limited to wire, ACH, Real-Time Payments, account transfers, and loan payments or advances) require the approval of an authenticated user with appropriate entitlements in order for the transaction to be released and processed. Authentication methods and procedures may change from time to time and will always be stated in current reference materials.
4. Administrators and Operators. The two individuals designated as Truist One View Primary Administrator also become Digital Treasury Primary Administrators at enrollment. If Client has opted out of the Truist One View administrative approval security feature, the single individual designated as the Truist One View Primary Administrator is the Primary Administrator of the Digital Treasury service. A Primary Administrator may create additional users of the service and users with administrative entitlements, who may also be referred to as Company Operators and Administrators, respectively. Once entitlements are given to Administrators and Company Operators, each will have authority to perform all actions and transactions available through Digital Treasury as granted by the entitlements. Each Company Operator and Administrator may perform any entitled

actions or transactions on Client's accounts regardless of whether they are otherwise a designated signer on any such accounts. Should Client request Bank to revoke or change a Primary Administrator, Client must notify Bank of such revocation or change as soon as possible in writing and in accordance with Bank procedures.

5. Account Information. Client can select from a variety of reporting formats that may include different combinations of account balances and activity information.

6. Account Transfers. Client may initiate current day and future dated transfers between its accounts at Bank, as may be subject to any applicable restrictions on the number of transfers governing such account(s). Bank will execute any transfer request on the value date for the transfer indicated within the service. By initiating any transfer, Client assumes full responsibility for verifying the availability of collected funds for the requested transfer date.

   Bank is under no obligation to honor, either partially or entirely, any transfer request that exceeds the available funds in Client's account. If Bank in its sole discretion creates an overdraft to complete a transfer, Client agrees to repay Bank upon demand, together with any applicable interest or fees and if necessary, the costs of collection.

7. Stop Payments. Client may initiate stop payment requests or cancellations of a stop payment order in the form and manner specified in Digital Treasury. Client must provide the account number, check serial number, exact check amount, and stop payment reason in order for the stop payment instructions to be effective. Stop payments are subject to applicable terms within the Commercial Bank Services Agreement.

8. Images of Paid Checks, Deposits & Deposited Items, and Returned Deposited Items. Through Digital Treasury, Client may view digital images of cancelled (paid) checks, deposit slips and accompanying items, and returned deposited checks. Online images may be viewed only for such periods of time as Bank may establish and older images may be sent to Client via the method specified by Bank.

   As is common industry practice with various check "truncation" or "safekeeping" services, Bank destroys the original checks but retains the images for at least the number of years required by law. If an image of a check is missing or is illegible, Bank will attempt to provide Client with a legible copy upon Client's request, if Client gives Bank adequate information to identify the specific item. However, Bank will have no liability to Client if Bank is unable to provide a copy within Client's requested timeframe, or at all, due to any reason other than Bank's gross negligence, willful misconduct or criminal conduct. Bank reserves the right to charge a fee for such requests in some circumstances, such as when the image is missing or illegible due to circumstances beyond Bank's control.

9. Alerts. With this service, Client may choose to receive alerts concerning selected types of events relating to Client's accounts or services. Client may then log on to Digital Treasury to obtain more details. Bank accepts no responsibility or liability if Client does not receive any alerts in a timely manner due to email outages or any other reason.

10. eStatements. With this service, Client may choose to receive images of Client's statements including bank statements, and other reports or information. Bank accepts no responsibility or liability if these statements or reports are not available in a timely manner due to outages or any other reason. When a deposit account is included within the service, paper statement delivery will be suppressed for such account, and the statements for such account will only be available within Digital Treasury to entitled users. **Bank strongly recommends that Client establish appropriate internal controls to monitor and review statements for deposit accounts, especially in the event that statements are only available through Digital Treasury.** If Client requires paper statement delivery for deposit accounts included within the service, Client must request paper statements from Bank and additional fees may apply.

11. Loan, Line of Credit, and Card Accounts. If any loan, line of credit, or credit, commercial, or purchasing card account types are included in Client's setup of the service, the term "account" when used in reference to the service includes these account types. By requesting the account to be included in the service, Client authorizes Bank to provide or display information relating to such loan, line of credit or card accounts within the service or to entitled users, and to provide any available functionality or service with respect to those accounts as may be requested or enabled by an entitled user, including, but not limited to, the ability to view account and transaction information, to make payments on the accounts, or to perform drawdowns, advances, or other transactions on the accounts. Client represents and warrants to Bank that inclusion of such accounts in Digital Treasury is in accordance with and does not violate any terms, resolutions, or agreements relating to the accounts. Client shall indemnify and hold Bank harmless against any claim, loss, damage, cost or expense including litigation expenses and reasonable attorney's fees resulting from a breach of the representation and warranty in this Section 11 or resulting in any way from the inclusion of the account in Digital Treasury.

12. Loan Payments & Advances. Client may have the opportunity to request access to loan accounts through Digital Treasury to perform the following functions:

a. apply a payment to their loan obligation via one of the accounts available from the Digital Treasury application; and/or

b. loan advance service for loan eligible accounts to a deposit account established and entitled in the Digital Treasury application. Loan advances will be subject to applicable limits or availability per terms of the loan.

13. Commercial Card Accounts. If any commercial card, credit card, or purchasing card accounts are added to Digital Treasury, reporting and transaction information for such accounts will be available within Digital Treasury.

Electronic Bill Presentment and Payment Service

1. Description of Electronic Bill Presentment and Payment Service. The Electronic Bill Presentment and Payment ("EBPP") service enables Client to electronically collect bill payments from Client's customers (each a "payer") by initiating ACH debit entries against a payer's deposit account or by initiating charges against a payer's credit or debit card. These ACH debit entries and credit or debit card charges (which are generically referred to in these EBPP terms and conditions as "payments") are initiated in response to payment authorizations payers submit through the internet or an Interactive Voice Response (IVR) system or give to Client's authorized users over the telephone or in person. Additional details regarding EBPP's functionality and requirements that Client must follow when using the EBPP service are provided in the EBPP reference materials.

2. Functioning of the EBPP Service. Each payment authorization that Client or a payer submits through the EBPP service will initiate a payment in accordance with these EBPP terms and conditions. Client will be the "originator" and Bank will act as the originating depository financial institution or "ODFI" for each ACH debit entry initiated. Similarly, Client will be the "merchant" for each credit or debit card charge initiated through the EBPP service. However, Bank does not act as the merchant bank processor or "acquirer" with respect to those credit or debit card charges. Instead, the EBPP service merely routes information for those credit or debit card charges to Client's third-party merchant bank processor, which will act as the acquirer for those credit or debit card charges. In order to initiate credit or debit card charges through the EBPP service Client must have entered into a merchant services agreement with a third-party merchant bank processor acceptable to Bank.

3. Origination and Processing of Payments.

   a. Payment authorizations may be submitted through the EBPP service by (i) a payer through an internet website (the "biller website") or (ii) an authorized user of Client through the biller website based on a verbal authorization a payer gives such user over the telephone or in person or (iii) a payer through an Interactive Voice Response (IVR) system. The biller website is provided by Bank as part of the EBPP service and is the website through which payments are made. Client must provide and maintain a secure link to the biller website o n Client's general website and is responsible for ensuring that this link takes a payer to the appropriate area within the biller website. Client is also responsible for providing data concerning each payer who uses this link. The link and the linking process, including the manner in which Client submits data about each payer to Bank, must also meet Bank's encryption and security requirements.

   b. A payer may submit a payment via the guest payment channel. Or, a payer may self-register directly through the biller website or may be registered as a payer through the biller website by an authorized user based on information the payer gives the user over the telephone. In addition, if the Single Sign-On option (defined below) is used, a payer who has registered on Client's general website will be automatically registered in the EBPP system. The registration process must include a commercially reasonable fraudulent transaction detection system, a commercially reasonable methodology to establish a secure internet session, and commercially reasonable procedures to verify the identity of the payer.

   c. The biller website will be formatted in accordance with the specifications Client provides to Bank. Client grants Bank the right and a license to use (i) Client's name, trademarks, service marks, copyrights and logos and other textual information in connection with the biller website and (ii) Client's data in connection with the EBPP service, in each case as contemplated by these EBPP terms and conditions. Once a payer has accessed the biller website, that payer may authorize Client to initiate a payment against the payer's deposit account or credit or debit card on the day that the authorization is submitted, each a "current payment," or to initiate one or more payments on scheduled future dates, each a "scheduled payment." Before a payer may submit a payment authorization through the biller website, that payer must accept terms regarding use of the biller website that, among other things, authorize Client as "biller" to initiate one or more payments against that payer's deposit account or credit or debit card, as applicable, and permit Client and Bank to use the data provided by the payer to process those payments, including consent for that data to be sent outside of the United States. Given the types of potential payments, such terms of use must also comply with (i) the Nacha Operating Rules and Guidelines ("ACH Rules") as they are in effect at the relevant time and (ii) the operating

regulations and other requirements of the entity or association that issues or sponsors the applicable credit or debit card as they are in effect at the relevant time, or the "card rules." Bank may provide Client sample terms of use to assist Client in drafting terms regarding use of the biller website but, subject to the foregoing requirements, the final content of such terms is Client's responsibility; Bank makes no representation or warranty regarding the correctness, suitability, or sufficiency of any sample terms of use that it may provide. Through the biller website, a payer may view scheduled payments set up in, and prior payments made through, the EBPP system and may, prior to the deadline for submitting payment authorizations set forth in the EBPP reference materials, also delete or modify scheduled payments set up in the EBPP system.

d. An authorized user of Client may also use the biller website to initiate payments against a payer's deposit account or credit or debit card based on a verbal authorization that payer gives an authorized user over the telephone, but only if (1) the payer initiated the telephone call or (2) Client has an existing business relationship with the payer as more fully described in the EBPP reference materials. Client is solely responsible for establishing the validation procedures an authorized user must follow to verify the identity of a payer and the authenticity of verbal payment or other authorizations a payer gives an authorized user over the telephone before those payment or other authorizations are submitted through the biller website. An authorized user must provide the information specified in the EBPP reference materials to the payer and obtain the payer's unambiguous verbal authorization prior to initiating a payment through the biller website. After an authorized user has initiated a payment through the biller website, the EBPP system sends the payer an email confirming the payment. Such email will be sent to the email address established at the payer's registration and reflected in the EBPP system as part of the payer's profile. This confirmation notice must comply with the ACH rules or the card rules, as applicable.

e. Each ACH debit entry initiated through the EBPP service must be originated using the applicable SEC (or Standard Entry Class) code, as described in the EBPP reference materials. The EBPP system will assign an SEC code based on information provided by the payer or an authorized user of Client when initiating the payment. ACH debits and credit or debit card charges processed through the EBPP service will be processed and debited/charged to the payer's account according to the timelines set forth in the EBPP reference materials.

f. The EBPP service will use commercially reasonable procedures to verify that the routing number associated with any ACH debit entry initiated using the EBPP service is valid.

g. Client may opt to assess surcharge fees, convenience fees, or service fees for payments processed through EBPP. Any such fees must be determined, disclosed to the payer, and collected in accordance with card network regulations and applicable law, which may vary from state to state. Bank does not advise on permissible types or amounts of fees or disclosure requirements and is not liable for any failure to follow the card network rules or applicable law, or any consequences that may result from such failure.

4. Administrative Functions. Client may use the biller website to perform certain administrative functions in connection with Client's use of the EBPP service. These functions may include registering a payer, administering a payer's registration, viewing the status of payments, deleting payments, modifying scheduled payments, receiving certain notices, generating and viewing certain transaction reports, establishing authorized users and the limits on each authorized user's authority, and downloading and uploading certain files of data. Any modification or deletion of a payment must be completed prior to the deadline for submitting payment authorizations set forth in the EBPP reference materials. Reports are available to be viewed through the biller website for the number of days set forth in the EBPP reference materials. All files uploaded or downloaded through the biller website will be transmitted to Bank or to Client as specified during implementation of the EBPP service.

5. Representations and Warranties. Client agrees that (a) for each ACH debit entry Client initiates through the EBPP service, Client must comply with all obligations of an originator of that ACH entry and Client makes all representations, warranties, and agreements set forth in the ACH rules and the terms and conditions for the ACH Origination service related to that ACH entry; and (b) for each credit or debit card charge Client initiates through the EBPP service, Client must comply with all obligations of a merchant with respect to, and Client makes all representations, warranties, and agreements set forth in the card rules related to, the credit or debit card charge. Client further represents that any payment or other authorization Client or a payer submits through the EBPP system has been authorized by the relevant payer. Client also represents and warrants to Bank that Bank's use of Client's (i) name, trademarks, service marks, copyrights and logos and other textual information in connection with the biller website and (ii) data in connection with the EBPP service, as contemplated by these EBPP terms and conditions, does not infringe or otherwise violate any intellectual property or other proprietary rights of any third party. If Client assesses any surcharge, convenience fee, or service fee (however described) on payers, Client further represents and warrants that the amount of such fees and its disclosures to payers are and will continue to be in compliance with card network regulations and applicable law.

6. Designation of Primary Administrators. Client must designate a Primary Administrator for the EBPP service. The Primary Administrator will be set up with full user permissions with respect to the biller website, including the right to administer the rights and permissions of all other users, and to create additional administrators.

7. Security Procedures. The security procedures for the EBPP service are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.

    a. Client's use of the biller website. Valid access credentials are required to log on to the biller website.

    b. Payers' use of the biller website. Except as otherwise described below for the Single Sign-On option, to access and use the biller website, a payer must log on to the biller website using that payer's valid access credentials. If a payer self-registers in the EBPP system through the biller website, the payer will select the payer's own user ID and password. If an authorized user registers a payer through the biller website, Client will designate the payer's user ID and a temporary password.

    c. Control totals. Immediately prior to transmitting the Nacha formatted file to Bank, the EBPP system will communicate the total dollar amount of the file (referred to as the "control total") to Bank through the biller website. Bank does not require that Client separately submit control totals in order to process files of ACH debit entries initiated through the EBPP service.

8. ACH Origination Service. The ACH Origination service terms and conditions are incorporated by reference herein, and all applicable provisions of such terms and conditions apply to ACH entries originated through the EBPP service. Terms that are defined in the ACH Origination terms and conditions have the same meanings when used in these EBPP terms and conditions. If there is any inconsistency on a particular issue between these EBPP terms and conditions and the ACH Origination terms and conditions, these EBPP terms and conditions will control.

9. Single Sign-On Option. Single Sign-On is an optional feature of the EBPP service that allows payers to access the biller site through Client's general website's authentication process without entering an additional user ID and password. Client's election to use the Single Sign-On feature will be designated during implementation. In order to use Single Sign-On, the authentication procedures and methodology used to establish a secure internet session employed by Client's general website must be commercially reasonable and must meet certain requirements set forth in the EBPP reference materials. Client must maintain records of the authentication of each payer who logs in to Client's general website and accesses EBPP through Single Sign-On for a minimum of five (5) years from the date of login. Such records must evidence the authentication and identification of the payer and must include, at a minimum, the payer's user name, system name, session ID, date/time stamp, and payer's IP address. Client must provide copies of such records to Bank, in a format that is satisfactory to Bank, within five (5) business days of Bank's request. Additionally, Client will be required to obtain, install and manage, at Client's own expense, a valid X.509 certificate issued by a Certificate Authority as further described in the EBPP reference materials. Client must comply with all requirements and complete all required testing and all implementation and software development tasks as further described in the EBPP reference materials. If Bank determines, in Bank's sole discretion, that Client does not meet any of the requirements or are not otherwise eligible for Single Sign-On, Client will not be permitted to use this feature of the EBPP service. Under the Single Sign-On option, payer registration and authentication, including selection and reset of user IDs and passwords, will be Client's responsibility and will take place within Client's general website. If Client uses Single Sign-On, Client is responsible for the actions of any person who accesses the biller site and/or the EBPP system through Client's general website, including any unauthorized payments initiated by such person. In addition to any other indemnity obligation Client has under this Agreement and to the extent permitted by applicable law, Client agrees to indemnify and hold Bank harmless from and against any claims, liabilities, losses, damages, costs and expenses (including, without limitation, attorneys' fees) arising from or related to any person's access to the biller site and/or the EBPP system through Client's general website, including but not limited to any losses resulting from the breach or failure of the security features of Client's general website or Client's failure to comply with any requirements for Single Sign-On contained in this Agreement, including requirements set forth in the EBPP reference materials.

10. Effective Date. The EBPP service is replacing Online Bill Presentment and Payment ("OBPP"). For OBPP users, these EBPP service terms apply from the implementation of EBPP and the OBPP service terms will continue to apply until then.

Electronic Data Interchange Service

1. Description of Electronic Data Interchange Service. Electronic Data Interchange ("EDI") refers to the electronic exchange of payments, payment-related information and other financial data in formats that meet certain standards. The EDI services that Bank offers fall into the following three categories: payment initiation, payment receipts or "electronic receivables delivery", and financial reporting services. Client may select one or more types of EDI service and will designate which accounts are associated with each service. The EDI services are described below:

a. Payment Initiation. Client provides an electronic file to Bank in order to initiate entries through Bank's ACH Origination service and/or create paper checks through Bank's Integrated Payables service.

b. Payment Receipts. Bank sends Client an electronic reporting file via direct transmission containing payment and payment-related data relating to Client's ACH Origination and/or lockbox service(s) to Client in various formats as selected by Client. ACH Origination payment and payment-related data may also be provided in a Human Readable report.

c. Financial Reporting. Client can send and receive electronic files related to Bank's Account Reconciliation Plan, Controlled Payment Reconciliation and Positive Pay services (both issue and paid item files), and ACH Fraud Control service (authorization records). Client may also elect to receive a file of Account Analysis billing data though EDI.

2. Files Bank receives from Client or sends to Client via EDI services must be in a format that Bank has tested and agreed to and must be sent or received by the applicable deadlines for the relevant service to allow Bank to perform the necessary edits and process and/or forward the files for the relevant payment or information purposes. The terms and conditions for each service that is utilized through or in connection with an EDI file apply to Client's use of such service.

Electronic Lockbox Service

1. Description of Electronic Lockbox Service. The Electronic Lockbox service enables Client to receive remittance information regarding payments sent to Client through the online bill payment service of any third-party online payment processor (each, an "online payment processor") who participates in the Electronic Lockbox service. Client's designation of accounts and online payment processors for the service are reflected on a Treasury Request Confirmation. Details regarding the functionality and requirements of the service are provided in the Electronic Lockbox reference materials.

2. Enrolling as a Biller.

   a. Client authorizes Bank to establish a "biller profile" for each designated online payment processor using information Client provides to Bank. If Client's discovers that any information in its biller profile is inaccurate or needs to be revised, Client must notify Bank immediately and take any required steps to modify or correct the information and adjust any funds incorrectly remitted to Client as a result of such incomplete or inaccurate information.

   b. Client represents and warrants to Bank that Client does not owe any outstanding amounts to an online payment processor and that Client is not currently using (and, as long as Bank provides the Electronic Lockbox service to Client, will not use) the services of any other financial institution to enroll in or otherwise obtain access to the online bill payment service for the same online payment processor(s) as those that are reported by Bank.

3. Remittance Files; Settlement; Reconcilement; Posting.

   a. Once Client has been enrolled as a biller and Bank has implemented Electronic Lockbox service for Client for the applicable online payment processor(s), the online payment processor(s) will send Bank remittance information for payments sent to Client through the applicable online bill payment service. Bank will reformat the information and send a "remittance file" of such information to Client. Client may designate whether Bank sends remittance files to Client as a separate transmission, appended to another product's file, or available for download in the Electronic Lockbox web application.

   b. Bank will settle all payments sent to Client in each remittance file via ACH credit to Client's designated settlement account. ACH credits to Client's settlement account are considered provisional until Bank receives final settlement from the applicable online payment processor. All payments credited to Client's settlement account, or otherwise owed to Client related to an online payment processor's online bill payment service are subject to any rights that online payment processor may have to unwind transactions and exercise setoff under that online payment processor's terms, including the right to reversals.

   c. Client is responsible for reconciling the remittance information to the ACH settlement credit each day. If Client is unable to reconcile the two, Client must notify Bank of the inconsistencies by the end of the banking day on the day of settlement. If Client notifies Bank in the time required, Bank will assist Client with any research requests to the applicable online payment processor regarding the inconsistencies.

4. Returns and Reversals.

   a. If Client is unable to successfully post a payment, then Client must return such payment through the Electronic Lockbox Returns function as described in the Electronic Lockbox reference materials.

b. Unless "guaranteed payment" (offered by some online payment processors) applies, processors can initiate reversals of payments previously made to Client through that online payment processor's online bill payment service. Reversals received from the processors will be debited from Client's settlement account via ACH and reported to Client within the Electronic Lockbox web application. Bank will not have any liability for any reversals processed through an online payment processor's online bill payment service.

5. Limitation of Liability; Disclaimer; Indemnity. In addition to any other limits on Bank's liability in this agreement and to the extent permitted by applicable law, Client agrees that Bank will not have any liability for any acts or omissions of an online payment processor (including, without limitation, (a) any error or delay in processing any payments or remittance information, including any error or delay in initiating any funds transfers to Client, (b) any breach of confidentiality of any information, including any of Client's or Client's customers' payment, account or personal information, (c) the inaccuracy of any remittance information, or (d) any reversals or other debits initiated against Client's account). In addition to any other indemnity obligation Client has under this Agreement and to the extent permitted by applicable law, Client agrees to indemnify and hold Bank harmless from and against any claims, liabilities, losses, damages, costs and expenses (including, without limitations, attorneys' fees) arising from or related to (i) any amounts or other obligations Bank owes an online payment processor that are related in any way to Client's use of that online payment processor's online bill payment service, (ii) faulty or erroneous information or instructions Client gives Bank or an online payment processor, (iii) any of Client's errors or delays in posting a payment to Client's accounts receivable system, (iv) any breach of Client's obligations under these Electronic Lockbox terms and conditions, or (v) any of Client's acts or omissions which result in a breach by Client or Bank of the terms of any online payment processor's documentation.

6. Online Payment Processor Documentation. Client's use of the Electronic Lockbox service is subject to the terms of each online payment processor's documentation. Client agrees to take all actions Bank or such processor deem necessary for compliance with each online payment processor's documentation. Client agrees that the Bank is not obligated to take any action under these Electronic Lockbox terms and conditions that would cause Bank to breach the provisions of any online payment processor's documentation. Client agrees that none of Bank's obligations under any online payment processor's documentation create obligations for Bank under these Electronic Lockbox terms and conditions unless expressly set forth as Bank's obligations in these Electronic Lockbox terms and conditions.

7. Electronic Lockbox Web Application. The Electronic Lockbox web application provides internet-based access to Client's online bill payment detail with flexible viewing parameters and search capability with 2 years of historical data. This web application allows users to change their passwords, download posting files, create stops or swaps, view reports and return invalid transactions. Client's Primary Administrator is responsible for setting up and maintaining Client's users' access to the application, which includes various roles for users.

8. Additional Services. The following features are optional for Electronic Lockbox:

   a. HOA (Homeowner Association)/Property Management Multi DDA-ability to post to multiple DDAs but under one Company ID (note: Client must have ability to provide HOA table or validation file).

   b. Validation/Stop File-allows more valid accounts to post and or stop invalid accounts from posting (note: Client must provide validation or stop file).

   c. Web Exceptions-ability for Client to decision items that would otherwise be returned to the payor because they do not pass Client's validation file (note: Client must provide validation file to have Web Exceptions).

Image Cash Letter

1. Description of Image Cash Letter Service. The Image Cash Letter ("ICL") service allows Client to transmit files containing electronic images of batches of checks and associated information describing each check along with check total information in place of forwarding the original checks to Bank for deposit. Each image and its associated information is an "Image" and a file containing Images and associated information is a "Letter". Details regarding ICL's functionality and certain formatting and other technical requirements that Client must follow when using ICL are provided in the ICL reference materials (which include, but are not limited to, a user guide). ICL is intended for transmission of Client's Images in a single file, not as separate transmissions for each Image. The ICL service may also encompass image quality analysis adjustments, image integrity analysis adjustments, duplicate item or duplicate file adjustments, and return item adjustments all as defined in the ICL reference materials. Client shall not use the ICL service outside the United States or to transmit files from outside the United States without Bank's prior written approval, or to transmit an electronic image of a remotely created check (as that term is defined in Regulation CC of the Federal Reserve Board, "Reg CC"). These ICL terms and conditions do not otherwise affect any other agreement between Client and Bank relating to the deposit of original checks.

2. Operation of the ICL Service. Client may use the ICL service with respect to the account(s) designated for the service.

   a. Each Image within a Letter is an "item" as defined in the Uniform Commercial Code as adopted in the state whose laws govern this Agreement and a "check" as defined in Reg CC, and each Image will be negotiated as such. Each Image must contain an exact image of the front and back of the original check with full-field magnetic ink character recognition (MICR) line encoding (absent the amount). Client should endorse the original check prior to image capture and Client must provide an electronic endorsement record in accordance with the ICL reference materials. Each Letter must be formatted as provided in the ICL reference materials, including but not limited to the batching of images, file specification requirements (including a Cash Letter Control Record) and use of standard American National Standards Institute's ("ANSI") file formats. To be eligible for processing, an Image must meet the requirements for items eligible for exchange as outlined in the ICL reference materials. At a minimum, the original documents of any Image must be a negotiable instrument the Uniform Commercial Code and all characters in all magnetic ink character recognition ("MICR") fields present on each document must be readable. It is not acceptable to pass digit errors (represented by an * within a MICR field) to Bank on any Image sent to Bank. All fields on the MICR line of an Image must be repaired prior to forwarding any Letters to Bank. Client warrants that any repair of the MICR line fields will be repaired accurately.

   b. Client must transmit each Letter to Bank through one of Bank's online services. To submit a Letter to Bank, Client is required to comply with applicable security procedures for that online service, including but not limited to use of valid access credentials to log in to the online service. Any Letter transmitted to Bank in accordance with those security procedures will be deemed a Letter submitted by Client. Transmission times, Letter receipt times, other applicable deadlines and transmission locations are set forth in the ICL reference materials.

   c. Each Letter and the Images contained therein must meet Bank's quality standards for processing as described in the ICL reference materials. Those standards are referred to in these ICL terms and conditions as the "ICL standards." Bank may add to or change the ICL standards at any time upon notice to Client. Once Bank receives Client's Letter, Bank will process each Image in that Letter that are "on-us" items (meaning that the items are drawn on Truist Bank). Bank offers qualified and unqualified versions of the ICL service. In order to use the "qualified ICL service", a version of the ICL service that does not require Bank to perform additional image quality analysis and image integrity analysis, Client must represent to Bank that Client's imaging process verifies that the Images included in a File meet Bank's ICL standards and any other applicable image quality or other standards as required in the ICL reference materials. If Client's imaging process does not produce acceptable images, Client will be required to use Bank's "unqualified ICL service" which is a version of the ICL service that performs image quality analysis and image integrity analysis on all items in each Letter. The unqualified ICL service may require an earlier file receipt time as described in the ICL reference materials. All Letters are also subject to duplicate item and duplicate file detection Bank may perform at Bank's discretion, but the responsibility for not submitting duplicates is solely Client's responsibility and Bank assumes no responsibility if Bank's process fails to detect any duplicate. If Image and associated information satisfies the ICL standards, then the Letter will be accepted, and Bank will begin processing the contents of the Letter. If Bank determines an Image or the associated information does not satisfy the ICL standards, the Image may be rejected and dropped from the Letter or the Letter, and all Images contained therein, may be rejected. A summary debit adjustment will be made to Client's account and a debit advice will be sent to Client.

   d. In addition, any Image and associated information included in a Letter must satisfy the quality standards of the Federal Reserve Bank or other collecting bank to which Bank forwards an Image and associated information for collection, the "collecting bank quality standards." Collecting bank quality standards include the parameters of Images relative to length, height, corners, document skew, darkness/lightness, noise and Image size compression. These standards are provided in the reference materials. Image quality adjustment detail reporting will be facilitated through the use of Bank's Online Courier service if Client elects to use that service. All Images failing to meet collecting bank quality standards will be sent to Client as a return advice. There are no specific timelines for these types of adjustments, but they are usually completed within 30 business days of deposit.

   e. If an Image is rejected for failing to meet the ICL standards or the collecting bank quality standards, Client must take corrective action to either recapture the Image and associated information and submit it in a new Letter or submit the original check for deposit. Once Client has transmitted a Letter to Bank, Client may not cancel it unless Bank has rejected the Letter or Images in the Letter. If more than two percent of the Images in a Letter fail to meet the ICL standards, the entire Letter may be rejected, which will require Client to resubmit that Letter.

   f. Once Bank has accepted a Letter for processing, Bank will use each Image in that Letter to process the Image as an electronic item or, at Bank's option, to create a substitute check (as defined in Reg CC). If Bank elects to process an Image as an electronic item, Bank will process that Image for deposit to Client's account and forward it for presentment to the drawee bank (as defined below) through the electronic item collection channels that Bank would otherwise use to present an electronic item to the drawee bank. If Bank uses an Image to create a substitute check, then Bank will process

that substitute check for deposit to Client's account and forward it for presentment to the financial institution on which the original check was drawn or through or at which it was payable (that institution is referred to in these ICL terms and conditions as the "drawee bank") through the check collection channels that Bank would otherwise use to present a check to the drawee bank. In either event, Client's deposit will be subject to the terms of any agreement Bank has with other financial institutions relating to the presentation of electronic items, and subject to all applicable terms of the Uniform Commercial Code and the Truist Commercial Bank Services Agreement relating to processing of the items. Bank will make funds for each electronic item or substitute check that Bank processes for deposit to Client's account available to Client under the float schedule assigned to Client's account based on the banking day that Bank received the Letter containing a conforming Image of that check; assigned account-specific float schedules are available upon request.

g. Bank must receive Client's Letter by the receipt times set forth in the ICL reference materials. In that regard, Bank is not liable for any delays or errors in transmission of a Letter. If the online service Client uses to transmit Client's Letter is not available, Client must make Client's deposits by another method. Client may not transmit to Bank a Letter which exceeds 20,000 items per file if Client is using the unqualified ICL service, or 25,000 items per file if Client is using the qualified ICL service. Client may, however, send more than one Letter each day prior to the applicable receipt time.

h. Client agrees to make original checks available to Bank promptly upon request. Client agrees that Client will not capture more than one Image of any original check and that Client will not negotiate, deposit or otherwise transfer any original check to Bank or to any other person or entity after Client has captured an Image of the check. Client also agrees that (i) Client will not transmit an Image of any original check to Bank more than once (unless that item has been returned to Client by Bank for corrective action), (ii) Client will not transmit an Image of any original check to Bank that Client previously transmitted to any other person or entity, (iii) Client will not transmit an Image of any original check to any other person or entity after Client has transmitted it to Bank; (iv) Client will not transmit an Image of any original check to Bank if that check has been used as a source document for the initiation of an Automated Clearing House ("ACH") or other electronic debit; and (v) Client will not use any original check as a source document for the initiation of an ACH or other electronic debit after Client has transmitted an Image of that check to Bank. Client agrees to use commercially reasonable procedures to safeguard the original checks, images and associated information in Client's possession to ensure such checks are not negotiated beyond ICL.

i. If there is any discrepancy between the Image count and/or the total dollar amount of the Letter and Bank's count of Images and/or the total dollar amount of Images included in the Letter, Bank's count will control and the Letter may be rejected. Bank will also debit Client's account and send Client a deposit adjustment notice for any image which was rejected by Bank for failing the ICL standards, was determined to be a duplicate, or rejected for failing the collecting bank quality standards, or returned by any collecting bank for any reason.

j. Bank may reject, impose a special fee and/or delay processing of any Letter if (i) the Letter was not prepared and formatted in accordance with the requirements set forth in the ICL reference materials or does not otherwise meet the requirements contained in these terms and conditions, (ii) the number of Images in the Letter or the total dollar amount of the Letter does not match what is included in the Letter control record for the Letter delivered to the Bank and as more particularly described in the reference materials, or (iii) the number of Images in a Letter transmitted to Bank exceeds the number permitted under these ICL terms and conditions.

k. Returns will be handled by printing substitute checks and returning them through existing return channels.

3. Client's Representations and Warranties. Client makes all of the representations and warranties to Bank with respect to each Image and associated information that Client transmits to Bank that Client would have made if Client had deposited the original check into Client's account. In addition, Client represents and warrants to Bank with respect to each Image and associated information that Client transmits to Bank that (a) the Image and associated information (i) accurately represent all of the information on the front and back of the original check at the time the Image and associated information were captured and (ii) are otherwise sufficient for Bank to satisfy Bank's obligations as the truncating and/or reconverting bank, and (b) no person or entity will receive a transfer, presentment or return of, or otherwise be charged for, (i) the original check, (ii) an electronic item or substitute check that Bank creates from the image and associated information, or (iii) a paper or electronic representation of the original check or of a substitute check that Bank creates from the image and associated information, such that the person or entity will be asked to make a payment based on a check that it has already paid.

4. Client's Indemnification Obligations. In addition to any other obligation Client has to indemnify Bank, Client agrees to indemnify and hold Bank and Bank's affiliates harmless from and against any and all liabilities, claims, damages, losses, demands, fines (including those imposed by any Federal Reserve Bank, clearing house or funds transfer system), judgments, disputes, costs, charges and expenses (including litigation expenses, other costs of investigation or defense and reasonable attorneys' fees) which relate in any way to (a) the receipt by any person or entity of (i) an electronic item, (ii) a substitute check or (iii) a paper or electronic representation of the original check or the substitute check that Bank creates from an

electronic check image and associated information that Client transmits to Bank, instead of the original check, or (b) any encoding error on any check included in an image cash letter, or (c) any duplicate item or duplicate file created or authorized by Client, or (d) the delayed processing of any returned items by any subsequent bank for any items that were processed as electronic items, or (e) a remotely created check being included in an image cash letter.

Image Cash Letter Service for Web Instaposit Users

1. Description of Image Cash Letter Service for Web Instaposit User. The Image Cash Letter for Web Instaposit ("Instaposit") service allows Client to use the ICL service by submitting Images and Letters through Web Instaposit, an internet based web portal, in place of presenting the original checks to Bank for deposit. Details regarding Instaposit's functionality and certain formatting, transmittal and processing instructions, and other technical requirements that Client must follow when using the Instaposit service are provided during implementation of the service and/or within the Web Instaposit portal and are referred to as the "Instaposit reference materials." These Instaposit terms and conditions do not otherwise affect any other agreement between Client and Bank relating to the deposit of original checks.
2. ICL Terms and Conditions. The ICL terms and conditions are incorporated herein and apply to use of the Instaposit service, except as stated otherwise in these Instaposit terms and conditions or in the Instaposit reference materials. Terms defined in the ICL terms and conditions and used herein shall have the meanings set forth in the ICL terms and conditions. Web Instaposit is one of the online services used to transmit Letters to Bank per the ICL terms and conditions. By transmitting an Image to Bank via Web Instaposit, Client makes all the representations and agreements with respect to the Image as contained in the ICL terms and conditions, and agrees to the indemnification obligations set forth in the ICL terms and conditions. Once Bank receives a Letter, it will be processed according to the applicable ICL terms and conditions. All image quality and file specification requirements within the ICL terms and conditions apply to the Images transmitted via Web Instaposit, and Bank may delay processing of or reject any Image or Letter that fails to meet such requirements or for any other reason set forth in the ICL terms and conditions.
3. Rejections and Returns. Bank shall provide notice of any rejected or adjusted Images or Letters according to Client's instructions or, if Client has not provided instructions to Bank for delivery of such notices, Bank may provide the notice to Client per Client's contact information (according to Bank's records).

Image Cash Letter Service for Financial Institutions

1. Description of Image Cash Letter Service for Financial Institutions. The Image Cash Letter for financial institutions or "ICL-FI" service allows Client to transmit files containing electronic images of batches of checks and associated information describing each check referred to as "presentment notice") along with check total information, (each such file an "image cash letter,") in place of forwarding the original checks to Bank for deposit. Details regarding ICL-FI's functionality and certain formatting and other technical requirements that Client must follow when using ICL-FI are provided in the ECCHO Rules (as defined herein), Section XIX and in the ICL-FI reference materials. By using this service, Client agrees to be bound by the Electronic Check Clearing House Organization Operating Rules referred to as "ECCHO Rules" for these electronic image transactions and Bank will sponsor Client's membership if Client is not currently a member of ECCHO. ECCHO Rules can be obtained at www.eccho.org. Unless otherwise agreed upon, Client will be charged for the ECCHO sponsorship fees. Unless otherwise indicated, terms used in these ICL-FI terms and conditions shall have the meanings ascribed to such terms in the ECCHO Rules. The ICL-FI service is intended for transmission of Client's presentment notice and electronic images in a single file, not as separate transmissions. The ICL-FI service may also encompass image quality analysis adjustments, image integrity analysis adjustments, duplicate item or duplicate file adjustments, and return items adjustments all as defined in the ICL reference materials. Client shall not use the ICL-FI service outside the United States and files may not be submitted from outside the United States without Bank's prior written approval, or to transmit an electronic image of a remotely created check (as that term is defined in Regulation CC of the Federal Reserve Board, "Reg CC"). These ICL-FI terms and conditions do not otherwise affect any other agreement between Client and Bank relating to exchanges under the ECCHO Rules or deposit of original checks.
2. Operation of the ICL-FI Service. Client may use the ICL-FI Service with respect to the account(s) designated for the service.
    a. Each electronic check image included in an image cash letter is an "item" under the Uniform Commercial Code, a "check" under Reg CC and an "item" under ECCHO Rules which must be an exact image of the front and back of the original check with full magnetic ink character recognition ("MICR") line information. Client must endorse the original check or the electronic check image with the bank of first deposit endorsement in accordance with standard American National Standards Institute's ("ANSI") endorsement requirements, ECCHO Rules and ICL-FI reference materials. Each image cash letter must be formatted, including the batching of images, as provided in the ECCHO Rules and the ICL-FI

reference materials. To be eligible for processing, an electronic check image must meet the items eligible for exchange requirements as outlined in the ECCHO Rules, Section III (A). The ECCHO Rules require, at a minimum, that the item be a negotiable item, and all characters in all MICR fields present on the document must be readable. This will allow Client to capture the information required for the image cash letter. Repair of the MICR line on documents in order to make the items eligible for processing must be done with responsibilities assigned as outlined in ECCHO Rules, Section III(B). It is not acceptable to pass digit errors to Bank (represented by an * within a MICR field) on any file forwarded to Bank. All fields on the document must be repaired prior to forwarding any files. Repair of the MICR line fields will be governed by ECCHO Rules.

b. Client must transmit each image cash letter to Bank through one of Bank's online services which support the transmission of image cash letters**.** To submit an image cash letter to Bank through an online service, Client is required to comply with the security procedures for that online service. Any image cash letter transmitted to Bank in accordance with those security procedures will be deemed an image cash letter submitted by Client. Transmission times, cutoff times, other applicable deadlines and transmission locations are set forth in the ICL-FI reference materials.

c. Each image of (and associated information regarding a check) included in an image cash letter must meet Bank's quality standards for processing an image for deposit as described in the ECCHO Rules and the ICL- FI reference materials. Those standards are referred to in these ICL-FI terms and conditions as the "ICL-FI standards." Bank may add to or change the ICL-FI standards at any time upon notice to Client. Once Bank receives Client's image cash letter, Bank will process each image and associated information included in that image cash letter that are "on-us" items (meaning that the items are drawn on Truist Bank). Bank offers qualified and unqualified versions of the ICL-FI service. In order to use the "qualified ICL-FI service", a version of the service that does not require Bank to perform additional image quality analysis and image integrity analysis, Client must represent to Bank that Client's imaging process verifies that the images in an image cash letter meet Bank's ICL-FI standards and any other applicable image quality or other standards as required in the reference materials. If Client's imaging process does not produce acceptable images, Client will be required to use Bank's "unqualified ICL-FI service", the version of the service that performs image quality analysis and image integrity analysis on all items in each image cash letter. The unqualified ICL-FI service may require an earlier file receipt time as described in the ICL-FI reference materials. All image cash letters are also subject to duplicate item and duplicate file detection Bank may perform at Bank's discretion, but the responsibility for not submitting duplicates is solely Client's responsibility and Bank assumes no responsibility if Bank's process fails to detect any duplicate. If the images and associated information satisfies the ICL-FI standards, then the image cash letter will be accepted, and Bank will begin processing the contents of the image cash letter. If Bank determines an image or associated information does not satisfy the ICL-FI standards, the image may be rejected, which shall mean those items are sent back to Client for reasons of poor quality or missing images, and Bank will provide Client with a list of rejected images and a research and adjustment debit advice. In addition, any image and associated information included in an image cash letter must satisfy the quality standards of the Federal Reserve Bank or other collecting bank to which Bank has forwarded an image and associated information for collection, the "collecting bank standards." All check images which fail to meet Federal Reserve Bank quality standards will be returned as an advice to Client. All check images which fail to meet collecting bank quality standards will result in items coming back to Client in return item processing. If an image is rejected for failing to meet the ICL-FI standards or the collecting bank standards, Client must either recapture the image and associated information and submit it in a new image cash letter or submit the original check for deposit. Once Client has transmitted an image cash letter to Bank, Client may not cancel it.

d. Once Bank has received an image cash letter for deposit, Bank will use each image and associated information included in that deposit to create a substitute check (as defined in Reg CC) or, at Bank's option, process it as an electronic item. If Bank uses an image and associated information to create a substitute check, Bank will process that substitute check for deposit to Client's account and forward it for presentment to the financial institution on which the original check was drawn or at which it was payable (that institution is referred to in these ICL-FI terms and conditions as the "drawee bank") through the check collection channels that Bank would otherwise use to present a check to the drawee bank. If Bank elects to process an image and associated information as an electronic item, Bank will process that image for deposit to Client's account and forward it for presentment to the paying bank through the electronic item collection channels that Bank would otherwise use to present an electronic item to the paying bank. In either event, Client's deposit will be subject to the terms of any agreement Bank has with other financial institutions relating to the presentation of electronic items, and subject to all applicable terms of the Uniform Commercial Code and the Truist Commercial Bank Services Agreement relating to processing of the items. Bank will make funds for each substitute check or electronic item that Bank processes for deposit to Client's account available to Client under the float schedule assigned to Client's account based on the banking day that Bank received the file containing a conforming image of that check.

e. Bank must receive Client's image cash letter by the deadline set forth in the ICL-FI reference materials. In that regard, Bank is not liable for any delays or errors in transmission of an image cash letter. If the online service Client uses to

transmit Client's image cash letter is not available, Client must make Client's deposits by another method. Client may not transmit to Bank an image cash letter which exceeds 20,000 items per file if Client is using the unqualified ICL-FI service, or 25,000 items per file if Client is using the qualified ICL- FI service. Client may, however, send more than one image cash letter each day prior to the applicable receipt time.

f. Client agrees to make original checks available to Bank promptly upon Bank's request. Client agrees that Client will not capture, nor will Client allow any of Client's customers to capture, more than one image of any original check and that Client will not negotiate, deposit or otherwise transfer, or allow any of Client's customers to negotiate, deposit or transfer, any original check to Bank or to any other person or entity after Client (or Client's customer) has captured an image of the check. Client also agrees that (i) Client will not transmit an image of any original check to Bank more than once (unless that item has been returned to Client by Bank for corrective action), (ii) Client will not transmit an image of any original check to Bank that Client or one of Client's customers has previously transmitted to any other person or entity, (iii) neither Client nor any of Client's customers will transmit an image of any original check to any other person or entity after Client has transmitted it to Bank; (iv) Client will not transmit an image of any original check to Bank if that check has been used as a source document for the initiation of an Automated Clearing House ("ACH") or other electronic debit; and (v) neither Client nor any of Client's customers will use any original check as a source document for the initiation of an ACH or other electronic debit after Client has transmitted an image of that check to Bank. Client agrees to use and cause Client's customers to use commercially reasonable security procedures to safeguard the original checks, images and associated information to ensure such checks are not negotiated beyond ICL-FI.

g. If there is any discrepancy between check image count and/or the total dollar amounts of the deposit reflected by Client in an image cash letter and Bank's count of check images and/or the total dollar amount of images included in the image cash letter, Bank's count will control and the image cash letter may be rejected. Bank will also debit Client's account and send Client a deposit adjustment notice for any image which was rejected by Bank for failing the ICL-FI standards, was determined to be a duplicate, rejected for failing the Federal Reserve Bank quality standards or the collecting bank standards, or returned by any collecting bank for any reason.

h. Bank may reject, impose a special fee and/or delay processing of any image cash letter if (i) the image cash letter was not prepared and formatted in accordance with the requirements set forth in the ECCHO Rules and ICL-FI reference materials or does not otherwise meet the requirements contained in these terms and conditions, (ii) the number of checks images or batches of check images in the image cash letter, the dollar amount of a batch of check images in an image cash letter or the total dollar amount of the image cash letter does not match what is included in the presentment notice for that image cash letter, or (iii) the number of check images in all image cash letter files transmitted to Bank exceeds the number permitted under these ICL-FI terms and conditions. Returns will be handled by printing substitute check documents and returning them through existing paper return channels. As a financial institution, Client acts as the bank of first deposit ("BOFD") on all items Client deposits with Bank. This will require Client to place a BOFD endorsement on all physical items deposited and/or a 26 record containing the BOFD record on all image cash letter items deposited with Bank. This endorsement must be in compliance with Reg CC regarding content and placement, ANSI x9.37 standards, and as provided in ECCHO Rules Section XIX (E).

i. As the BOFD, Client is expected to be the primary point of resolution of all research items. As the BOFD, Client's organization has total access to the clearing cycle of each item deposited with Bank. As Client's clearing agent, Bank does not have access to all of the returns information and as such Bank is less able to resolve all research items. Client may re-deposit indemnified copies of previously missing items with Bank at any time through any depository channel.

3. Client's Representations and Warranties. Client makes all of the representations and warranties to Bank with respect to each electronic check image and associated information that Client transmits to Bank that Client would have made if Client had deposited the original check into Client's account. Client further agrees to the Sending Bank Warranties and Indemnification as provided in ECCHO Rules Section XIX (M).

4. Client's Indemnification Obligations. In addition to any other obligation Client has to indemnify Bank, Client agrees to indemnify and hold Bank and Bank's affiliates harmless from and against any and all liabilities, claims, damages, losses, demands, fines (including those imposed by any Federal Reserve Bank, clearing house or funds transfer system), judgments, disputes, costs, charges and expenses (including litigation expenses, other costs of investigation or defense and reasonable attorneys' fees) which relate in any way to (a) the receipt by any person or entity of (i) an electronic item, (ii) a substitute check or (iii) a paper or electronic representation of the original check or the substitute check that Bank creates from an electronic check image and associated information that Client transmits to Bank, instead of the original check, or (b) any encoding error on any check included in an image cash letter, or (c) any duplicate item or duplicate file created or authorized by Client, or (d) the delayed processing of any returned items by any subsequent bank for any items that were processed as electronic items, or (e) a remotely created check being included in an image cash letter.

Image Statement Transmission Service

1. Description of Image Statement Transmission Service. This service provides delivery of checking and savings account statements for designated accounts via data transmission. Image Statement Transmission provides a zip file of all PDF statements with the same end cycle dates. Client will receive the transmission the day following the end statement cycle date. Details regarding Image and Statement Transmission's functionality and formatting are provided in the Image Statement Transmission reference materials.
2. Paper DDA Statement Suppression. Paper checking and savings statements for all accounts included in Image Statement Transmission are automatically suppressed. Suppression will begin upon successful completion of the transmission testing. In the event Client opts to receive a paper statement as well as Image Statement Transmission for any account, additional fees will apply.

Integrated Payables Service

1. Description of Integrated Payables Service. The Integrated Payables ("IP") service is a service where, in accordance with Client's service elections, Bank will print and disburse checks, create and transmit entries to settle through the Automated Clearing House ("ACH") Network, initiate U.S. Dollar wire transfers, and/or create and process commercial card payments to pay Client's designated payees. Details regarding the functionality of the IP service, file delivery methodology, security procedures, and certain formatting and other technical requirements that Client must follow when using the IP service are provided in the IP reference materials. Client must designate a Primary Administrator for IP within a Primary Administrator Designation agreement (or other similar agreement accepted by Bank).
2. Processing of Payments.
    a. For each payment entry included in an IP data file Client transmits to Bank, Bank will print and disburse a check, create and transmit an ACH credit entry or a commercial card payment, or initiate a U.S Dollar wire transfer payment. Each payment entry will be drawn on or settle to the applicable designated account. Client's use of each payment type within the IP service is subject to Bank's approval and completion of any additional documentation or agreements relating to the payment type that may be required by Bank.
    b. For each payment entry to be paid by check, the check will be printed in accordance with the format specifications established between Client and Bank. Checks can be denominated in U.S. dollars only, or, if the check is drawn on a Canadian currency account, in Canadian dollars. Bank will disburse checks by either U.S. mail or courier as designated by Client, with associated costs passed through to Client. Bank shall have no responsibility for any checks once delivered to the United States Postal Service or Client's courier.
    c. For each payment entry to be paid via ACH credit entry, Client will be the originator of the ACH entry Bank creates from Client's IP data file. The ACH Origination service terms and conditions are incorporated by reference herein, and all applicable provisions of such terms and conditions apply to ACH entries originated through the IP service. Terms that are defined in the ACH Origination terms and conditions have the same meanings when used in these IP terms and conditions.
    d. For each payment entry to be paid via U.S Dollar wire transfer, Client will be the authorized sender of the payment order Bank initiates from Client's IP data file. The Truist Wire Agreement is incorporated by reference herein, and all applicable provisions of such Wire Agreement apply to wire transfers initiated through the IP service. Terms that are defined in the Wire Agreement have the same meanings when used in these IP terms and conditions.
    e. In order to include commercial card payables files in the IP data file, Bank must have agreed to provide Client a commercial card account and Bank's associated card program management solution. Client must execute a Commercial Card Agreement with Bank and any additional documentation Bank may require relating to the card program management solution (together, the "Commercial Card Agreements"). The Commercial Card Agreements are incorporated by reference herein, and all applicable provisions of the Commercial Card Agreements apply to commercial card payments transmitted through the IP service.
    f. Remittance data included with Client's IP data file may be printed with the corresponding checks, made available at Bank's designated website for a registered payee, emailed to a registered payee or sent by separate mailing for ACH entries or U.S. Dollar wire transfers to the payee at the address provided by Client.

3. Transmission of Client's Integrated Payables Data File. Client must transmit the IP data file to Bank (i) through a designated website or (ii) through Straight Through Processing ("STP") by using Bank's File Transfer transmission method, as more specifically described in the reference materials. As used herein, "File Transfer" means the secure transmission of files to and from Bank using an internet browser or secure FTP (File Transfer Protocol). The File Transfer transmission method may also be referred to as "direct transmission." If the IP data file requires file translation before it can be processed by Bank, one of Bank's file translation services must be used to translate the file into a format that can be processed. Client must transmit the IP data file to Bank by the cut-off deadline established by Bank; otherwise, the IP data file may not be processed or processing may be delayed. In order to make a change to Client's IP data file (other than adding one or more payment entries), including changes in formatting, adding an account, or changing the settlement account for a payment entry, Client must test the changes with Bank, to Bank's satisfaction, before transmitting a data file containing the changes; failure to test a changed IP data file may result in the data file not processing or delay in processing. Bank will notify Client each time an IP data file is received. Client is required to validate and/or provide control totals to release the file for processing, as described in Section 5 below.

   Client is responsible for payment entries included in IP data file that are submitted and released for processing according to the terms herein, even if the payment entry is a duplicate of another payment entry or otherwise is submitted in error. Bank is under no obligation to determine if an IP data file or any payment entry in an IP data file is a duplicate of a previously submitted IP data file or payment entry. For files sent to Bank using File Transfer, Client must provide Bank with all IP addresses from which files will be sent and must update these IP addresses when changes are made, as Bank's system will recognize and process only files transmitted from an IP address that Client has provided to Bank. Client will designate individuals that Bank may contact to resolve processing issues with Client's IP data files and Client authorizes Bank to release information to these individuals regarding the data files.

4. Cancellation Instructions. Bank has no obligation to comply with any request to cancel the processing of any IP data file, to amend any payment entries, to pull from disbursement a printed check, or cancel any ACH entry, commercial card payment, or U.S. Dollar wire transfer file created in accordance with Client's IP data file. As an accommodation to Client, however, Bank will use good faith efforts to comply with Client's request to cancel the processing of an IP data file or a payment entry, or pull a printed check from disbursement, if Client's request complies with any applicable cancellation requirements and Bank receives the request at a time and in a manner that gives Bank a reasonable opportunity to act on the request. Bank is not liable if Bank is unable to honor Client's request to cancel such processing of an IP data file or payment entry. Client agrees to reimburse Bank for any expenses Bank may incur in attempting to honor any such requests. Note that for commercial card payables files, any changes to a file (including cancellation) that has been submitted through IP must be made by logging in to the card program management solution.

5. Security Procedures. Client agrees that use of the IP service constitutes acceptance of the below security procedures.

   a. Data File Transmission and Access Credentials. Client must comply with applicable security procedures and requirements for the transmission method used to transmit an IP data file to Bank. For transmission methods that require access credentials, valid access credentials are required for log in to the transmission method application and/or to transmit a file. Valid access credentials are also required to log in to the designated website for file validation and control total submission, if applicable.

   b. Control Totals and Payment Approvals. If Client uses the STP file delivery option, an entitled user must submit the control total file along with the IP data file via File Transfer, and if the file totals match, the file will be released for processing.

      If Client transmits the IP data file to Bank through a designated website, an entitled user(s) must validate and approve payments within the designated IP website, or an entitled user must submit a matching control total (consisting of the aggregate dollar amount of all payment entries in the file), before the IP data file is processed by Bank.

      Bank strongly recommends that Client segregate duties within the IP service such that a single user is not entitled to perform all functions required to release payments for processing.

   c. Payee Access. Payee registration and valid access credentials are required for access to Bank's online remittance reporting feature or vendor enrollment feature. Client is responsible for providing registration instructions and initial access credentials to payees.

6. Creation of Issue File for Positive Pay, Account Reconciliation Plan, or Controlled Payment Reconciliation Services. Client may elect for the printed check information included in Client's IP data file to be used by Bank to create a Positive Pay, Account Reconciliation Plan, or Controlled Payment Reconciliation service issue file on Client's behalf to be used in connection with one of those services used by Client. By making this election, Client authorizes Bank to create an issue file on Client's behalf on each day on which checks are printed against any Truist account that is included in Client's setup for Positive Pay,

Account Reconciliation Plan, or Controlled Payment Reconciliation service. Client's use of the Positive Pay, Account Reconciliation Plan, or Controlled Payment Reconciliation service is governed by the terms and conditions for each service.

7. Payee Access. Payees have access to several optional features of IP service through a designated website.

   a. Online Remittance Reporting Feature. Before a payee can access Bank's online remittance reporting feature, that payee must register in the designated website and agree to terms and conditions for use of the website. Through the website, registered payees may utilize the online remittance reporting feature to view and download documents and information in connection with payments, including remittance data and statements.

   b. Vendor Enrollment. Under the vendor enrollment feature, Bank collaborates with Client on outreach to Client's vendors to obtain vendors' election to receive electronic payments (ACH or commercial card) instead of checks. This election of the vendor (payee) is for Client's information and Bank has no duty to comply with Client's payee's election to receive payments by ACH or commercial card, but Client may choose to change the payment type for the payee by specifying the applicable payment type in Client's IP data file.

   c. IP Vendor Services. Client or Client's payees may elect to obtain additional services directly from Bank's IP vendor, including, but not limited to, data download capabilities. Bank does not provide these additional services, and such services are governed solely by the agreement between the vendor and Client. The third party vendor is not acting on behalf of Bank in providing such additional services to Client. Bank has no obligations or liabilities with respect to such additional services and is not responsible for any obligations or liabilities that may arise in the course of the vendor providing such additional services directly to Client or Client's payees.

8. Document Printing. The document printing services provided hereunder will be limited to the printing of invoices and other documents approved by Bank (collectively, "Documents"). Client will submit separate data files for processing the Documents as agreed upon during implementation of the Document printing services.

9. IP Reconciliation File Service Option. Client can select this option to receive a single monthly or daily file of the IP check, ACH and commercial card (but not wire) payments that have been settled against Client's account(s).

Integrated Receivables Service

1. Description of Integrated Receivables Service. The Integrated Receivables ("IR") service is an online browser, information reporting and archive service that allows Client to receive a custom extract file of Client's receipt information in a consolidated format. Details regarding IR functionality and formatting and other technical requirements that Client must follow when using the IR service are provided in the IR reference materials. The IR service allows for the extraction and reporting of receipt information from certain of Bank's source payment channels and treasury management services as designated by Client during implementation of the service. Client acknowledges and agrees that the data provided within the IR service consists of information initially received through the applicable source payment channel or treasury management service, and such data may not reflect the final information that is posted to such source payment channel or treasury management service (for example, if a transaction initially received from a channel or service is later adjusted or rejected). Therefore, data within the IR service may not reflect final posted transaction information from the applicable source payment channel or treasury management service, and Client must refer to the source payment channel or treasury management service for any final and correct transaction information.

2. Access and Administration. Client will access the IR service through one of Bank's online services. Client must designate a Primary Administrator for the IR service on a Primary Administrator Designation agreement or other similar document accepted by Bank.

3. IR Functionality. The IR service offers the following functionality:

   a. Images and/or Data Archive. Entitled users have access to receivables images and/or data based on the archive storage option Client selects from options provided by Bank. Image and/or data archive information is delivered to the IR solution throughout the day once transactions are completed in the source channel (i.e., ACH, Wire, Lockbox). Bank will have no obligation to retain images or data beyond the retention period selected by Client.

   b. Dashboard. The dashboard page of the service functions as an information repository and permits entitled users to view images and/or data of payments by workgroup ID or payment source, and view batch and demand deposit account summary and detail. A workgroup ID is a number assigned to facilitate a logical grouping of Client's receipt transactions as defined by routing and demand deposit account by channel(s) as designated by Client during implementation of the

service. The dashboard includes a graphical representation of transactional detail which shows daily total processing volume by channel.

c. Archive Search. The IR service is configurable and can receive processed items from certain other Truist treasury management receivables services used by Client. Items are automatically archived and made available for searching, viewing, reporting and printing or download. Archived images and/or data are available based on the archive retention period Client selects from options provided by Bank. Images and/or data will be purged following the end of the specified retention period at the end of each business day.

4. Reporting. The IR service provides entitled users with access to pre-formatted reports available for online view, download or print. Images and/or data available for reporting are based on the archive retention period selected by Client. The following reports are available:

   a. Extract Audit Report. This report includes all data extracts created manually by a user or data extracts created by the file extract scheduler. The file extract scheduler automatically generates file extracts based on a schedule specified by Client.

   b. User Access Reports. These reports include administration group and user reports, which show user activity, user access and user role assignments.

5. Extract File. The IR service allows Client to manually extract file output from the search feature or receive a system generated consolidated extract file in a format customized to Client's specifications. Extract file(s) consist of consolidated receipt information, which includes applicable images and/or data. System generated file(s) are available based on the schedule and frequency as defined during implementation. System generated extract file delivery options include direct transmission or downloading within the IR service.

6. Termination. Once the IR service is terminated, Client will no longer be able to access IR through the online service. Once the service is terminated, Client acknowledges that there will be no access or availability of stored images and/or data within IR. Therefore, it is advised that prior to termination of IR, users should download or otherwise confirm accessibility to previously generated consolidated extract files for any future reference or historical research needs.

7. Data Handling. The IR service will attempt to read and store payment and related document images and/or data it receives from the source system(s). Should the information received be unreadable because it is either in a format that cannot be interpreted or data is not formatted to the applicable industry file standards, these data points may be unsearchable and unavailable for inclusion in Client's consolidated extract file.

8. Credit Card Exclusions. For Clients that process credit card transactions within a Lockbox service, Electronic Bill Presentment and Payment service, or Online Bill Presentment and Payment service, Bank will make a reasonable attempt to identify these items and exclude them from loading into the IR service. Transaction information for these items will be made available within the source system. Bank will also use reasonable efforts to mask card information that may be included in an electronic bill payment received and reported via the IR service. However, Client acknowledges and agrees that certain card information may be reported through the IR service, and that such card information may not be masked or redacted. Client agrees that it is solely responsible for any obligations relating to exposure or access of such card information through Client's use of the IR service, and that Bank shall not be liable for any losses relating to such exposure or access.

Integrated Receivables Service

[Applicable from 9/30/25 for implementations occurring after this date]

1. Service Version. The following terms apply to the version of the Integrated Receivables ("IR") service first offered on or after September 30, 2025. If you are unsure as to which version of the Integrated Receivables service you use, contact Bank.

2. Description of Integrated Receivables Service. The IR service is an online browser, information reporting, matching, and archive service that allows Client to receive a custom output file of Client's matched receipt information in a consolidated format. Details regarding IR functionality and formatting and other technical requirements that Client must follow when using the IR service are provided in the IR reference materials. The IR service allows for the extraction and reporting of receipt information from certain of Bank's source payment channels and treasury management services as designated by Client during implementation of the service. Client acknowledges and agrees that the data provided within the IR service

consists of information initially received through the applicable source payment channel or treasury management service, and such data may not reflect the final information that is posted to such source payment channel or treasury management service (for example, if a transaction initially received from a channel or service is later adjusted or rejected) and may exclude some batch or document types (i.e., credit card, correspondence only). Therefore, data within the IR service may not reflect final posted transaction information from the applicable source payment channel or treasury management service, and Client must refer to the source payment channel or treasury management service for any final and correct transaction information.

3. Access and Administration. Client will access the IR service through Truist One View. As a standard, the IR Primary Administrator will be defined as the same Primary Administrator that is designated for Truist One View. Client must designate a Primary Administrator on a Primary Administrator Designation agreement or other similar document accepted by Bank.

4. IR Functionality. The IR service offers the following functionality:

    a. Images and/or Data Archive. Entitled users have access to receivables images and/or data based on the archive storage provided through the online application. Image and/or data archive information is delivered to the IR solution throughout the day once transactions are completed in the source channel (i.e., ACH, Wire, Lockbox). Bank will have no obligation to retain images or data beyond the retention period defined for the service.

    b. Dashboard. The dashboard page of the service functions as an information repository and permits entitled users to access menu items for view of images and/or data of payments by payment source, view batch, and transaction summary and details. The dashboard also provides notifications of information that could be relevant to you for communication of maintenance, system availability, or other event.

    c. Research. The IR service is configurable and can receive processed items from certain other Truist treasury management receivables services used by Client. Items are automatically archived and made available for searching, viewing, reporting, and printing or download. Stored images and/or data are available based on a defined system retention. Images and/or data will be purged following the end of the specified retention period at the end of each business day.

    d. Open Invoice (Accounts Receivable) Data. A daily input file containing open AR data is required as input to facilitate payment to invoice match. File should be free from defects and securely transmitted to meet import requirements.

    e. Payment to Invoice Match. IR leverages complex algorithms to match incoming payments to open invoices/accounts. Match validations are defined for all payment channels based on system configuration at service set-up. Match processing requires daily input of open invoice data from a designated accounting platform and optional email input to provide remittance detail for posting and straight-through processing. Client must ensure that its entitled users review system generated auto matches each processing day. Client acknowledges that failure to conduct such reviews constitutes its acceptance of the risk of errors. Available match configuration settings include the following:

        i. System auto-mapping. Enables automatic matching of incoming funds (ACH or Wire payments) that are sent via email or included on a securely delivered transmission file. Options available under this configuration will allow manual, intuitive, historical, or reference ID matches based on existing database records. These options are defined during set-up and may affect match optimization, which should be examined on a routine basis to ensure configuration meets business requirements.

        ii. Match Strategies. System configuration which allows the additional designation of business rules that are applied to each payment during validation.

        iii. Match Rules. Configuration options that work with Match Strategies to determine and prioritize which business rules will match and auto-validate for each payment. Multiple versions of the same rule can be configured to allow for different configuration settings by Payment Channel.

        iv. Match Constraints. Can be used to prevent a payment from auto-validating.

        v. Payment Pause Rules. Allow imported payments to be ‘paused’, making them temporarily unavailable for review, validation or posting until the pause rule has expired.

5. Reporting. The IR service provides entitled users with access to pre-formatted reports available for online view or email delivery. The following report types are available:

    a. Scheduled Reports. This report type can be scheduled to auto-generate at a defined time and can be configured for email and viewed online.

    b. Post Reports. These reports include standard reports to be created for each post job. Each configured report will

be available in a separate reports tab for each post job when the output file is created.

6. Post File. The IR service generates a post file output in industry standard formats or alternatively generated in a format customized to Client's specifications. Post file(s) consist of consolidated payment data matched manually or auto matched by the system. System generated file(s) are available based on the schedule and frequency as defined during implementation. All system generated post files are delivered via secure file transmission (push or pull).

7. Archive File. The IR service can be optionally configured to generate an archive file output to include matched payment images. Information will be delivered in industry standard image formats. System generated file(s) are available based on the schedule and frequency as defined during implementation. All system generated archive files are delivered via secure file transmission (push or pull).

8. Data Handling. The IR service will attempt to read and store payment and related document images and/or data it receives from the source system(s). Should the information received be unreadable because it is either in a format that cannot be interpreted or data is not formatted to the applicable industry file standards, these data points may be unsearchable and unavailable for inclusion in Client's configured archive and/or post file(s).

9. Credit Card Exclusions. For Clients that process credit card transactions within a Lockbox service or Electronic Bill Presentment and Payment service, Bank will make a reasonable attempt to identify these items and exclude them from loading into the IR service. Transaction information for these items will be made available within the originating source system. Client acknowledges and agrees that certain card information may be inadvertently or incidentally reported through the IR service, and that such card information may not be masked or redacted. Client agrees that it is solely responsible for any obligations relating to exposure or access of such card information through Client's use of the IR service, and that Bank will not be liable for any losses relating to such exposure or access.

10. Private Health Information (PHI) Exclusion. Certain terms used in this paragraph are defined in the Business Associate Agreement terms incorporated above in this Agreement. Bank states that the IR service is not designed to process PHI in compliance with HIPAA and Bank assumes no obligations of a Business Associate in connection with the IR service. If Client is a Covered Entity, Client acknowledges the foregoing statement and agrees that (i) it will ensure that transactions and documentation containing PHI will not be reported through the IR service from source payment channels; and (ii) source payment channels that may generate transactions and documentation containing PHI will be identified upon initial set-up. Any transmission of PHI by Client, whether inadvertent, incidental, or otherwise, must be communicated to Bank immediately upon discovery. Bank accepts no liability arising from its receipt of PHI in connection with the IR service.

11. Termination. Once the IR service is terminated, Client will no longer be able to access IR through the online service. Once the service is terminated, Client acknowledges that there will be no access or availability of stored images and/or data within IR. Therefore, it is advised that prior to termination of IR, users should download or otherwise confirm accessibility to previously generated archive and/or post files for any future reference or historical research needs.

Medical Lockbox Service

1. Description of Medical Lockbox Service. The Medical Lockbox service facilitates healthcare revenue cycle management by presenting information that allows Client to manage healthcare transaction data. These terms and conditions apply to services known as or previously known as Medical Data Lockbox and eClaim Revenue Gateway, and the term "Medical Lockbox service" within these terms and conditions generally includes both Medical Data Lockbox and eClaim Revenue Gateway. The Medical Lockbox service allows Client to reconcile healthcare claims data with paper and electronic remittance advices and other payment data received from third- party payers and patients. Claims, remittance advices, payment data, and correspondence are all processed through the service. The HIPAA compliant portal is available as part of the service for searching, viewing, archiving, and reporting. Further details regarding functionality of the Medical Lockbox service and information regarding certain formatting, security, and other technical requirements are provided in the Medical Lockbox reference materials. The Medical Lockbox service may not be used outside of the United States, U.S. territories, U.S. military bases or U.S. Embassies and files may not be transmitted to/from outside the United States unless transmitted from a U.S. territory, military base or embassy.

2. Lockbox Payment Data Processing. Utilization of Bank's Medical Lockbox service requires that Client also subscribe to a lockbox service provided by Bank. Bank will process each paper Explanation of Benefit (EOB), invoice remittance document or "coupon", check, draft, money order and other miscellaneous correspondence that is received in Client's lockbox according to Client's lockbox instructions. The lockbox payment data will be sent each banking day by image transmission to

the Medical Lockbox repository to optically lift the detailed data from all remittance advices for matching to the open claims file received from Client in order to convert the paper payment and remittance detail into an electronic posting file.

3. Paper Conversion, Claims Matching and Posting. To allow for electronic conversion and matching on previously submitted claims to the payment data received in or submitted through the Medical Lockbox service, Client must submit a file containing electronic copies of Client's healthcare claims data (relating to claims generated through Client's practice management system or hospital information system which Client has separately submitted to payers for payment) to the Medical Lockbox service. Client must submit Client's electronic claims and or other file(s) to Bank in ANSI 837 format or other format that Bank approves. The claims and data will then be processed through the Medical Lockbox service, converting paper payment and remittance detail to an ANSI 835 format, ready for posting into Client's practice management system.

4. Electronic Payment Data Processing. In addition to converting paper payments and remittance detail into post- ready electronic files, the Medical Lockbox service has the ability to receive and process existing 835 files along with ACH payment detail for re-association.

5. Correspondence. Medical Lockbox can also receive and lift certain critical data elements from Client's correspondence (denial letters, need for more information, etc.) These images and data can be searched and viewed within the Medical Lockbox portal.

6. Medical Data Lite. In addition to the full solution, which includes processing of ANSI 837 files and producing ANSI 835 files, Bank also offers a "Medical Data Lite" solution for clients that require certain data elements lifted from Client's paper lockbox remittance detail but do not have the ability to produce and retrieve said files. Medical Data Lite is not available for all Clients.

7. Reporting Options. The Medical Lockbox service offers various reporting and analytic options through the Medical Lockbox portal, as described in the Medical Lockbox reference materials.

8. Transmission, Primary Administrator, and Authorization Codes.

    a. Transmission. To send or receive certain electronic healthcare images and/or data to or from the Medical Lockbox service through Client's practice management system or hospital information system, Client must (i) establish a secure, direct file transmission with Bank, and/or (ii) send or receive images and/or data through the Medical Lockbox portal.

    b. Primary Administrator. Client must designate an individual as Client's Medical Lockbox Primary Administrator. This Primary Administrator can then create additional users and users with administrative entitlements (administrators).

    c. Authorization Codes. To log onto the Medical Lockbox portal, each of Client's users is required to enter that user's authorization codes. The user's initial authorization codes to access the Medical Lockbox portal will be supplied as described in the Medical Lockbox reference materials.

9. Use of Third-Party Suppliers and Clearinghouse Status. As part of the service, Bank's vendor or agent for the service or its agent may (a) process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction or (b) receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity. These actions may result in Bank's vendor or agent being classified as a healthcare clearinghouse for purposes of 45 C.F.R. § 160.103. However, Client acknowledges and agrees that neither such actions of Bank's vendor or agent nor any provision of these Medical Lockbox terms and conditions shall cause Bank to be considered as a healthcare clearinghouse within the meaning of 45 C.F.R. § 160.103.

10. Additional Terms. In addition to any other disclaimers or limits on Bank's liability in this Agreement, Client acknowledges and agrees that Bank has no responsibility for (a) Client's use of payment data or other information Client chooses to upload and/or access through the Medical Lockbox service to perform any management, tracking and/or reconcilement of claims functions, (b) the accuracy, integrity, legality, reliability, or appropriateness of any data submitted to Bank by Client, a third-party payer, or a third-party lockbox provider that is uploaded to the Medical Lockbox service, or (c) the failure of any third-party lockbox provider to send Client's lockbox image file to the Medical Lockbox service according to the instructions and by the deadlines set forth in the reference materials. Client also agrees that Client must comply with all requirements of the Health Insurance Portability and Accountability Act as amended from time to time and all related rules and regulations applicable to Client while using the Medical Lockbox service.

11. Authority for Other Entities. If Client requests that accounts or information of other entities be included in Client's setup of Medical Lockbox service, then Client represents and warrants to Bank that the other entity has given Client authority to add that entity's account or information to Client's setup of the Medical Lockbox service, including without limitation authority to submit or receive healthcare data and claims information of that entity to or from the Medical Lockbox service and to

access any information and accounts of that entity through use of the Medical Lockbox service to the same extent as if Client owned that information and/or accounts.

12. Termination. Upon termination of the Medical Lockbox service, Bank can provide information on options to access historical images and data from the service to Client upon request. Additional fees may apply.

Multi-Bank Reporting Service

1. Description of Multi-Bank Reporting Service. The Multi-Bank Reporting service provides Client with a consolidated view of Client's account balance and transaction data from multiple bank.

    a. Inbound Multi-Bank Reporting. Bank receives Client's account information (balances and transactions) from one or more other financial institutions or third party vendors and loads the data into Truist Commercial Online, Truist Treasury Manager or Online Courier service.

    b. Outbound Multi-Bank Reporting. Bank sends Client's Truist account information (balances and transactions) to one or more other financial institutions or third party vendors. By electing Outbound Multi-Bank Reporting, Client consents to such transmission of Client's Truist account information to the designated third parties.

    Client many select to use Inbound Multi-Bank Reporting, Outbound Multi-Bank Reporting, or both.

2. Liability. Bank makes no representations with respect to and assumes no liability for the ability or willingness of other financial institutions or third parties to participate in the service, or for the correctness, accuracy, completeness, integrity or timeliness of any information or data whether (a) received by Bank from Client, a third party financial institution, vendor, or other source of data or (b) transmitted, reported, communicated, or broadcast by any such party.

Online Bill Consolidator Service

1. Description of Online Bill Consolidator Service. The Online Bill Consolidator ("OBC") service enables Client to receive remittance information regarding payments sent to Client through the online bill payment service of any third-party online payment processor (each, an "online payment processor") who participates in the OBC service. Client may use the OBC service with respect to the accounts and the online payment processors identified in Bank's records that are included in Bank's implementation of the OBC service. Details regarding the functionality of the service and requirements that Client must follow when using it are provided in the OBC reference materials.

2. Enrolling as a Biller.

    a. Client authorizes Bank to establish a "biller profile" using information Client provides Bank during implementation of this service. Client must ensure that all information Client gives Bank or that Client provides directly to a processor to enroll in the service is complete and accurate.

    b. Client represents and warrants to Bank that Client does not owe any outstanding amounts to an online payment processor and that Client is not currently using (and, as long as Bank is providing the OBC service to Client, will not use) the services of any other financial institution to enroll in or otherwise obtain access to the online bill payment service of an online payment processor.

    c. Client agrees to complete, sign and give Bank or the applicable online payment processor all forms that are necessary to receive payments and remittance information for payments processed through an online payment processor's online bill payment service, including an ACH debit authorization form.

3. Remittance Files; Settlement; Reconcilement; Posting.

    a. Once Client has been enrolled as a biller in an online payment processor's online bill payment service, that online payment processor will send Bank remittance information regarding payments sent to Client through that online payment processor's online bill payment service. After Bank receives that remittance information from an online payment processor, Bank will reformat it in accordance with the file formatting requirements Bank has agreed to with Client and create a file of such reformatted remittance information (each, a "remittance file"). Unless an earlier deadline for an online payment processor's online bill payment service is provided in the OBC reference materials or any guides, rules or other documentation (collectively, the "online payment processor's documentation") that governs participation in such online payment processor's online bill payment service, Bank will send each remittance file to Client no later than the

first banking day after the day Bank receives the relevant remittance information from an online payment processor. Client may designate whether Bank sends remittance files to Client as a separate transmission or appended to another product's file.

b. Each online payment processor will be responsible for settling all payments sent to Client in each remittance file. The applicable online payment processor will do so by sending one or more ACH credit entries to the account Bank includes in Bank's implementation of OBC that has been identified as the settlement account for that online payment processor. All payments credited to a settlement account, or otherwise owed to Client, for payments sent to Client through an online payment processor's online bill payment service are subject to any rights that online payment processor may have to unwind transactions and exercise setoff under that online payment processor's documentation.

c. Client is responsible for reconciling the remittance information in each remittance file to the ACH credits Client receives from each online payment processor. If Client is unable to reconcile the two, Client must notify Bank of the inconsistencies by the end of the banking day on the day Client receives the ACH credit. If Client has notified Bank in the time required, Bank will use good faith efforts to attempt to resolve any such inconsistencies with the applicable online payment processor.

d. Client is responsible for posting each payment reflected in a remittance file to the correct customer account in Client's receivables system. Unless an earlier time for posting for an online payment processor's online bill payment service is provided in the OBC reference materials or that online payment processor's documentation, Client must electronically post each payment reflected in a remittance file to Client's receivables system so that such payment is posted to the correct customer account before Client's posting cut-off time on the calendar day immediately following the date Bank received the applicable remittance information from an online payment processor, as reflected by the date in the file header information (the "file header date"). If the immediately following calendar day is a holiday or weekend day, Client must post the payment on the next business day, and Client must also backdate the time the payment is shown to have been posted in Client's receivables system so that it reflects it was posted before Client's payment posting cut-off time on the calendar day immediately following the file header date.

4. Returns; Refusals; Reversals.

a. If Client is unable to determine from a remittance file the correct customer account to which a payment should be posted, then (unless a shorter period for an online payment processor's online bill payment service is provided in the OBC reference materials or that online payment processor's documentation) Client must complete Client's research of the payment and post it to the correct customer account within two banking days from the file header date of that remittance file. Client may not post the payment to a general ledger suspense account or otherwise hold the payment beyond that period while Client continues to research the payment. If Client has been unable to determine the correct customer account and post the payment within that period, then (unless a shorter period for an online payment processor's online bill payment service is provided in the OBC reference materials or that online payment processor's documentation) Client must request that Bank returns the payment and Bank must receive that request no later than 5:00 p.m. ET (the "returns deadline") on the second banking day after the file header date of that remittance file and, if required by the applicable online payment processor, Client must notify the applicable online payment processor directly by the time specified in such online payment processor's documentation. If a remittance file contains incorrect information, but Client is able to post the payment, then (unless a shorter period for an online payment processor's online bill payment service is provided in the OBC reference materials or that online payment processor's documentation) Client must give Bank a notice that describes what was incorrect in the remittance information no later than the returns deadline on the day that is two banking days after the file header date of that remittance file and, if required by the applicable online payment processor, Client must notify the applicable online payment processor directly by the time specified in such online payment processor's documentation.

b. Client may not refuse to accept a payment that one of Client's customers sends Client through an online payment processor's online bill payment service unless (i) the customer account data for that payment is incorrect or incomplete or (ii) Client has elected not to accept any payments from that customer. If Client is not willing to accept any payments from a customer, then (unless a shorter period for an online payment processor's online bill payment service is provided in the OBC reference materials or that online payment processor's documentation) Client must request that Bank returns the payment no later than the returns deadline on the day that is two banking days after the file header date of the remittance file containing that payment information.

c. Some online payment processors offer "guaranteed payments". If an online payment processor does not offer guaranteed payments, originators can initiate reversals of payments previously made to Client through that online payment processor's online bill payment service. The online payment processor will then send an ACH debit entry to Client's settlement account for such reversals. Bank will not have any responsibility for any reversals processed through

an online payment processor's online bill payment service or debits by an online payment processor to one of Client's accounts to reverse a payment.

5. Limitation of Liability; Disclaimer; Indemnity. In addition to any other limits on Bank's liability under this Agreement and to the extent permitted by applicable law, Client agrees that Bank will not have any liability for any acts or omissions of an online payment processor (including, without limitation, (a) any error or delay in processing any payments or remittance information, including any error or delay in initiating any funds transfers to Client, (b) any breach of confidentiality of any information, including any of Client's or Client's customers' payment, account or personal information, (c) the inaccuracy of any remittance information, or (d) any reversals or other debits initiated against Client's account). In addition to any other indemnity obligation Client has under this Agreement and to the extent permitted by applicable law, Client agrees to indemnify and hold Bank harmless from and against any claims, liabilities, losses, damages, costs and expenses (including, without limitations, attorneys' fees) arising from or related to (i) any amounts or other obligations Bank owes an online payment processor that are related in any way to Client's use of that online payment processor's online bill payment service, (ii) faulty or erroneous information or instructions Client gives Bank or an online payment processor, (iii) any of Client's errors or delays in posting a payment to Client's accounts receivable system, (iv) any breach of any of Client's other obligations under these OBC terms and conditions, or (v) any of Client's acts or omissions which result in a breach by Client or Bank of the terms of any online payment processor's documentation.

6. Online Payment Processor Documentation. Client's use of the OBC service is subject to the terms of each online payment processor's documentation. Client agrees to take all actions Bank or such processor deem necessary for both Client and Bank to be in compliance with each online payment processor's documentation. Client agrees that Bank is not obligated to take any action under these OBC terms and conditions that would cause Bank to breach the provisions of any online payment processor's documentation. Client agrees that none of Bank's obligations under any online payment processor's documentation create obligations for Bank under these OBC terms and conditions unless expressly set forth as Bank's obligations in these OBC terms and conditions.

Online Bill Presentment and Payment Service

1. Description of Online Bill Presentment and Payment Service. The Online Bill Presentment and Payment ("OBPP") service enables Client to electronically collect bill payments from Client's customers (each, a "payer") by initiating ACH debit entries against a payer's deposit account or by initiating charges against a payer's credit or debit card. These ACH debit entries and credit or debit card charges (which are generically referred to in these OBPP terms and conditions as "payments") are initiated in response to payment authorizations payers submit through the internet or give Client's authorized users over the telephone. Details regarding OBPP's functionality and requirements that Client must follow when using the OBPP service are provided in the OBPP reference materials.

2. Functioning of the OBPP Service. Each payment authorization that Client or a payer submits through the OBPP service will initiate a payment in accordance with these OBPP terms and conditions. Client will be the "originator" and Bank will act as the originating depository financial institution or "ODFI" for each ACH debit entry initiated. Similarly, Client will be the "merchant" for each credit or debit card charge initiated through the OBPP service. However, Bank does not act as the merchant bank processor or "acquirer" with respect to those credit or debit card charges. Instead, the OBPP service merely routes information for those credit or debit card charges to Client's third-party merchant bank processor, which will act as the acquirer for those credit or debit card charges. In order to initiate credit or debit card charges through the OBPP service Client must have entered into a merchant services agreement with a third-party merchant bank processor acceptable to Bank.

3. Origination and Processing of Payments.

   a. Payment authorizations may be submitted through the OBPP service by (i) a payer through an internet website (the "biller website") or (ii) an authorized user of Client through the biller website based on a verbal authorization a payer gives such user over the telephone. The biller website is provided by Bank as part of the OBPP service and is the website through which payments are made. Client must provide and maintain a secure link to the biller website on Client's general website and is responsible for ensuring that this link takes a payer to the appropriate area within the biller website. Client is also responsible for providing data concerning each payer who uses this link. The link and the linking process, including the manner in which Client submits data about each payer to Bank, must also meet Bank's encryption and security requirements.

   b. Before a payer may submit a payment authorization through the OBPP service, that payer must be registered in the OBPP system. A payer may self-register directly through the biller website or may be registered as a payer through the biller website by an authorized user based on information the payer gives the user over the telephone. In addition, if the

Single Sign-On option (defined below) is used, a payer who has registered on Client's general website will be automatically registered in the OBPP system. The registration process must include a commercially reasonable fraudulent transaction detection system, a commercially reasonable methodology to establish a secure internet session, and commercially reasonable procedures to verify the identity of the payer. At Client's option (as designated by Client during implementation of the service), payers may be allowed to give payment authorizations immediately following the registration process or may be prohibited from giving payment authorizations until Client has authorized them to do so.

c. The biller website will be formatted in accordance with the specifications Client provides to Bank. Client grants Bank the right and a license to use (i) Client's name, trademarks, service marks, copyrights and logos and other textual information in connection with the biller website and (ii) Client's data in connection with the OBPP service, in each case as contemplated by these OBPP terms and conditions. Once a payer has accessed the biller website, that payer may authorize Client to initiate a payment against the payer's deposit account or credit or debit card on the day that the authorization is submitted, each a "current payment," or to initiate one or more payments on scheduled future dates, each a "scheduled payment." Before a payer may submit a payment authorization through the biller website, that payer must accept terms regarding use of the biller website that, among other things, authorize Client as "biller" to initiate one or more payments against that payer's deposit account or credit or debit card, as applicable, and permit Client and Bank to use the data provided by the payer to process those payments, including consent for that data to be sent outside of the United States. Given the types of potential payments, such terms of use must also comply with (i) the Nacha Operating Rules and Guidelines ("ACH Rules") as they are in effect at the relevant time and (ii) the operating regulations and other requirements of the entity or association that issues or sponsors the applicable credit or debit card as they are in effect at the relevant time, or the "card rules". Bank may provide Client sample terms of use to assist Client in drafting terms regarding use of the biller website but, subject to the foregoing requirements, the final content of such terms is Client's responsibility. Through the biller website, a payer may view scheduled payments set up in, and prior payments made through, the OBPP system and may, prior to the deadline for submitting payment authorizations set forth in the OBPP reference materials, also delete or modify scheduled payments set up in the OBPP system.

d. An authorized user of Client may also use the biller website to initiate payments against a payer's deposit account or credit or debit card based on a verbal authorization that payer gives an authorized user over the telephone, but only if (1) the payer initiated the telephone call or (2) Client has an existing business relationship with the payer as more fully described in the OBPP reference materials. Client is solely responsible for establishing the validation procedures an authorized user must follow to verify the identity of a payer and the authenticity of verbal payment or other authorizations a payer gives an authorized user over the telephone before those payment or other authorizations are submitted through the biller website. An authorized user must provide the information specified in the OBPP reference materials to the payer and obtain the payer's unambiguous verbal authorization prior to initiating a payment through the biller website. After an authorized user has initiated a payment through the biller website, the OBPP system sends the payer an email confirming that verbal authorization. Such email will be sent to the email address established at the payer's registration and reflected in the OBPP system as part of the payer's profile. This confirmation notice must comply with the ACH rules or the card rules, as applicable.

e. Each ACH debit entry initiated through the OBPP service must be originated using the applicable SEC (or Standard Entry Class) code, as described in the OBPP reference materials. The OBPP system will assign an SEC code based on information provided by the payer or an authorized user of Client when initiating the payment. ACH debits and credit or debit card charges processed through the OBPP service will be processed and debited/charged to the payer's account according to the timelines set forth in the OBPP reference materials.

f. The OBPP service will use commercially reasonable procedures to verify that the routing number associated with any ACH debit entry initiated using the OBPP service is valid.

4. Administrative Functions. Client may use the biller website to perform certain administrative functions in connection with Client's use of the OBPP service. These functions may include registering a payer, administering and approving a payer's registration, viewing the status of payments, deleting payments, modifying scheduled payments, receiving certain notices, generating and viewing certain transaction reports, establishing authorized users and the limits on each authorized user's authority, and downloading and uploading certain files of data. Any modification or deletion of a payment must be completed prior to the deadline for submitting payment authorizations set forth in the OBPP reference materials. Reports are available to be viewed through the biller website for the number of days set forth in the OBPP reference materials. All files uploaded or downloaded through the biller website will be transmitted to Bank or to Client as specified during implementation of the OBPP service.

5. Representations and Warranties. Client agrees that (a) for each ACH debit entry Client initiates through the OBPP service, Client must comply with all obligations of an originator of , and Client makes all representations, warranties and agreements set

forth in the ACH rules and the terms and conditions for the ACH Origination service related to, any ACH entries and (b) for each credit or debit card charge Client initiates through the OBPP service, Client must comply with all obligations of a merchant with respect to, and Client makes all representations, warranties and agreements set forth in the card rules related to, the credit or debit card charge. Client further represents that any payment or other authorization Client or a payer submits through the OBPP system has been authorized by the relevant payer. Client also represents and warrants to Bank that Bank's use of Client's (i) name, trademarks, service marks, copyrights and logos and other textual information in connection with the biller website and (ii) data in connection with the OBPP service, as contemplated by these OBPP terms and conditions, does not infringe or otherwise violate any intellectual property or other proprietary rights of any third party.

6. Designation of Primary Administrators. Client must designate a Primary Administrator for the OBPP service. The Primary Administrator will be set up with full user permissions with respect to the biller website, including the right to administer the rights and permissions of all other users, and to create additional administrators.

7. Security Procedures. The security procedures for the OBPP service are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.

   a. Client's use of the biller website. Valid access credentials are required to log on to the biller website.

   b. Payers' use of the biller website. Except as otherwise described below for the Single Sign-On option, to access and use the biller website, a payer must log on to the biller website using that payer's valid access credentials. If a payer self-registers in the OBPP system through the biller website, the payer will select the payer's own user ID and password. If an authorized user registers a payer through the biller website, Client will designate the payer's user ID and a temporary password.

   c. Control totals. Immediately prior to transmitting the Nacha formatted file to Bank, the OBPP system will communicate the total dollar amount of the file (referred to as the "control total") to Bank through the biller website. Bank does not require that Client separately submit control totals in order to process files of ACH debit entries initiated through the OBPP service.

8. ACH Origination Service. The ACH Origination service terms and conditions are incorporated by reference herein, and all applicable provisions of such terms and conditions apply to ACH entries originated through the OBPP service. Terms that are defined in the ACH Origination terms and conditions have the same meanings when used in these OBPP terms and conditions. If there is any inconsistency on a particular issue between these OBPP terms and conditions and the ACH Origination terms and conditions, these OBPP terms and conditions will control.

9. Single Sign-On Option. Single Sign-On is an optional feature of the OBPP service that allows payers to access the biller site through Client's general website's authentication process without entering an additional user ID and password. Client's election to use the Single Sign-On feature will be designated during implementation. In order to use Single Sign-On, the authentication procedures and methodology used to establish a secure internet session employed by Client's general website must be commercially reasonable and must meet certain requirements set forth in the OBPP reference materials. Client must maintain records of the authentication of each payer who logs in to Client's general website and accesses OBPP through Single Sign-On for a minimum of five (5) years from the date of login. Such records must evidence the authentication and identification of the payer and must include, at a minimum, the payer's user name, system name, session ID, date/time stamp, and payer's IP address. Client must provide copies of such records to Bank, in a format that is satisfactory to Bank, within five (5) business days of Bank's request. Additionally, Client will be required to obtain, install and manage, at Client's own expense, a valid X.509 certificate issued by a Certificate Authority as further described in the OBPP reference materials. Client must comply with all requirements and complete all required testing and all implementation and software development tasks as further described in the OBPP reference materials. If Bank determines, in Bank's sole discretion, that Client does not meet any of the requirements or are not otherwise eligible for Single Sign-On, Client will not be permitted to use this feature of the OBPP service. Under the Single Sign-On option, payer registration and authentication, including selection and reset of user IDs and passwords, will be Client's responsibility and will take place within Client's general website. If Client uses Single Sign-On, Client is responsible for the actions of any person who accesses the biller site and/or the OBPP system through Client's general website, including any unauthorized payments initiated by such person. In addition to any other indemnity obligation Client has under this Agreement and to the extent permitted by applicable law, Client agrees to indemnify and hold Bank harmless from and against any claims, liabilities, losses, damages, costs and expenses (including, without limitation, attorneys' fees) arising from or related to any person's access to the biller site and/or the OBPP system through Client's general website, including but not limited to any losses resulting from the breach or failure of the security features of Client's general website or Client's failure to comply with any requirements for Single Sign-On contained in this Agreement, including requirements set forth in the OBPP reference materials.

TRUIST

Online Courier Service

1. Description of Online Courier Service. The Online Courier ("OLC") service is an online information reporting service that provides various statements, alerts, and reports to Client via selected delivery channels, as designated during implementation. OLC may also be used to upload Positive Pay service files. Details regarding OLC's functionality and formatting and other technical requirements that Client must follow when using the OLC service are provided in the OLC reference materials.
2. Designation of Primary Administrator. In order to use OLC, Client must designate an OLC Primary Administrator by executing a Primary Administrator Designation Agreement.
3. Security Procedures. OLC users must use authorization codes to access the service. Authorization codes will be provided by an administrator.

Payables and Invoice Management Service

1. Description of Payables and Invoice Management Service. The Payables and Invoice Management ("PIM") service synchronizes with Client's accounting software to automate invoice processing and payment execution. Payments can be made via checks, Automated Clearing House ("ACH") entries, or commercial card. Details regarding the functionality of the PIM service and certain formatting and other technical requirements that Client must follow when using the PIM service are provided in the PIM reference materials. Client must designate a Primary Administrator for PIM within a Primary Administrator Designation agreement (or other similar agreement accepted by Bank).
2. Invoice Processing. Invoices are uploaded to the PIM application via the following methods a) invoices keyed into Client's accounting software will be loaded to PIM; b) Client can key invoice data into PIM; c) invoices can be uploaded to PIM; or d) invoices can be emailed to a designated mailbox. If Client selects the automated invoice capture option, invoice header or invoice header and line level invoice detail is captured electronically using optical character recognition (OCR). Client is responsible for reviewing invoice data for accuracy and making any required updates. Invoice images and/or data are routed to Client's designated users for approval.
3. Payment Processing and Initiation. Once an invoice has been approved, Client will be prompted to authorize and approve payments for processing based on the invoice. One approved by Client, data for payment entries ("Payment Data file") is delivered to Bank via the PIM service for processing, and Bank then initiates payments via check, ACH entry, or commercial card payment, to designated payees in accordance with Client's instructions contained in the Payment Data file. Client must submit Payment Data files to Bank by the applicable cut-off deadline; otherwise, the Payment Data file may not be processed or there may be a delay in processing. Any payments made through PIM are subject to the applicable terms and condition of the payment type. Approved invoice and payment data is synched back to Client's accounting software.

   Client is responsible for payment entries included in the Payment Data file that are authorized and approved for processing according to the terms herein, even if a payment entry is a duplicate of another payment entry or otherwise is submitted in error. Bank is under no obligation to determine if a Payment Data file or any payment entry is a duplicate of a previously submitted Payment Data file or payment entry.
4. Processing of Payments.
   a. For each payment entry submitted for processing, Bank will, according to Client's instructions, print and disburse a check in U.S. dollars, create and transmit an ACH credit entry, or initiate a commercial card payment. Each payment entry will be drawn on or settle to the applicable designated account. Client's use of each payment type within the PIM service is subject to Bank's approval and completion of any additional documentation or agreements relating to the payment type that may be required by Bank.
   b. For each payment entry to be paid by check, the check will be printed in accordance with the format specifications established between Client and Bank. Bank will disburse checks by first-class U.S. mail, with associated costs passed through to Client. Bank shall have no responsibility for any checks once delivered to the United States Postal Service.
   c. For each payment entry to be paid via ACH credit entry, Client will be the originator of the ACH entry Bank creates from Client's Payment Data file. The ACH Origination service terms and conditions are incorporated by reference herein, and all applicable provisions of such terms and conditions apply to ACH entries originated through the PIM service. Terms that are defined in the ACH Origination terms and conditions have the same meanings when used in these PIM terms and conditions.

d. In order to include commercial card payables files in the Payment Data file, Bank must have agreed to provide Client a commercial card account and Bank's associated card program management solution. Client must execute a Commercial Card Agreement with Bank and any additional documentation Bank may require relating to the card program management solution (together, the "Commercial Card Agreements"). The Commercial Card Agreements are incorporated by reference herein, and all applicable provisions of the Commercial Card Agreements apply to commercial card payments transmitted through the PIM service.

e. Remittance data included with Client's Payment Data file may be printed with the corresponding checks, made available at Bank's designated website for a registered payee, emailed to a registered payee or sent by separate mailing for ACH entries to the payee at the address provided by Client.

5. Cancellation Instructions. Bank has no obligation to comply with any request to cancel the processing of any of Payment Data file or payment entry, to amend any Payment Data file, to pull from disbursement a printed check, or cancel any ACH or commercial card payment created in accordance with Client's Payment Data file. As an accommodation to Client, however, Bank will use good faith efforts to comply with Client's request to cancel the processing of a Payment Data file or payment entry, or pull a printed check from disbursement, if Client's request complies with any applicable cancellation requirements and Bank receives the request at a time and in a manner providing Bank with a reasonable opportunity to act on the request. Bank is not liable if Bank is unable to honor Client's request to cancel the processing of any Payment Data file or payment entry. Client agrees to reimburse Bank for any expenses Bank may incur in attempting to honor any such requests. Note that for commercial card payments, any changes to payments (including cancellation) that have been submitted through the PIM service must be made by logging on to the card program management solution.

6. Security Procedures. Client agrees that use of the PIM service constitutes acceptance of the below security procedures.

   a. Access Credentials. Valid access credentials are required to log in to the PIM service and to approve invoices or payment entries within the service.

   b. Dual Approval. Approval of any payment entry for processing within the PIM service requires dual approval, which means that one authorized user with sufficient entitlements must approve the invoice upon which the payment entry is based, and a different authorized user with sufficient entitlements must approve the payment entry, in order for the payment entry to be released and processed. At Client's option, Client may require additional approvals (three or more users) for such transactions; additional approval requirements will be selected by an administrator.

   c. Two-Factor Payment Verification. In order to approve a payment entry, an entitled user must enter a one- time security code in order for the payment entry to be released and processed.

   d. Payee Access. Payee registration and valid access credentials are required for access to Bank's online remittance reporting feature or vendor enrollment feature. Client is responsible for providing registration instructions and initial access credentials to payees.

7. Creation of Issue File for Positive Pay, Account Reconciliation Plan, or Controlled Payment Reconciliation Services. Client may elect for the printed check information included in Payment Data file to be used by Bank to create a Positive Pay, Account Reconciliation Plan, or Controlled Payment Reconciliation service issue file on Client's behalf, to be used in connection with one of those services used by Client. By making this election, Client authorizes Bank to create an issue file on Client's behalf on each day on which checks are printed against any Truist account that is included in Client's setup for Positive Pay, Account Reconciliation Plan or Controlled Payment Reconciliation service. Client's use of the Positive Pay, Account Reconciliation Plan or Controlled Payment Reconciliation service is governed by the terms and conditions for each service.

8. Payee Access. Payees have access to several optional features of the PIM service through a designated website.

   a. Online Remittance Reporting Feature. Before a payee can access Bank's online remittance reporting feature, that payee must register in the designated website and agree to terms and conditions for use of the website. Through the website, registered payees may utilize the online remittance reporting feature to view and download documents and information in connection with payments, including remittance data and statements.

   b. Vendor Enrollment. Under the vendor enrollment feature, Bank collaborates with Client on outreach to Client's vendors to obtain vendors' election to receive electronic payments (ACH or commercial card) instead of checks. This election of the vendor (payee) is for Client's information and Bank has no duty to comply with Client's payee's election to receive payments by ACH or commercial card, but Client may choose to change the payment type of the payee by specifying the applicable payment type in Client's Payment Data file.

   c. PIM Vendor Services. Client or Client's payees may elect to obtain additional services directly from Bank's PIM service vendor, including, but not limited to, data download capabilities. Bank does not provide these additional services and such services are subject to this Agreement solely between the vendor and Client, and vendor is not acting on behalf of

Bank in providing such additional services to Client. Bank has no obligations or liabilities with respect to such additional services and is not responsible for any obligations or liabilities that may arise in the course of the vendor providing such additional services directly to Client or Client's payees.

Positive Pay, Payee Positive Pay, Check Block and Reverse Positive Pay

1. Description of Positive Pay, Payee Positive Pay, Check Block and Reverse Positive Pay Service. Positive Pay, Payee Positive Pay, Check Block, and Reverse Positive Pay services allow Client to provide Bank instructions regarding payment or return of certain checks Client believes are fraudulent or not validly issued. Details regarding the functionality, formatting, and other technical requirements for these services are provided in the applicable reference materials.

2. Service Options. Client may select either Positive Pay, Payee Positive Pay, Check Block or Reverse Positive Pay. Each account enrolled in the respective service option is referred to herein as an "enrolled account."

    a. Positive Pay and Payee Positive Pay. Positive Pay and Payee Positive Pay services help Client detect unauthorized, counterfeit, altered or otherwise fraudulent checks on Client's enrolled account(s) by comparing issued check (and any voided check) information provided to Bank by Client against the checks that post to an enrolled account. Payee Positive Pay provides stronger protection against fraudulent checks by comparing payee names from Client's issued check file with the payee name on the check, in addition to the standard check number and account fields that are compared with the Positive Pay service. In order for the payee name verification process to function correctly, the payee name must be clearly displayed on client's printed checks, and the payee name provided in the issued check file should exactly match the name printed on the check. The following terms apply to both Positive Pay and Payee Positive Pay service options.

        i. Presentment Processing. Positive Pay and Payee Positive Pay require Client to transmit an issue file to Bank on each day on which Client has issued any checks against an enrolled account. Bank must receive that issue file by the deadline set forth in the reference materials and the file must contain the information set forth in the reference materials with respect to each check listed in the file. Client may send Bank a separate issue file for each enrolled account, or may send an aggregate issue file for all of Client's enrolled accounts. Once Bank has received Client's issue file, then Bank will compare the checks identified in that issue file with the information in Bank's systems regarding the checks (1) that have been presented to Bank through normal check clearing channels for payment against the enrolled account and that Bank has posted to the enrolled account, and (2) for which Bank has provisionally settled. Client authorizes Bank to finally settle the charges against the enrolled account, for each check that Bank reasonably determines to match the information in Client's issue file. Bank will notify Client of each presented check that is not included in the issue file or that reflects information that does not reasonably match the information in the issue file ("mismatched checks"). Client must instruct Bank to pay or return each mismatched check by the payment decision deadline set forth in the reference materials; such instruction is a "decision."

        ii. Mismatched Checks. Client may elect one of two ways for Bank to handle mismatched checks if Client fails to provide a pay or return decision by the payment decision deadline for Positive Pay or Payee Positive Pay. Bank will process and pay all exceptions according to Client's default settings.

            1) Return Default. Under the "return default" option, Client authorizes Bank to return each mismatched check as unpaid, unless Bank receives an instruction from Client to pay it before the payment decision deadline. Even if Client selects a return default option, Bank may post, finally settle and charge against the enrolled account a mismatched check the Client hasn't decisioned (A) as otherwise provided below, for mismatched checks presented over the counter in one of Bank's branches and (B) mismatched checks that Bank believes in good faith result solely from encoding errors.

            2) Pay Default. Under the "pay default" option, Client authorizes Bank to finally settle each mismatched check and charge it against the enrolled account unless Bank receives an instruction from Client to return it before the payment decision deadline.

        Client may opt not to provide information in Client's issue file for (i) one or more check attributes that Positive Pay and Payee Positive Pay are capable of matching or (ii) certain items in situations where Client deems it necessary to avoid mismatch situations, such as instances where Client believes an item has already been legitimately paid. Client acknowledges that not providing information to allow for matching of all available check attributes or not including information for all items increases the risk that a fraudulent check will not be detected as a mismatched check. If Client fails to provide information in Client's issue file regarding all available check attributes that the service is capable of matching, or Client fails to provide an issue record for a check at all for any reason, then Bank will not be

liable for paying any check that is fraudulent with respect to the attributes for which Client failed to provide the Bank information, or for paying an item for which the Client chose to provide no issue record, provided Bank otherwise satisfied its duty of care with respect to the other aspects of the Positive Pay or Payee Positive Pay service in processing that check.

iii. Teller Access Service. As part of the Positive Pay or Payee Positive Pay service, Bank will also make Client's issue files available to Bank's branches to assist Bank's tellers in cashing checks ("teller access"). If a check presented for payment against an enrolled account over the counter in one of Bank's branches (1) is presented before Bank has received and processed an issue file for such check, (2) is a mismatched check, or (3) is otherwise identified by Bank as suspect, then Bank will not pay the check and will refer the presenter back to Client. If a check that matches the issue file information in check number and amount is presented to Bank for cashing over the teller line and the payee name, if provided by Client, does not match the name viewed on the check by the teller, then Bank may in its discretion decide to pay the check, or to not pay the check and refer the presenter back to Client.

b. Check Block. If the Check Block option is selected, all incoming check entries to an enrolled account will be blocked.

c. Reverse Positive Pay. Reverse Positive Pay helps Client detect unauthorized, counterfeit, altered or otherwise fraudulent checks on Client's enrolled account(s), by providing Client with information on checks (i) that have been presented to Bank through normal check clearing channels for payment against the enrolled account, (ii) that Bank has posted to the enrolled account, and (iii) for which Bank has provisionally settled. Client must compare that information with Client's own information for checks that have been issued from the enrolled account. If Client determines that a check included in the information Bank provides should be returned, then Client must notify Bank by the payment decision deadline set forth in the Reverse Positive Pay reference materials. If Bank does not receive a notice from Client to return a check by the payment decision deadline, then Client authorizes Bank to finally settle and charge that check against the enrolled account. Teller access is not available for Reverse Positive Pay and checks submitted through the teller line will not be available for pay or return decisions by Client. As a result, Client agrees that if Client selects Reverse Positive Pay, then Bank will not have any liability for paying or returning any check that is presented over the counter in one of Bank's branches, whether or not such check bears a forged or unauthorized signature or is counterfeit, altered or otherwise fraudulent or is not validly issued, so long as Bank otherwise processes that check in accordance with Bank's standard check cashing procedures. In addition, Client acknowledges that if Client selects Reverse Positive Pay, Bank may not provide Client information for all check attributes (such as the payee name) that the Positive Pay or Payee Positive Pay option is capable of matching.

3. Transmission of Information. Bank will transmit information regarding mismatched checks (for Positive Pay and Payee Positive Pay) and information regarding checks that have posted to an enrolled account (for Reverse Positive Pay) to Client by using one of Bank's online services designated in the reference materials. Client must transmit the issue files (for Positive Pay and Payee Positive Pay) and/or Client's pay or return decisions to Bank by using one of Bank's online services as designated in the reference materials. Client's issue files and pay or return decisions must be in a format acceptable to Bank. In the event the applicable online service is not available, then a mutually agreed-upon alternative delivery method and process will be used to provide the relevant information to Client and for Client to provide the issue files and/or pay or return decisions to Bank. Client will designate one or more operational contacts for Positive Pay, Payee Positive Pay or Reverse Positive Pay. Bank may, in its sole discretion, contact these operational contacts in the event Bank has questions about Client's issue file, the relevant online service is not available, to set up an alternative delivery method, or for other operational issues with the service options. These operational contacts are authorized to instruct Bank to pay or return any mismatched check (for Positive Pay or Payee Positive Pay) or any check that has posted to Client's account (for Reverse Positive Pay), in the event that Bank, in its sole discretion, contacts an operational contact regarding such check.

4. Limits on Bank's Liability. Client acknowledges that Bank will rely on information and instructions Client gives Bank in providing Positive Pay, Payee Positive Pay or Reverse Positive Pay service and that Bank is not required to inspect any attribute of a check (other than those included in the relevant issue file) that is processed through these service options. Bank will not have any liability for paying or returning any check in accordance with these terms and conditions, including any check that (i) bears a forged or unauthorized signature or is counterfeit or otherwise not validly issued or (ii) is altered or otherwise fraudulent with respect to an attribute that the Positive Pay, Payee Positive Pay or Reverse Positive Pay service is not designed to match. Client will be precluded from asserting any claims against Bank with respect to losses for any fraudulent check that was paid or returned in accordance with these terms and conditions. Client also acknowledges that Positive Pay, Payee Positive Pay and Reverse Positive Pay services are not a substitute for Bank's stop payment service, or a means to reject checks that were validly issued but for which there exists a dispute with respect to the underlying transaction, and Client agrees not to report an item as "void" if Client has released the item for payment.

TRUIST

Real-Time Payments Service

1. Description of Real-Time Payments Service. Real-Time Payments Service ("RTP") allows Client to send or receive messages through a Real-Time Transfer System ("RT System"). Client sends and receives messages through an online banking service provided by Bank, and the messages may or may not be associated with a particular payment, initiate a payment, or send requests for payments in accordance with these terms ("RT Terms").

   Messages are sent or received by a natural person, business, government, nonprofit organization, or other entity ("Person") through a financial institution or third party service provider participating in the RT System ("Service Participant"). Client must be approved by Bank before using RTP to send requests for payment to Persons. Client agrees that any use of RTP, including but not limited to receiving or sending messages or payments, failure to return payments, or error resolution, will be in accordance with the Real-Time Payments Operating Rules ("Rules"), located at www.theclearinghouse.org. The Rules are hereby incorporated by reference into the RT Terms.

2. Important Disclosures regarding RTP.
   a. Payments through RTP are irrevocable and cannot be reversed. Client is responsible for verifying the correct Receiver Addressing Information of Payment Messages as such terms are defined herein.
   b. Bank will rely solely on the bank routing number and account number, in a received payment or message regardless of whether the name of the Person in the payment or message matches the name associated with the account number in the Bank's records.
   c. Client should only use RTP to make payments to Persons known to the Client. If a Person contacts the Client outside of RTP and asks for payment, then Client should verify the identity, legitimacy and contact information of the requestor and the amount of the payment prior to submitting a RTP Transfer Request, as such term is defined below. Client may lose the full amount of Client's payment if Client:
      i. sends payment to a Person whose identity is not accurately verified,
      ii. provides improper payment routing information, or
      iii. fails to verify the legitimacy of a payment.
   d. Client acknowledges and agrees that Bank has no obligation to verify the accuracy or completeness of the information that Client provides in order to send a payment.

3. Security procedures. The security procedures for RTP are the security procedures applicable to external payments initiated within the Bank's online banking service including but not limited to authorization codes required to log in to the online banking service, dual approval requirements, and token authentication requirements. Client agrees that use of RTP constitutes acceptance of these security procedures.

4. Messages. Client initiates RTP messages by submitting a request ("RTP Transfer Request") through Bank's online banking service, or such other access channels as made available by Bank from time to time and in accordance with applicable terms for such access channels. The Person sending a message through RTP is a "Sender." When Client submits a RTP Transfer Request as a Sender, Client will be required to provide information about the Person to receive the message including but not limited to a routing number to identify a Service Participant and as more particularly contained in the reference materials. The Person receiving the message is the "Receiver," and the Receiver's information is collectively the "Receiver Addressing Information." By submitting a RTP Transfer Request, Client represents and warrants that such RTP Transfer Request and any funds transfer associated with it complies with these RT Terms. Bank will submit Client's message to the RT System and the RT System will deliver Client's message to the Service Participant in accordance with these RT Terms and as identified through the Receiver Addressing Information provided by Client. The Service Participant will deliver the message to the account identified in the Receiver Addressing Information.

5. Transaction Limits. Transaction limits may be established and adjusted, as well as daily, weekly, or monthly limits on amounts sent and received through RTP for such period ("Transaction Limits"). Any attempted Payment Message that exceeds a respective Transaction Limit may fail. Bank will provide applicable limits upon client request. It is Client's responsibility to notify any Person of the Transaction Limits, if such Person has a need to know the limits.

6. Sending Funds. Client, as a Sender, may use a RTP Transfer Request to initiate a funds transfer to a Receiver ("Payment Message"). In addition to the Receiver Addressing Information, a Payment Message will require the amount of funds ("PM Amount") the Sender directs the Bank, as the "Sending Participant," to transfer to a Receiver. The Payment Message will be delivered to a Service Participant as identified through routing and account information in the Receiver Addressing

Information (such Service Participant is a "Receiving Participant"). The Receiving Participant does not verify any Receiver Addressing Information in the Receiving Participant's records matches the account number in the Receiver Addressing information.

By submitting a Payment Message, Client irrevocably and unconditionally authorizes Bank to initiate a payment for the PM Amount using the Receiver Addressing Information, and immediately deduct the PM Amount plus any fees payable by Client to Bank in conjunction with the applicable Payment Message from Client's account. For Payment Messages, **EXCEPT AS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW, BANK'S SOLE OBLIGATION SHALL BE TO INITIATE A PAYMENT BY SENDING A PAYMENT MESSAGE THROUGH RTP IN THE PM AMOUNT INDICATED BY CLIENT USING THE RECEIVER ADDRESSING INFORMATION PROVIDED BY CLIENT. EXCEPT AS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW, BANK SHALL HAVE NO LIABILITY TO CLIENT WITH RESPECT TO ANY LOSS THAT CLIENT EXPERIENCES DUE TO THE INACCURACY OR INCOMPLETENESS OF SUCH RECEIVER ADDRESSING INFORMATION, THE FAILURE OF SUCH INFORMATION TO BE ASSOCIATED WITH CLIENT'S INTENDED RECEIVER, OR CLIENT'S FAILURE TO CORRECTLY ENTER THE RECEIVER ADDRESSING INFORMATION OR THE PAYMENT MESSAGE AMOUNT.**

No buyer protection is provided with respect to RTP and Client cannot reverse or dispute a Payment Message on the basis that Client is dissatisfied with the goods or services provided in association with the Payment Message i) because goods are not delivered or services are not performed, whether at all or in a timely manner; or ii) because Client wishes to return purchased goods or cancel a pre-paid service.

7. Requesting Return of Funds. RTP permits Client to submit a RT Transfer Request for a Receiver to return funds from a previous Payment Message sent by Client ("Return Request"), but the Receiver is not obligated to return the funds. This includes circumstances in which the incorrect amount of funds was transferred because Client entered the incorrect PM Amount, or funds were sent to someone other than Client's intended Receiver because Client incorrectly entered the Receiver Addressing Information or the Receiver Addressing Information entered by Client was associated with someone other than Client's intended Receiver. If Client wishes to send a Return Request, Client must notify Bank at 800-774-8179. Bank's sole obligation is to transmit the Return Request through RTP to the Receiving Participant for such Payment Message. Bank makes no representation that funds will be returned in whole or in part, and Bank shall have no obligation to make any effort to recover such funds beyond the transmission of the Return Request. Client agrees Bank will not be liable for failure of Receiver to return funds or any deficiency in amounts returned to, or recovered by, Bank.

   Any dispute between Client and a Receiver must be resolved directly between Client and the Receiver. **Bank has no responsibility for, and shall not be liable to Client in connection with, any dispute between Client and a Receiver.**

8. Availability of Funds. In accordance with the Rules and Failed Message section below, Funds transferred through RTP will be credited to the Receiver's account by the Receiving Provider immediately upon completion of the RTP Transfer Request and will be available for withdrawal by the Receiver immediately. Funds are immediately available 24 hours per day, 7 days per week, including weekends and state and federal holidays. RTP Transfer Requests are typically completed within 30 seconds of transmission of the RTP Transfer Request by the Sender, unless the Payment Message fails or is delayed as described below.

9. Receiving Payments. Client may receive a Payment Message through RTP as a Receiver if a Sender sends a Payment Message to Client. Client is not obligated to accept a payment that is sent to Client as a Receiver through RTP. If Client wishes to reject a payment sent to Client through RTP, Client must contact Bank at 800- 774- 8179.

   A Sender may send Client, as Receiver, a Return Request through RTP. If Bank receives a return request, then Bank will contact Client.

10. Requests for Payment. Client may not issue RTP Transfer Requests to submit requests for payment unless Client has been approved by Bank to do so. If Client wishes to submit RTP Transfer Requests, as a Sender, requesting payments from Receivers ("Request Message"), please contact Bank at 800-774-8179.

11. Requesting Messages. If Client has been approved to submit Request Messages, the following Terms apply:

    a. Client may only submit a Request Message to Persons who (i) are known to Client and (ii) reasonably expect to receive a request for payment from Client;

    b. by submitting a Request Message, Client represents and warrants that the request is not for a Prohibited Payment (as defined below) and is not fraudulent, abusive, or unlawful;

    c. Client acknowledges and agrees that Bank does not warrant that the Request Message Receiver will send payment in response to, or otherwise accept, Client's Request Message; and

d. any dispute between Client and the Receiver of a Request Message must be resolved directly between Client and the Receiver. **Bank has no responsibility for and shall not be liable to Client in connection with any dispute between Client and a Receiver regarding the Request Message and any related Payment Message.**

12. Failed or Delayed Payment Message. Any Payment Message may fail or be delayed if:

    a. any Service Participant suspects or determines that the Payment Message does not comply with these RT Terms or Receiving Institution's terms for RTP;

    b. the Receiver rejects the Payment Message or has declined to receive Payment Messages or Request Messages;

    c. the RTP Transfer Request exceeds a Transaction Limit for a transaction or period;

    d. the Sender's or Receiver's account at the respective Service Participant is closed, invalid, ineligible to receive Payment Messages or Request Messages, or is being monitored for suspected fraudulent or other illegal activity;

    e. any Service Participant otherwise declines to process the Payment Message for risk-management, legal, or regulatory reasons; or

    f. any component or RTP or Real-Time Transfer System is unavailable.

    If Client is the Sender, Bank will notify Client if a Payment Message fails. Client is responsible for communicating to the Receiver that the Payment Message has failed.

13. Reporting. If a RTP Transfer Request requesting a payment form Client does not relate to a payment Client was expecting to make to the Sender, Client should notify Bank immediately at 800-774-8179.

14. Prohibited Payments. Client agrees that it shall not use RTP to send or receive any of the following types of payments (a "Prohibited Payment"):

    a. payments that violate any local, state, or federal law or regulation;

    b. payments to accounts domiciled outside the United States;

    c. payments transmitted solely for the purpose of determining whether the Receiver Addressing Information is valid (a "Test Payment"), provided Client may conduct a Test Payment if Client has a bona fide need to do so in order to determine the validity of Receiver Addressing Information provided to Client by a Receiver that wishes to receive a payment from Client; or

    d. any other payment that the Bank may deem as prohibited, to which the Bank will provide notice to the Client.

    Client acknowledges that Client is permitted to use RTP solely for the purpose of sending or receiving messages (i) on Client's own behalf or (ii) on behalf of Persons that are residents of or domiciled in the United States. If Client sends or receives payments on behalf of another Person, then Client must comply with all applicable laws and regulations in conjunction with such payments, including all regulations of the Office of Foreign Assets Control. Client acknowledges that any payment that violates the foregoing restrictions is a Prohibited Payment.

15. Transaction Errors; Unauthorized Transactions; Lost or Stolen Credentials. If Client believes that an erroneous or unauthorized payment has been made through RTP using Client's account or that Client's account credentials, Client should contact Bank immediately at 800-774-8179.

Remote Deposit Capture Service

1. Description of Remote Deposit Capture Service. The Remote Deposit Capture ("RDC") service and the internet based RDC system allow Client to capture an electronic image of an original physical paper check and an image of associated information describing that check including optical character recognition (OCR) remittance coupons and transmit the image of the check to Bank for deposit to Client's account. The RDC service also provides access to, and the ability to export and print, deposited check images and remittance coupon images as well as reports regarding Client's use of the RDC service. Further details regarding RDC's functionality and formatting and other technical requirements that Client must follow when using the RDC service are provided in the RDC reference materials. The RDC service may not be used outside of the United States, U.S. territories, U.S. military bases or U.S. embassies and files may not be transmitted from outside the United States unless transmitted from a U.S. territory, military base or embassy. The RDC Service may not be used to deposit ineligible items as described in the RDC reference materials.

2. Required Hardware and Software. Before Client can use the RDC service, Client must have a computer capable of internet access, a scanner of a model approved by Bank, and the related software needed to capture electronic images of checks, associated information and remittance data. Equipment upgrades or replacements may be required from time to time, and it is the responsibility of Client to upgrade or replace scanner(s) as needed. When Client acquires a scanner from a third-party vendor Client agrees that all warranty obligations and contracts are between Client and the vendor, and Bank does not have any responsibility or liability for the performance of the vendor, the delivery of the scanner or any aspect of the operation, use or maintenance of the scanner. At Client's request, Bank may provide Client's contact information and information related to Client's desired scanner to a third party vendor, in order to facilitate communication between the vendor and Client regarding Client's scanner acquisition or rental. Client agrees that Bank is only providing this information to the third party vendor as an accommodation to Client to facilitate Client's potential acquisition or rental of a scanner and that Bank does not have any responsibility or liability for the performance of the vendor or the delivery of the scanner(s) or any aspect of the operation, use or maintenance of the scanner(s).

3. Primary Administrator. Client must designate a Primary Administrator of the RDC service who can establish additional RDC users and administrators.

4. Use of the RDC Service. A user of the RDC service must log on to the RDC system using valid credentials. The user will be required to provide a control total for each deposit, consisting of the total dollar amount of all checks included in the deposit. Images of checks submitted for deposit must meet the eligibility and image quality standards set forth in the RDC reference materials and in these RDC terms and conditions. All such standards are referred to as the "RDC standards." If the RDC system determines an image does not satisfy the RDC standards, the RDC system will reject the nonconforming image and ask the user to either a.) rescan the check, b.) manually provide or verify information or, c.) for certain types of limited image quality failures, confirm the user's election to submit the image or associated information as captured. **Please note that the option for the user to elect to submit an image as captured in the RDC system in certain limited situations does not relieve Client of the representations and warranties Client makes with respect to each image and associated information Client transmits to Bank.** Only users with approval permission can submit the deposit to Bank for processing. Once a deposit has been submitted, it may not be cancelled. Once Bank has received a deposit Bank will process the deposit file per Bank's normal check processing channels.

5. Dual Approval. Dual approval is an optional security feature of the RDC service. If the dual approval option is selected, one user must scan the check images and then a second user with approval permissions must release and send the check image file to Bank. **Bank highly recommends that Clients use the dual approval option.**

6. Posting File. If Client elects to receive an accounts receivable posting file as a part of this service, Bank will deliver the file to Client in the format and via the method and schedule agreed upon with Bank.

7. Deposit Credit and Alternative Deposit Methods. Bank must receive Client's deposit by the daily deadline set forth in the RDC reference materials in order for Client to receive credit for that deposit on that business day. Deposits received after the deadline or a non-business day will be considered deposited on the next business day. Bank is not liable for any delays or errors in transmission of the images or associated information. If the RDC service is not available, Client must make Client's deposits by another method, such as an in-person deposit at one of Bank's branches, at an ATM or a deposit by mail. If Client must make a deposit by other means due to RDC service being unavailable, Client should deposit only checks and should retain in Client's possession the other documents Client would normally scan with an RDC deposit.

8. Funds Availability. Bank will make funds for each substitute check or electronic item that Bank processes for deposit to Client's account available to Client under the same schedule that would have applied if Client had deposited the original paper check to Client's account.

9. Returns and Rejected Images. If Bank determines an image or associated information is not in a satisfactory form or is a duplicate, Bank may reject the nonconforming image or duplicate item and provide any associated debit adjustment and/or debit advice. Bank will send Client all check images which fail to meet collecting bank quality standards. If an image is rejected for failing to meet the RDC standards or the collecting bank quality standards, Client must take corrective action to either recapture the image and associated information and submit it in a new RDC file transmission or submit the original check for deposit.

10. Original Checks and Captured Images. Client agrees to use commercially reasonable policies and procedures, and to comply with any requirements in the RDC reference materials, to safeguard the original physical paper checks, images of the checks and associated information in Client's possession both before and after Client has transmitted images of such items to Bank, and to endorse or mark paper checks to indicate they have been transmitted for deposit. Client also agrees to make all such items available to Bank promptly upon Bank's request. Client also agrees to establish reasonable retention and destruction schedules in accordance with any applicable requirements within the RDC reference materials.

11. Client's Representations and Warranties. Client represents, warrants, and agrees that Client will not:

    a. capture or transmit more than one image of any original check;

    b. negotiate, deposit, or otherwise transfer any original check to Bank or to any other person or entity after Client has captured an image of it;

    c. transmit an image of any original check to Bank that Client has previously transmitted or given to any other person or entity;

    d. transmit an image of any original check to any other person or entity after Client has transmitted it to Bank;

    e. transmit an image of any original check if that check has been used as a source document for the initiation of an ACH or other electronic debit; or

    f. use any original check as a source document for the initiation of an ACH or other electronic debit after Client has transmitted an image of (or associated information regarding) that check to Bank.

    Client also makes all the representations and warranties to Bank with respect to each check image that Client transmits to Bank that Client would have made under the Uniform Commercial Code (UCC) if Client had deposited the original physical paper check into Client's account.

    In addition, Client represents and warrants to Bank with respect to each captured check image and associated information Client transmits to Bank that:

    a. the image and associated information (i) accurately represent all the information on the front and back of the original physical paper check at the time it was received by Client and at the time the image and associated information were captured; and (ii) are otherwise sufficient for Bank to satisfy its obligations as the truncating and reconverting bank; and

    b. no person or entity will receive a transfer, presentment or return of, or otherwise be charged for, (i) the original check, (ii) an electronic item or substitute check other than the one that Bank creates from the image and associated information, or (iii) a paper or electronic representation of the original check or of a substitute check other than the one that Bank creates from the image and associated information, such that the person or entity will be asked to make a payment based on a check that it has already paid.

12. Duty of Cooperation, Document Production, Audit. Client agrees that Client shall make original and imaged documents available to Bank to facilitate investigations related to unusual transactions or poor image quality transmissions, or to resolve disputes. Client further agrees that Bank, at Bank's option, upon prior notice, may perform periodic audits of Client's processes related to use or proposed use of the RDC service including Client's information technology, security and internal control infrastructure related to Client's use of the RDC service. Client agrees that Bank has the right to mandate specific internal controls at any of Client's locations that use the RDC service where Bank deems such actions necessary to protect the security and integrity of the RDC service or if required by law, and that Bank may terminate the service if Client refuses to implement such controls.

13. Client's Indemnification Obligations. In addition to any other obligation Client has to indemnify Bank, Client agrees to defend, indemnify, protect and hold Bank, Bank's affiliates, Bank's vendors and Bank's respective officers, directors, employees, attorneys, agents, and representatives harmless from and against any and all liabilities, claims, damages, losses, demands, fines (including those imposed by any Federal Reserve Bank, clearing house or funds transfer system), judgments, disputes, costs, charges and expenses (including litigation expenses, other costs of investigation or defense and reasonable attorneys' fees) which relate in any way to (a) the use of the RDC system or RDC service to capture an image of a remotely created check, (b) Client's use of the RDC system or the RDC service in a manner other than as expressly provided in these RDC terms and conditions or (c) the receipt by any person or entity of (i) an electronic item, (ii) a substitute check or (iii) a paper or electronic representation of the original check or the substitute check that Bank creates from a captured check image and associated information that Client transmit to Bank, instead of the original check.

14. Termination. Upon termination of the RDC service by either Client or Bank, Client shall be solely responsible for complying with any terms or contracts relating to rental of a scanner, and for paying any early termination fees that may apply to Client's rental or acquisition of a scanner.

Sub-Accounting Service

1. Description of Sub-Accounting Service. Sub-Accounting Services provides the ability to maintain separate information within one master demand deposit account for virtual sub-accounts containing funds owned by individual entities / customers.

Using the Sub-Accounting Services web portal, Client can (a) set up, manage and close virtual sub-accounts under a master account, (b) allocate transactions to virtual sub-accounts, and (c) view and download reports. Details regarding the web portal's functionality, creation of users and additional administrators, adding or deleting sub-accounts, and certain formatting and other technical requirements for Sub-Accounting Services are provided in the current versions of the Sub-Accounting Services reference materials which include a user manual for the web portal.

2. User Administration. Client must identify a User Administrator for Sub-Accounting Services. This User Administrator will be reflected on a Treasury Request Confirmation and will have the ability to (a) create and establish entitlements for users, (b) reset user passwords, and (c) create additional administrators with the appropriate level of entitlements, up to and including those of the User Administrator. To change the User Administrator, an Authorized Individual must contact Bank. The User Administrator change will be reflected on a Treasury Request Confirmation.

3. Deposits and Withdrawals. Funds may be deposited into and withdrawn from the master account. No deposits or withdrawals can be transacted directly to or from a sub-account. Within the web portal, entitled users can virtually allocate funds to or from the applicable sub-account and view reports. **Except as explicitly provided in these Sub-Accounting Services terms and Conditions, Client is responsible for all sub-account allocation and administration.** Withdrawals from the master account may be made by any means made available by Bank. Following a withdrawal from the master account Client must indicate one or more sub-accounts from which the funds are to be debited. No third party, including any beneficial owner of a sub-account, shall have the right to exercise any control over or provide instructions to Bank regarding Sub-Accounting Services or any master account or sub-account.

4. Allocation Rules and Interest Allocation. At the time of service implementation, Client can specify rules for automatic allocation of funds to sub-accounts. An Authorized Individual can also request or modify automatic allocation rules by contacting Bank. For interest bearing master accounts, Client can request an automatic interest allocation at the sub-account level based on the pro rata share of the master account's monthly average balance. Interest allocation occurs at the end of the month based on the total amount of interest earned by the master account. Client can request automatic interest allocation at the time of service implementation. In addition, an Authorized Individual can request or revoke automatic interest allocation at any time by contacting Bank.

5. Addition and Deletion of Accounts Associated with the Sub-Accounting Services. To add or completely delete a master account, an Authorized Individual must contact Bank. Sub-accounts can be added or deleted by any entitled user within the web portal.

6. Responsibility for Compliance. In using Sub-Accounting Services, Client acts as the fiduciary for the beneficial owners of funds held in sub-accounts, and Client is solely responsible for the management and disbursement of all funds held in the master account, the actions of all users of Sub-Accounting Services, access to information regarding the accounts through the service, timely allocations to and from sub-accounts (including any applicable interest) and compliance with any laws, regulations, tax reporting and other requirements or agreements applicable to such funds. Client acknowledges that Sub-Accounting Services is not designed to comply with the requirements of any state's law that may govern funds deposited in such sub-account structures, or to satisfy Client's obligations with respect to the beneficial owner of funds in any sub-account, including any obligation under applicable law or regulation to pay any prescribed interest on the principal. Bank is not acting as escrow agent, trustee or in any other fiduciary capacity with respect to Sub-Accounting Services, any master account or any sub-accounts and undertakes no duty to monitor usage of Sub-Accounting Services or the actions of any user. Sub-Accounting Services is not designed as a system of record for establishing pass-through of FDIC insurance coverage for the virtual sub-accounts; therefore, Client is responsible for maintaining any records necessary to comply with FDIC regulations regarding eligibility for pass-through FDIC insurance. Client should consult with tax and legal advisors regarding all legal, tax, or other liability or regulatory issues with respect to use of Sub-Accounting Services.

7. Tax Reporting. Bank will provide required tax information reporting for each master account. At Client's request, Bank will provide tax information reporting for each sub-account by mail, provided Client has supplied Bank with necessary tax documents (IRS Form W-9 or W-8) for such sub-account. Client is responsible for the accuracy of all balances reported in the sub-accounts, interest allocation and tax reporting related to such interest allocations, as well as the accuracy of the necessary tax documents Client obtains from its customers.

SWIFT for Corporates Service

1. Description of SWIFT for Corporates Service. The SWIFT for Corporates service ("SWIFT") allows Client (as a direct participant, a SCORE member, or via an initiating party) to exchange SWIFT messages with Bank through the SWIFT network. Bank may

provide certain details regarding formatting and technical requirements to Client within SWIFT service reference. The SWIFT service supports the following FileAct and FIN messages and file types:

a. FileAct Services – Secure File Transfer Services. BAI2
EDI 822
EDI 820
Bulk Payment Files ACH
Positive Pay
ISO PAIN.001 – Payments (Wire, ACH, Check) ISO
PAIN.002 – Level 1-3 Acknowledgements CAMT.052
– Current Day Reporting CAMT.053 – Previous Day
Reporting

b. FIN Services – Core Messaging & Information Reporting Services. MT101 –

Request for Transfer
MT103
MT900 – Debit Confirmation MT910 –
Credit Confirmation
MT940 – Customer Statement Message MT942 –
Current Day
MT950 – Statement Message

2. Definitions. The following terms have the specified meanings for purpose of these SWIFT terms and conditions:

a. "Authorized SWIFT participant" means a person who is duly bound as a party to a SWIFT agreement allowing access to SWIFT and meets all eligibility criteria specified or referred to in that SWIFT agreement or the SWIFT documentation; provided, for the avoidance of doubt, that Client will continue to be an authorized SWIFT participant despite no longer satisfying such eligibility criteria during any period(s) specified in such SWIFT agreement as the period(s) (if any) given to Client to migrate to an alternative solution.

b. "Banking services" means the banking and other services (including treasury management services and wire transfer services) Bank provides Client in relation to which SWIFT messages are exchanged by way of the SWIFT messaging services that are identified in Client's SWIFT service documentation.

c. "Banking services agreement" means, with respect to any banking service, the agreement governing Client's use of such banking service. Without limiting the generality of the foregoing, the banking services agreement with respect to any of Bank's treasury management services addressed in this Agreement means this Agreement including all applicable terms of such treasury management services, and Bank's Wire Agreement.

d. "Wire Agreement" means, Bank's Wire Agreement (which is incorporated into this Agreement).

e. "Information" means the content of any SWIFT message Bank sends Client by way of the SWIFT messaging services including any account status or other information.

f. "Initiating party" means a third party designated by Client and acting on behalf of Client to send or receive SWIFT messages. To the extent Client designates any initiating party as part of Client's SWIFT service documentation, SWIFT messages received by Bank from such initiating party shall be deemed to be received from Client, and SWIFT messages sent by Bank to such initiating party shall be deemed to be sent to Client.

g. "Instruction" means the content of any SWIFT message Bank receives from Client by way of the SWIFT messaging services, including any actual or purported advice, request, instruction or communication, whether received directly from Client or from an initiating party.

h. "Operating account" means a bank account Client maintain(s) with Bank that is identified in Client's SWIFT service documentation.

i. "SCORE" means the standardized corporate environment service set up and administered by SWIFT.

j. "SWIFT" means S.W.I.F.T. SCRL, a Belgian limited liability co-operative society of Avenue Adele 1, B-1310 La Hulpe, Belgium.

k. "SWIFT agreement" means any then current agreement Bank or Client has with SWIFT in relation to the use of the SWIFT messaging services.

l. "SWIFT documentation" means the SWIFT terms, conditions, guides and procedures applicable to the SWIFT messaging services, to SCORE or to the sending and receiving of SWIFT messages within SCORE, as incorporated into Client's SWIFT agreement or that Bank or SWIFT notifies Client of from time to time.

m. "SWIFT message" means an electronic communication, message or file sent or appearing to have been sent using the SWIFT messaging services.

n. "SWIFT messaging services" means SWIFT's messaging services which are available within SWIFT and/or SWIFT SCORE from time to time.

o. "SWIFT service documentation" means any Bank documentation relating to Client's implementation or setup of SWIFT services, including but not limited to any Treasury Request Confirmation and internal Bank implementation form relating to the SWIFT service.

3. Scope of This Agreement.

a. Client, or an initiating party on behalf of Client, as designated in Client's SWIFT service documentation, (i) may electronically transmit SWIFT messages (including SWIFT messages which contain instructions), by way of the SWIFT messaging services, to Bank and (ii) will receive SWIFT messages (including SWIFT messages which contain information), by way of the SWIFT messaging services from Bank.

b. Bank (i) will receive SWIFT messages (including SWIFT messages which contain instructions) by way of the SWIFT messaging services, from Client, or an initiating party on behalf of Client, and process them as described herein and as defined in Client's SWIFT service documentation, and (ii) may electronically transmit SWIFT messages (including SWIFT messages which contain information), by way of the SWIFT messaging services to Client, or an initiating party on behalf of Client, as defined in Client's SWIFT service documentation.

c. These SWIFT terms and conditions, SWIFT messages from Client, and Client's SWIFT service documentation constitute valid and binding instructions from Client granting Bank authority to act in accordance with SWIFT messages and instructions.

d. Bank and Client will use the SWIFT messaging services to facilitate Bank's provision, and Client's use of the banking services as specified in Client's SWIFT service documentation. However, Client acknowledges that provision and use of such banking services are outside the scope of these SWIFT terms and conditions and shall be governed by the relevant banking services agreement rather than these SWIFT terms and conditions, except as specifically provided otherwise in these SWIFT terms and conditions. In the event of a conflict between these SWIFT terms and conditions and the terms of any banking services agreement, the terms of these SWIFT terms and conditions shall control.

4. Payment Orders and Security Procedures. To the extent Client uses the SWIFT service to send "Payment Order" (as such term is defined in the Wire Agreement) instructions to Bank, or Bank sends any information to Client relating to a Payment Order, then (as applicable) (A) each such instruction shall be deemed to be an "Instruction" or a "Payment Order" for all purposes of, and shall be subject to the terms of, the Wire Agreement; (B) such information shall be deemed to be a "Confirmation" or a "Statement" for all purposes of, and shall be subject to the terms of, the Wire Agreement; (C) the security procedure for verifying the authenticity of each such instruction for all purposes of the relevant banking services agreement shall be deemed to be the steps that are mandated at the time by the then current SWIFT documentation to establish that Client authorized the SWIFT message (rather than the security procedures specified in the relevant banking services agreement) and Client agrees that the steps outlined in the SWIFT documentation constitute a "commercially reasonable security procedure" as that term is used in Article 4A of the Uniform Commercial Code as in effect in the state whose laws govern the relevant banking services agreement, and Client agrees that use of the SWIFT service constitutes acceptance of such security procedure; and (D) any such instruction, the authenticity of which is verified in accordance with the steps that are mandated at the time by the then current SWIFT documentation to establish that Client sent the SWIFT message shall be deemed to be Client's valid and binding instructions, for all purposes of the relevant banking services.

5. Rights and Obligations Related to the Use of SWIFT Messaging Services.

a. Bank will provide the electronic communication services designated in Client's SWIFT service documentation, through the use of the SWIFT messaging services.

b. If applicable to Client's use of the SWIFT messaging services, Client must be an authorized SWIFT participant at all times these SWIFT terms and conditions are in effect or the terms and conditions are applicable to SWIFT services used in conjunction with another product or service.

c. Client must at all times comply with all requirements relating to SWIFT messaging services, including security requirements and requirements relating to SWIFT messages, arising out of the SWIFT agreement or the SWIFT

documentation, in connection with these SWIFT terms and conditions. If Client or an initiating party sends a SWIFT message (including a SWIFT message that includes an instruction) by way of the SWIFT messaging services to Bank and such message is not defined in Client's SWIFT service documentation, Bank may, at Bank's option (i) reject or otherwise not act on such SWIFT message and any instruction contained in such SWIFT message or (ii) accept and otherwise act on such SWIFT message and any instruction contained in such SWIFT message.

d. Client must (i) at all times comply with Bank's requirements as set out in the reference materials, and such reasonable instructions and recommendations as Bank provides Client from time to time in relation to the use of the SWIFT messaging services; and (ii) confirm that Client has assessed the security arrangements relating to Client's access to and use of the SWIFT messaging services and concluded that they are commercially reasonable and adequate to protect Client's interests.

e. Client must immediately notify Bank if Client becomes aware of or suspect any potential breach or compromise of the security of the SWIFT messaging services including any that relate to Client's or Bank's rights and obligations under these terms and conditions, such as any loss or disclosure of (or any person other than a person duly authorized in accordance with the SWIFT documentation and Client's own procedures seeking to obtain or obtaining) the means to send SWIFT messages or the actual transmission of a SWIFT message, and provide Bank full details of the suspected breach or compromise.

f. Client must (except to the extent prohibited by any applicable law or regulatory obligation) (i) fully and promptly cooperate with any steps Bank takes to investigate and/or rectify any apparent or suspected breach or compromise of the security of the SWIFT messaging services which is reported under Section 5(e) or otherwise comes to Client's or Bank's attention, including providing such further information regarding the apparent breach as Bank may request; and (ii) promptly provide Bank with such information as Bank reasonably requests to assist Bank in the performance of Bank's obligations under any SWIFT agreement.

6. Bank's Reliance on Instructions.

a. Client must ensure that any instruction included in any SWIFT message Client (or an initiating party) sends Bank by way of the SWIFT messaging services fully and accurately reflects the advice, request, instruction or communication that Client intends to provide Bank and is duly authorized.

b. Client irrevocably authorizes Bank (i) to treat as accurate, authentic and properly authorized, rely upon and implement any instruction in a SWIFT message Bank receives by way of the SWIFT messaging services which Client or an initiating party on behalf of Client originates or appears to originate (including, in the case of a payment instruction, authorizing Bank to debit the operating account specified in the instruction); and (ii) to process each such instruction; provided that, subject to Section 6(c), Bank takes such steps as are mandated at the time by the then current SWIFT documentation to establish that Client sent such SWIFT message. Client acknowledges that (A) such steps constitute a "commercially reasonable security procedure" as that term is used in Article 4A of the Uniform Commercial Code as in effect in the state whose laws govern the relevant banking services agreement and (B) Bank is not obliged to verify such authorization, authenticity or integrity, even in the case of fraud, unless Bank has actual knowledge of the fraud.

c. In determining the steps to be taken to establish that Client sent a SWIFT message (i) no regard shall be given to any steps, or any information provided with the SWIFT message, that goes beyond what is mandated at the time by the then current SWIFT documentation, to identify Client as the sender of the SWIFT message; and (ii) Bank is not required to make any subjective judgment as to the appropriateness of the SWIFT message or any accompanying signature or certificate or otherwise.

d. Without prejudice to Sections 6(a) and 6(c), Bank is not obliged to act on an instruction or to treat an instruction as accurate, authentic or authorized, if: (i) the SWIFT message through which that instruction is provided does not meet the requirements of the then current SWIFT documentation or the reference materials or otherwise appears not to have been prepared or sent in accordance with these SWIFT terms and conditions; (ii) Bank considers that the execution of that instruction may place Bank in breach of any law or regulation; or (iii) Bank reasonably suspects that the SWIFT message in which that instruction was received may not (A) fully and accurately reflect an advice, request, instruction or communication that Client intended to give Bank; or (B) have been given in accordance with Client's authorization procedures. Except to the extent prevented by applicable law or regulation, Bank will use reasonable attempts to notify Client if, under this Section 6(d), Bank does not act on an instruction.

7. Termination and Suspension. In addition to any rights of termination and suspension in this Agreement, (a) Bank may terminate Client's use of the SWIFT service by notice to Client with immediate effect if (i) either Bank or Client, if applicable, are no longer an authorized SWIFT participant, (ii) SWIFT has ceased to provide the SWIFT messaging services, (iii) SWIFT, in exercise of its rights under a SWIFT agreement, has required Bank to terminate the SWIFT service, or (iv) Bank ceases

providing the banking services; and (b) Bank may suspend Client's use of the SWIFT service for such period as Bank considers appropriate in Bank's absolute discretion by notice to Client: (i) if suspension is necessary for the purposes of either routine or emergency maintenance; (ii) for security or technical reasons, including a suspension of the SWIFT messaging services by SWIFT; (iii) if use of the SWIFT messaging services is impossible or cannot be achieved without unreasonable cost; (iv) if suspension is required by SWIFT or the SWIFT documentation; or (v) if suspension is necessary to avoid or reduce any material damage or disadvantage to Bank.

Truist One View Service

1. Description of Truist One View Service. Truist One View is an online platform that provides a single point of access to certain banking services and account and transaction details. The services that can be accessed through One View fall into three categories:

    a. One View services. One View services are embedded in the online platform and include account balance information and transaction details and account statements for certain account types. Account balance information and transaction details may initially be displayed in One View based on Client's setup in Truist Treasury Manager or Digital Treasury but will later be managed within One View independently by a One View administrator. Additional One View services may be added over time. One View services may be opt- in services that require enrollment or may, at Bank's option, be automatically enabled within the service.

    b. Single sign-on services. Certain banking services (or applications) are or will in the future be enabled (either upon the instruction of a One View administrator or, at Bank's option, automatically enabled if Client uses the service) as single sign-on from within One View and are referred to as "SSO services". Terms and conditions for each SSO service apply to Client's use of such service and are incorporated herein. Users who are entitled to an SSO service can access the service from within One View without entering additional access credentials or authorization codes. The user's ability to access accounts or functions within the SSO service may require the user to be granted both (i) applicable One View entitlements by a One View administrator, as well as (ii) entitlements to the SSO service itself by either an administrator for that SSO service, or by a One View administrator.

    c. Other banking services. Links to other Truist banking services that Client may use are included in the service as a convenience. These services are not embedded in the One View service, nor are they single sign-on enabled. To access such a service, each user must enter the applicable access credentials and/or authorization codes assigned to them by an administrator for that specific service. The process to sign on to these other, "non-SSO services" is the same whether a user accesses the service using the link provided within One View or using the URL that has been provided by Bank for that service. Bank may enable some of these banking services as single sign-on over time. If Client uses one of these banking services and Bank enables that service for single sign-on within One View, Bank may automatically enable those services as SSO services within One View, or may, at Bank's option, require the instruction of a One View administrator in order to enable that service as an SSO service.

2. Security Procedures. The security procedures for the service are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.

    a. Access Credentials and Authentication. Valid access credentials (User ID and Password) and a second authentication method, which may include authorization codes, tokens, or other Bank-approved authentication methods, are required to log in to the service. Authentication may also be required to perform certain actions within One View.

    b. SSO Services. SSO services within One View may require additional security procedures to initiate funds transfers or payments, or to take other actions; the applicable security procedures described in the terms and conditions for each SSO service are incorporated herein by reference.

3. Administrative Approval. Administrative approval is a standard security procedure within the service. The administrative approval security procedure requires that, for certain administrative actions initiated by one user (including, without limitation, creating new users, updating user profiles, and user permission changes), at least one other user with sufficient permissions must review and approve the administrative action. Client can elect to require more than one administrative approval, in which case Client must create the users and assign permissions allowing these users to approve administrative actions. If Client elects to opt out of the administrative approval security procedure for Truist One View, Client must document this decision in writing and in accordance with Bank procedures. **Bank strongly recommends that Client not opt out of the administrative approval security procedure**.

4. Mobile App. A One View administrator can enable use of banking functions within the One View mobile application (app). Once banking functions within the app are enabled for Client, entitled users who download and install the app can, with valid access credentials and authentication, access certain banking functionalities of the service from their mobile device. A user's permissions within the app are limited by that user's permissions in One View (online). The app is available for iOS and Android devices. Certain banking features or functionality available within One View (online) may differ from those available within the app. If mobile banking functions are not enabled for a user, that user will have no access to banking features within the mobile app but can utilize their credentialed access to the mobile app for authentication purposes in connection with online services.

5. Designation and Entitlements of Truist One View Primary Administrators. Unless Client opts out of the administrative approval security feature as described in paragraph 3 above, Client must designate two One View Primary Administrators within a Primary Administrator Designation agreement (or similar agreement accepted by Bank). Client acknowledges that the Primary Administrator(s) have or may in the future have all of the following entitlements, which the Primary Administrator(s) can also assign to other users and users with administrative entitlements (One View administrators) such that other users have up to and including the same entitlements as the Primary Administrator:

   a. Full entitlements to all One View services and accounts set up for Client on One View. If services are opt-in, the Primary Administrator(s) may have the authority to opt-in for Client.

   b. The role of an administrator for the SSO services, including full entitlements and ability to perform all administrative functions for each SSO service.

   c. Ability to create, edit and delete users and users with administrative entitlements (One View administrators) within One View and the SSO services, assigning such users and administrators with the appropriate level of entitlements. The Primary Administrator(s) will not have any entitlements to non-SSO services, unless such individual(s) have been granted entitlements to the non-SSO services by the applicable administrator for the service.

   d. Ability to modify or delete the SSO service administrators.

   e. Ability to select statement delivery preferences (paper and online, or online only) for all deposit accounts included within One View. When online-only (electronic) statement delivery is selected for a deposit account, paper statement delivery will be suppressed for such account, and the statements for such account will only be available within One View to entitled users. Bank strongly recommends that Client establish appropriate internal controls to monitor deposit accounts for which statement suppression has been selected. Client's statements will be posted and available within One View in electronic format at the same time intervals (e.g., weekly, monthly, quarterly) that the paper statement for such account would have otherwise been printed and sent to Client.

   f. Ability to add any of the accounts (including, but not limited to, deposit accounts, loan or line of credit accounts, and credit, commercial, or purchasing card accounts) opened with Client's Tax ID Number (TIN) or otherwise associated or affiliated with Client (such as via an Associated Entity Agreement for Treasury Management Services, or other documentation accepted by Bank) to Client's One View setup, and to select which One View services or functionalities are available for such accounts.

   The Primary Administrator(s) as well as other One View administrators can create users (including administrators), disable/re-enable or delete users, and assign entitlements for accounts, One View services, and SSO services. However, an administrator can assign to others only those accounts and services to which the administrator is entitled. The Primary Administrator(s) can assign to others all accounts and services, since the Primary Administrator(s) have full access to accounts and services within One View.

6. Change of Truist One View Primary Administrator. To change the One View Primary Administrator(s), Client must execute a new Primary Administrator Designation agreement, naming the new One View Primary Administrator(s). **Note that when Client designates a new Truist One View Primary Administrator, the entitlements of a previous Truist One View Primary Administrator may not be automatically removed; therefore, it is the responsibility of the new Primary Administrator(s) to modify the entitlements of or deactivate any previous Primary Administrator(s) as appropriate.**

7. Terms for Specific Truist One View Services. Services accessed through Truist One View by clients that do not use deposit products with Truist, are not subject to any deposit account terms of the CBSA and any CBSA terms conflicting with the referenced agreements and/or terms in that specific Service section below ("Referenced Terms").

   Each Service listed below (each a Service under this this Agreement and referred to as a "Truist One View Service") is governed by the Referenced Terms and is accessed through Truist One View in accordance with this this Agreement. All capitalized terms in each Truist One View Service section are defined in the Referenced Terms or this this Agreement. Accessing any Service through Truist One View, or any other online access, is governed by this this Agreement, including but

not limited to the authorized individuals, administrative authorities, and security procedures. All ***activity*** regarding a Truist One View Service, regardless of how such Truist One View Service is accessed, is governed by the Referenced Terms and any conflict between Referenced Terms and this Agreement, except for such access related terms contained in this Agreement, are solely controlled by the Referenced Terms. Only the terms applicable to Truist One View Services accessed through Truist One View are applicable to the Client, and terms for Services not used by the client are not applicable, except and unless the Services are used at some later date.

a) Commercial Loan and Card Accounts. If any loan, line of credit, or credit, commercial, or purchasing card account types are included in Truist One View, the term "account" when used in reference to the Truist One View Service includes these account types and are referred to as "Lending Accounts". The Lending Accounts will be governed by their Reference Terms, including but not limited to the terms, agreements, or resolutions relating to the Lending Accounts ("Referenced Documents"). By requesting the Lending Accounts to be included in Truist One View or any access Service, the Client authorizes the Bank to provide or display information relating to such Lending Accounts within the Truist One View Service or to entitled users, and to provide any available functionality or service with respect to the Lending Accounts as may be requested or enabled by an entitled user, including, but not limited to, the ability to view Lending Accounts and transaction information, to make payments on the Lending Accounts, or to perform drawdowns or other transactions on the Lending Accounts. Client represents and warrants to the Bank that inclusion of such Lending Accounts in Truist One View or an access Service is in accordance with and does not violate any Referenced Documents relating to the Lending Accounts. Client shall indemnify and hold Bank harmless against any claim, loss, damage, cost, or expense including litigation expenses and reasonable attorney's fees resulting from a breach of the representation and warranty in this Section 7 or resulting in any way from the inclusion of the Lending Accounts in Truist One View or as an access Service.

b) Commercial Loan Dashboard. Commercial Loan Dashboard (the "CLD") allows clients to securely upload and view loan-related documents and monitor the progress of their outstanding loan requests in a status tracker. The Commercial Loan Dashboard (the "CLD"), accessible through Truist One View, allows entitled users to view and receive information related to Lending Accounts, loan requests/applications, and other financial products (collectively referred to as "Loan Products") provided by Truist to a Client, to share information with Truist in connection with Loan Products and to submit information on behalf of a Client for Loan Products. All users must be entitled by the primary administrator.

Bank shall determine in its sole discretion which functions, and Loan Products are accessible via the CLD and may remove any function or Loan Product from the CLD at any time without notice.

CLD User Entitlement; CLD Functions. The Truist One View Primary Administrator for CLD (referred to as the "CLD Administrator") has the ability to grant other users' permission to access all functions available via the CLD. The CLD Administrator and each other user granted permission to access the CLD (all of the foregoing are referred to as "CLD Users" and each a "CLD User") will be able to access, view and exchange all Loan Product information and other documents contained in the CLD, whether shared by Bank or any CLD User ("CLD Information") and engage in transactions with respect to the Loan Products as functionality is made available in the CLD. Without limiting the foregoing, CLD Users will be able to: (1) view all Loan Product information and documentation shared by Bank through the CLD; (2) upload and share financial and other information relating to Client or any other entity or individual, all of which shall be considered CLD Information; (3) access, view and share information uploaded by any other existing or future CLD User, all of which shall be considered CLD Information; (4) on behalf of Client, prepare and submit to Bank applications for certain Loan Products (including new Loan Products and modifications and/or renewals of existing Loan Products); and (5) engage in such other transactions with respect to Loan Products as may be available through the CLD from time to time. Client is responsible for: (1) ensuring that the CLD Administrator permissions only CLD Users who Client intends to have access to CLD Information that is uploaded to or accessible via the CLD and who have authority to take action on behalf of the Client; and (2) enacting such processes and procedures as Client deems necessary to instruct all CLD Users as to the information which they may upload to the CLD and any action they may take in the CLD. Client represents and warrant to Bank that all CLD Information provided by any CLD User through the CLD will be true and correct in all material respects. Bank will have no liability for disclosure of any information among CLD Users through use of the CLD and is not responsible for any content or information uploaded to or shared via the CLD.

Liability. Client agrees that:

i. Client is responsible for all actions taken by any CLD User through the CLD, each of which shall be binding on Client;

ii. Client assumes all risk for any action taken by a CLD User based upon any CLD Information to which the CLD User has access;

iii. Client assumes all risk for the possibility that any CLD Information a CLD User downloads and stores outside of the CLD may be accessed by unauthorized third parties;

iv. If a CLD User sends any information in a manner that is not secure, or if a CLD User takes any information out of Bank's secure environment by downloading it, Bank is no longer responsible for the security and confidentiality of that information, and the responsibility becomes solely Client's;

v. Bank is not responsible for the security and confidentiality of any CLD Information if a CLD User: (i) uses unsecured wireless connections to download CLD Information, in which case Client acknowledges such connection may permit other persons to access the CLD Information being downloaded; or (ii) allow other persons access to Client's software applications; and

vi. Any CLD Information that a CLD User downloads is processed at Client's own risk and Client is solely responsible for any damage that might occur to the computer (or other electronic device) to which such CLD User downloads any CLD Information, or any loss or corruption of data that might occur as a result of the downloading or storage of CLD Information in an electronic device.

Miscellaneous. Loan Product application and documentation status provided via the CLD is for informational purposes only and shall in no event constitute notice of a credit approval or decline, nor a binding agreement to extend credit. The establishment and maintenance of any loan or other financial accommodation shall be governed by Bank normal credit criteria and by separate loan documentation.

Indemnity. In addition to any other indemnity obligations Client has under this Agreement, Client agrees to indemnify, defend and hold harmless Bank, its service provider, and their respective affiliates, partners, officers, directors, employees, consultants, and agents from any and all claims, liability, losses, damages and/or costs (including, but not limited to, attorneys fees) arising from Client's use of the CLD or Bank's reliance on the information provided via the CLD.

c) Commercial Credit Card. Truist offers a Truist One View Services for a suite of Commercial Card solutions that provide features designed to better inform decisions, control purchasing, and enhance working capital. These solutions include:

- "Truist Purchasing Card" is typically used by Authorized Users for purchasing business-to-business, non-travel related goods and services related to the Organization's business needs. A Purchasing Card can be either a Physical Card or a Virtual Card.
- "Truist Corporate Card" is typically used by Authorized Users for travel and entertainment-related purchases. A Corporate Card can be either a Physical Card or a Virtual Card.
- "Truist Executive Card" is a subset of a Truist Corporate Card that is typically issued to the Organization's executives and provides enhanced insurance coverages, benefits, and features. These coverages, benefits, and features are not guaranteed and Truist, in its sole discretion, may modify or discontinue same without prior notice.
- "Truist One Card" is typically used by Authorized Users for the purchase of business-to-business goods and services as well as travel and entertainment purchases. A Truist One Card can be either a Physical Card or a Virtual Card.
- "Truist ePayables" (sometimes also referred to as "payables") are Virtual Cards used by the Organization to pay merchant(s) for business-to-business goods and services based upon, for example, an invoice from a merchant.

This Truist One View Service for these Lending Accounts are governed by the Reference Documents of the Commercial Card Terms and Conditions, the Commercial Card Client Acceptance Form, the Incentive Addendum, the Commercial Card Attestation, and any other schedules, agreements, documents, or other instruments including all riders, amendments, restatements, supplements, and addenda thereto govern the establishment and use of Commercial Cards solutions. For more information on all Commercial Card solutions, please review your Truist Commercial Card Terms and Conditions or visit Commercial & Corporate Cards | Truist.

d) Online Foreign Exchange (OFX). Truist Bank offers online currency exchange as governed by the Truist Foreign Exchange Agreement (the "FX Terms and Conditions"), where trading activity is limited to Foreign Exchange ("FX") and/or Currency Options with counterparties. The OFX Service is subject to the applicable trading agreement between Truist Bank and the counterparty and is subject to the FX Terms and Conditions as listed below, along with any other schedules, agreements, addenda, or supplements related thereto that may be provided to the counterparty, and such terms shall apply to the counterparty as set forth below.

- **Annex I (FX Trading Agreement) of the FX Terms and Conditions:** Annex I of the FX Terms and Conditions will apply unless Counterparty has executed an ISDA Master Agreement with Bank that applies to foreign exchange transactions. In such an event, the terms of the ISDA Master Agreement and Schedule entered into by Bank and Counterparty will apply to such transactions
- **Annex II (OFX System) of the FX Terms and Conditions:** Annex II will apply if Counterparty is subscribing to or in the future subscribes to or uses Bank's OFX Service.
- **Annex III (Miscellaneous) of the FX Terms and Conditions:** Annex III applies to all Counterparties to the extent described in the FX Terms and Conditions.
- **Multi-Currency Transaction Account:** The Multi-Currency Transaction Account terms will apply if Counterparty is applying for or in the future opens one or more Multi-Currency Transaction Accounts.
- **Foreign-Currency Time Deposits:** The Foreign Currency Time Deposit Account terms will apply if Counterparty is opening or in the future opens one or more Foreign Currency Time Deposits.

Truist Treasury Manager Service

1. Description of Truist Treasury Manager Service. The Truist Treasury Manager service is an online web-based information reporting and transaction initiation service. Details regarding functionality and certain technical requirements are included in the Truist Treasury Manager reference materials. Client's selection of accounts to be included in the service as well as certain options or transaction capabilities shall be reflected in a Treasury Request Confirmation. Certain options or transaction capabilities may be governed by additional service terms and conditions, and to the extent Client selects such options or capabilities for use within the service, those additional applicable terms and conditions are incorporated into these Truist Treasury Manager service terms and conditions.
2. Administrators. The two individuals designated as Truist One View Primary Administrators in the Primary Administrator Designation agreement (or other similar agreement accepted by Bank) are the Primary Administrators of the Treasury Manager service. If Client has opted out of the Truist One View administrative approval security feature, the single individual designated as the Truist One View Primary Administrator in the Primary Administrator Designation agreement (or other similar agreement accepted by Bank) is the Primary Administrator of the Treasury Manager service.
3. Security Procedures. The security procedures for the service are described below. Client agrees that use of the service constitutes acceptance of the below security procedures.
   a. Access Credentials. Valid access credentials are required to log in to the service.
   b. Dual Payment Approval. Any ACH or wire transaction initiated through the service requires dual approval, which means that one authorized user with sufficient entitlements must initiate the transaction and a different authorized user with sufficient entitlements must approve the transaction in order for the transaction to be released and processed.
   c. Administrative Approval. Administrative actions initiated through the service such as, but not limited to, specifying the type of payments a user can initiate or limiting payment amount by payment type or source account, must be approved by a second user with the appropriate permissions. Administrative approval entitlements in Treasury Manager are the same as those established for Truist One View. If Client elects to opt out of the administrative approval security procedure for Truist One View/Treasury Manager, Client must document this decision in writing and in accordance with Bank procedures. **Bank strongly recommends that Client not opt out of the administrative approval security procedure**.
   d. Wire Transactions. Any wire transactions initiated through the service require the approval of an authenticated user with appropriate entitlements in order for the transaction to be released and processed. Authentication methods and procedures may change from time to time and will always be stated in current reference materials.
4. Secure Browsing Software. A secure browsing software such as Rapport, the secure browsing software provided by Trusteer Inc. (an IBM company), may be required to be installed on any computer or other supported device used to log in to the

service. If Bank requires the secure browsing software for Client's setup of the service, a user may not be able to access the service if the user attempts to login from a device on which the secure browsing software is not installed and running. Users may be required to download the secure browsing software and accept a separate software license agreement in order to install the secure browsing software on each device which is used to access the service. Client agrees that Client's use of the secure browsing software is subject to, and Client is bound by and will comply with, the terms of the software license agreement. **BANK DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES OF ANY KIND RELATING TO THE SECURE BROWSING SOFTWARE, INCLUDING ANY REPRESENTATIONS AND WARRANTIES OF PERFORMANCE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. BANK HAS NO RESPONSIBILITY FOR (i) THE PERFORMANCE OF THE SECURE BROWSING SOFTWARE OR THE VENDOR OF THE SECURE BROWSING SOFTWARE, (ii) COMPATIBILITY OR AVAILABILITY OF THE SECURE BROWSING SOFTWARE, OR (iii) DAMAGES OF ANY KIND CLAIMED UNDER ANY CAUSE OF ACTION ALLEGED TO INVOLVE OR RELATE TO THE SECURE BROWSING SOFTWARE OR THE VENDOR OF THE SECURE BROWSING SOFTWARE.** Client is solely responsible for determining if the secure browsing software is compatible with Client's equipment, communications capabilities, and other software and for ensuring any installation of the secure browser software is in accordance with Client's policies. Client agrees any vendor of the secure browsing software is authorized to make certain information related to the device on which it is installed, including but not limited to the IP address, browser information, and operating system information, available to Bank; Bank has no obligation to provide notice of any such information to Client, including with respect to any information made available to Bank for purposes of detection of potentially fraudulent or suspicious activity. Client's confidentiality obligations under the general terms and conditions apply to any secure browsing software and any related license agreement or other related documentation.

5. Loan and Card Accounts. If any loan, line of credit, or credit, commercial, or purchasing card account types are included in Client's setup of the service, the term "account" when used in reference to the service includes these account types. By requesting the account to be included in the service, Client authorizes Bank to provide or display information relating to such loan or card accounts within the service or to entitled users, and to provide any available functionality or service with respect to those accounts as may be requested or enabled by an entitled user, including, but not limited to, the ability to view account and transaction information, to make payments on the accounts, or to perform drawdowns or other transactions on the accounts. Client represents and warrants to Bank that inclusion of such accounts in Truist Treasury Manager is in accordance with and does not violate any terms, resolutions, or agreements relating to the accounts. Client shall indemnify and hold Bank harmless against any claim, loss, damage, cost or expense including litigation expenses and reasonable attorney's fees resulting from a breach of the representation and warranty in this Section 5 or resulting in any way from the inclusion of the account in Truist Treasury Manager.

Universal Payment Identification Code Service

1. Description of Universal Payment Identification Code Service. The Universal Payment Identification Code ("UPIC") service generates a unique number assigned to one of Client's Truist demand deposit accounts, which Client can then provide to Client's trading partners who make payments to Client through the Automated Clearing House (ACH) network. Client's use of the UPIC service allows Client to mask Client's banking relationship and account number to reduce the risk of fraudulent use of Client's account information. Details regarding UPIC's functionality, formatting, and other technical requirements that Client must follow when using the UPIC service are provided in the UPIC reference materials.

2. Roles under the UPIC Service. Bank will assign a separate UPIC number to each eligible account Client identifies. Under the UPIC Service, Bank acts as the receiving depository financial institution with respect to UPIC ACH entries that are sent to Bank for receipt into one of Client's accounts. As a receiver of the ACH entries, Client acknowledges that the entries shall be processed according to the Nacha Operating Rules and Guidelines governing the ACH network.

3. Eligible Accounts. The UPIC service may only be used for a demand deposit account or other transaction account of a corporation, partnership, limited liability company, or unincorporated association; the government of the United States or an agency of the United States; a state or local government or an agency of a state or local government; or one or more non-consumer accounts of individuals (such as sole proprietors) when the account is used primarily for business purposes. An account of one or more individuals used primarily for personal or household purposes, i.e., a consumer account, may not be used with the UPIC service.

4. Use of UPIC Number. The UPIC number is only to be used for incoming ACH credit entries. Client may provide the UPIC number and the related universal routing number to Client's business trading partners that will originate ACH credit entries to Client's designated accounts. Client represents that Client will not authorize any person or entity to originate any debit entries using the assigned UPIC number.

Wholesale Lockbox and Retail Lockbox Services

1. Description of Wholesale Lockbox and Retail Lockbox Services. Bank's Wholesale Lockbox and Retail Lockbox services are designed to facilitate the receipt and processing of Client's accounts receivable remittances. These terms and conditions apply to both Wholesale Lockbox and Retail Lockbox services unless otherwise stated. Note that certain features described in these terms and conditions are not available at all lockbox processing locations. Details regarding functionality and formatting and other technical requirements Client must follow when using a Lockbox service are provided in the reference materials for the applicable Lockbox service.

    a. Wholesale Lockbox Service.

        i. Wholesale Lockbox Service. Wholesale Lockbox service is designed to process large dollar payments along with related invoices, correspondence, or other document images.

        ii. Healthcare Processing. Client must disclose if they are a covered entity as defined by HIPAA regulations; certain processing standards may apply. Any paper returned to Client must be sent via a trackable mail delivery method.

        iii. Wholesale Lockbox Lite Service. Wholesale Lockbox Lite service is a form of Wholesale Lockbox service that is limited to a total of 500 items (as defined in applicable reference materials) per month in any combination of checks and remittance document images. If Client subscribes to this service and Client exceeds 500 items in any month, each item over 500 will be assessed an overage fee. The following limitations apply to Wholesale Lockbox Lite service: image services options include only check and document imaging, full text searching, and a seven-year archival period; Virtual CD ROM, Image Transmission file, Batch Download, Credit Card Authorization and Remitter Table are not included; signature and date Services shall not be available; remittance material services shall only include the mailing of rejected items back to Client. Other features of Wholesale Lockbox service may not be available under the Wholesale Lockbox Lite service.

    b. Retail Lockbox Service. Retail Lockbox service is designed to process a high volume of low-dollar payments with machine-readable remittance coupons. Retail Lockbox service may also be referred to as Scannable Lockbox service.

2. Implementation of Lockbox Service. Bank will implement the applicable Lockbox service for the accounts designated by Client, per lockbox operating instructions as agreed to between Bank and Client.

3. Transfer of Lockbox Materials. If Client designates a courier service or other agent to pick up copies of items, remittance materials, or any other property, from any lockbox site, then Client agrees that transfer of possession of such materials to Client's agent constitutes delivery to Client, and Client assumes any and all risks incidental to or arising out of such transfer to Client's agent. Client also agrees that any courier of Client shall be considered Client's agent and Bank shall have no liability once Bank delivers any items into the possession of that courier. In the event Bank mails any lockbox materials to an address designated by Client, Client agrees that Bank has no responsibility for such materials after Bank mails them.

4. Image Services. Image services options enable Client to view images of checks and remittance payment information that are received through Client's lockbox. Client can access these images and transaction information through Image Browser, Virtual CD, and/or Image Transmission file, as described below. Client must designate a Primary Administrator for the image service options. This individual will also act as the Primary Administrator for Online Decisioning/Web Exceptions (described below), if Client elects to use that feature.

    a. Image Browser. Image Browser provides internet-based access to Client's lockbox images and data with flexible viewing parameters and search capability for check and document information; Batch Download, Full Text Search, and Remitter Table capabilities are also available as additional service selections.

    b. Virtual CD. Virtual CD is downloaded from Image Browser to support Client's need for a long-term archive. Lockbox images of checks and documents can also be downloaded onto Client's computer from Virtual CD. Virtual CD file availability aligns with Client's image archive storage period.

    c. Image Transmission File. Image Transmission File provides customized access to Client's lockbox images along with index fields of information that can be downloaded directly into Client's accounts receivable systems. Image Transmission files are delivered to Client per specifications established during implementation.

    d. Rear image capture. Each lockbox may be configured to capture rear images (duplex capture) of payment and non-payment items. If this feature is configured, rear images will be stored whether images contain pixel data or are blank. Optionally, clients may utilize the service that will remove rear images of blank items from online availability, in which

case these items will still be stored offline, not accessible for retrieval from the image browser, and included in volume counts for this service.

5. Processing of Deposits. Bank will establish one or more post office boxes or "lockboxes" in Client's name as specified during implementation of the service. In the event Client owns a USPS PO Box and chooses to use it for Client's lockbox payment processing, Client is responsible for communicating all mail direction or other PO Box changes to the USPS. On each banking day after a lockbox has been established, Bank will process the checks, drafts and money orders (all of which are referred to as "items") received in a lockbox in accordance with the instructions in effect at the relevant time and Bank will communicate deposit totals and advices as agreed upon with Client.

   a. Processing of Wholesale Lockbox Items. An item containing a payee name that does not reasonably correspond to an acceptable payee list Client has given Bank will be handled in accordance with Client's lockbox instructions. Bank will not inspect an item for the drawer's signature or the date. Unless otherwise stated in Client's agreed-upon lockbox instructions, Bank will also not inspect any item and/or accompanying correspondence in an effort to identify "payment in full" or other similar payment dispute language or any language that states that acceptance or deposit of the item binds the payee or depositor to any agreement or terms. Bank will not be liable for any loss resulting from processing any such items, including any items Bank may inspect in an effort to identify such language. As part of processing an item, Bank will also enter data regarding certain aspects of an item per the lockbox instructions (such as the drawer's name and the account invoice number shown on the item) into the data file Client will receive. Client agrees that Bank will not be liable for errors entering any of that data.

   b. Processing of Retail Lockbox Items.

      i. Automated Processing System. Bank processes items through the use of automated systems. Client's remittance documents must be approved by Bank for use with Client's lockbox, include details and identifiers that are required by Bank to identify and validate items for automated processing. Bank will test the performance of Client's coupons and will begin providing the lockbox service to Client only upon the satisfactory completion of the test. If the form, layout or font on these documents changes it is important that Lockbox systems that read these items for processing are updated to reduce the potential for systemic read errors. Client must notify Bank of such changes before documents are received for Lockbox processing. Items that fail to read will be returned to Client for subsequent handling and/or redeposit.

      ii. Items with Coupons. Bank will automatically deposit items, regardless of payee name, into the relevant account when the items are accompanied by coupons that match Client's assigned P.O. Box number. Bank will not inspect these items, including any inspection for payee name, drawer signature, date, or for items and/or accompanying correspondence containing "payment in full" or other similar payment dispute language. Bank will not be liable for processing or depositing items without inspecting them.

      iii. Items Without Coupons. Items that are not accompanied by coupons will be returned to Client or processed manually as directed in the instructions agreed upon with Client. Bank will not inspect any item for the drawer's signature or the date. Bank will also not inspect any item and/or accompanying correspondence to attempt to locate "payment in full" or other similar payment dispute language, or any language that states that acceptance or deposit of the item binds the payee or depositor to any agreement or terms. Bank will not be liable for any loss resulting from processing any such items. As part of processing an item, Bank will also enter data regarding certain aspects of an item per the lockbox instructions (such as the drawer's name and the account invoice number shown on the item) into the data file Client will receive. Client agrees that Bank will not be liable for errors in entering any of that data.

      iv. Stop File. In accordance with Bank's instructions, Client may give Bank a file of items that Client does not want Bank to process. Provided Bank receives the stop file in a reasonable period of time before the items in question are received in a lockbox, Bank will use good faith efforts to attempt to stop the processing of items in Client's file and return them to Client, but Bank will not have any liability if Bank processes any such item.

      v. Data Files. On each banking day Bank will make a data file regarding the items processed in each lockbox that day available to Client through one of Bank's online services. Client should download these files regularly. Application files will not be retained for longer than 10 business days.

   c. Endorsement. Bank will endorse items for deposit with Bank's standard lockbox endorsement and deposit items to the relevant account. Bank will not be liable for any loss relating to Bank's failure to endorse an item properly.

   d. Forwarding and Returning Items. If Client receives an item that should have been delivered to a lockbox, Client may forward it to Bank's lockbox department. Bank will process all such items (whether accompanied by a coupon or not) automatically and without inspecting them. If Client receives an item or image of an item from Bank and Client or Bank

discovers that such information was mis-delivered to Client, Client must immediately notify Bank immediately and delete and/or return all such information to Bank. In addition to any other rights available to Bank, Bank may immediately terminate the Lockbox service if Client fails to comply with this provision.

e. Cash and Other Property. Bank will deposit any cash received in a lockbox into the relevant account; Bank's count of the cash will be considered final. Any property other than items, cash and related remittance materials received in a lockbox will be sent to Client, and applicable fees charged to Client. Client agrees that Bank shall have no liability for any cash or other property received in a lockbox.

f. Return Items. Unless otherwise stated in the instructions, Bank will handle dishonored or returned items in accordance with the terms of the Commercial Bank Services Agreement (CBSA).

6. Remittance Materials. Bank will destroy the original remittance materials (such as invoices, payment coupons, correspondence and the like) within a period of time (as determined by Bank) after receipt by Bank. Bank will only return original remittance materials received in a lockbox to Client if Client's lockbox instructions direct Bank to return those materials. Client agrees that Bank is not liable for loss, theft, or damage to such materials after they leave Bank's possession, if they are mailed to Client's address indicated in Bank's records or delivered to Client's agent or a courier. Once Bank destroys the original remittance materials, the images of that Bank may capture during processing will be the only source of information about their contents and although Bank may retain images for a certain period of time to comply with internal document retention requirements, Client will only have access to such images if Client selects one of Bank's image services. Client agrees that Bank will have no liability for any missing image, or if any image Bank captures is not legible, or if Client fails to subscribe to one of Bank's image services and thus does not have access to image items and materials received into Client's lockbox.

7. Affiliate Deposits. If Client has not given Bank an acceptable payee list, Client represents and warrants to Bank that Client has the authority to endorse and deposit each item received in Client's lockbox into Client's account(s), even if the payee name on an item is not Client's name as shown in Bank's records. In addition, if Client has given Bank an acceptable payee list, Client represents and warrants to Bank that if any name on that list is a separate legal entity (rather than merely a "d/b/a" or trade name that Client uses), that Client has authority from that entity to have items payable to the entity endorsed and deposited into Client's account(s). Client agrees to provide Bank with satisfactory evidence of such authority upon request.

8. Termination. If a Lockbox service is terminated for any reason, then Bank will complete the processing of items Bank received prior to the termination date. Upon request, Bank will forward mail for up to 90 days. After that time, Client may elect to extend the forwarding period in additional 90-day increments (additional fees will apply to this service) or Bank will return mail to the sender. The lockbox billing account must remain open and active during the mail forwarding period as account maintenance fees and annual P.O. box renewal fees will continue to apply. If Client implements image archival services as part of Client's Image Browser service and Client's Image Browser service is later terminated, it is incumbent on entitled users to download historical information from the system that is needed as browser access is immediately revoked upon box closure and no image retrieval is possible. Image of individual payment items may be requested through research request; additional fees will apply.

9. Online Decisioning/Web Exceptions. Online Decisioning (available for Wholesale Lockbox service) and Web Exceptions (available for Retail Lockbox service) are optional features of Lockbox services. Online Decisioning/Web Exceptions is a decisioning and data entry tool that allows Client to make processing decisions for lockbox exception items, and to input remittance data online. Client's lockbox exception items will be presented to Client, identifying the first reason code that caused the item to reject. Client may then use Online Decisioning/Web Exceptions to have each item forwarded to Client, or have each item processed by Bank for deposit. If Client fails to decision any item by Client's daily processing deadline, it will be rejected unless Bank, in Bank's sole discretion, has offered to allow Client to elect to holdover items not processed by daily cut-off time. If the holdover feature is utilized, Client will hold Bank harmless for any delay in processing applicable negotiable instruments and any associated remittance. The holdover feature may not be offered to all Clients.

10. Payment Card Transaction Handling. At Client's option, Bank will process payment card remittances sent to Client's lockbox. If Client selects this option, Client appoints Bank as Client's agent for purposes of processing payment card transactions and submitting transactions to Client's merchant processor for authorization, and Client agrees to provide Bank with all information required to access the merchant processor's authorization system. Client will hold Bank harmless from any and all claims asserted by Client's merchant processor that arise from an allegation that (i) Client does not have the authority to appoint Bank as Client's agent, or (ii) Client does not have the authority to grant Bank access to Client's merchant processor's system. Client will be solely responsible for notifying Client's merchant processor that Client has appointed Bank as Client's agent. Alternatively, as available in some processing locations, Client may request that Bank image Client's credit card payments but not authorize the transactions; Bank will use reasonable efforts to attempt to redact the CVV or CVC

information on the remitted documents prior to imaging but shall have no liability to Client if Bank fails to redact any such information.

11. Handling of CD Rom(s) and DVD(s). If Client receives or has received Image CD ROM(s) or Image DVD(s) (regularly or as a one-time delivery of historical lockbox materials), Client should download data from that medium to Client's own long-term storage/retention system, within 30 days of issuance, to meet Client's retention requirements. Client should not rely on the CD ROM or DVD for long-term retention of the data, as viewing software may become unavailable or obsolete and the associated encryption key(s) unable to be retrieved or reproduced.

Wire Service

Wire Service. Wires transfers initiated through one of the treasury management services governed by this Agreement are subject to the Truist Wire Agreement, in addition to the terms and conditions for the treasury management service used to initiate the wire transfer. The Truist Wire Agreement is included below and is also available at Truist Wire Agreement. In the event of any conflict between the version of the Truist Wire Agreement included below, and the Truist Wire Agreement posted online, the version of the Truist Wire Agreement posted online will control.

Truist Wire Agreement

This Truist Wire Agreement is made by and between Truist Bank ("Bank") and Client (as defined below). This Agreement shall govern all funds transfers initiated via the following methods or services, according to the terms herein: Corporate Call, Retail PIN, Drawdown Wire, Standing Order Wire, and wires initiated through any of Bank's treasury management services governed by this Agreement. Each of these methods or services is referred to herein as a "Wire Service", and any documentation relating to a Wire Service (including but not limited to another service agreement, implementation form, or other document providing service and account elections and details relating to wire transfers to be initiated via the Wire Service) is referred to herein as a "Wire Document". Client agrees to the terms of this Agreement by executing a Wire Document and/or requesting a Wire Service that is subject to the terms of this Agreement. Any wire initiated through a Wire Service shall be subject to the terms of this Agreement as well as the terms of the applicable Wire Document. The terms of Bank's Bank Services Agreement ("BSA") or Commercial Bank Services agreement ("CBSA"), as applicable to the Account used for wire initiation, are incorporated into this Agreement by reference, and shall apply to each wire initiated through a Wire Service and any claims or disputes that arise out of this Agreement, including but not limited to BSA or CBSA provisions regarding the mutual arbitration agreement, jury trial and litigation class action waiver, duty of care, costs, expenses, fees, applicable law, and jurisdiction. In the event of a conflict between the CBSA or BSA and this Agreement, the terms of this Agreement shall control.

1. Definitions. The following are defined terms:

   a. "Account" means the account(s) designated by Client on a Wire Document(s) to be used as the source of payment for Payment Orders.

   b. "Authorized Sender" means a person designated by Client on a Wire Document, and any user entitled by an administrator or otherwise within the Wire Service, who is authorized to initiate, submit and/or verify Payment Orders and Instructions to Bank. The term Authorized Sender when used herein includes "Authorized Representatives" designated on a Corporate Call or Retail PIN Wire Service Details and Authorized Representatives agreement.

   c. "Confirmation" means any notice (oral, written, electronic, or otherwise) informing Client of the date and amount of each Transfer to or from an Account.

   d. "Client" means the individual or entity that has executed a Wire Document and will use one or more or Wire Services for wire initiation that is governed by this Agreement.

   e. "Instructions" means the Transfer related directions given by an Authorized Sender to Bank, including amendments or cancellations of Payment Orders. Instructions will be provided pursuant to the terms of the applicable Wire Document.

   f. "Payment Order" means a request (oral, written, or electronic) from an Authorized Sender directing Bank to initiate a Transfer from an Account.

   g. "International Payment Order" means a Payment Order in which the beneficiary's bank is located outside of the United States.

   h. "Repetitive Transfers" mean Transfers initiated by Payment Orders in which the debit and beneficiary information, designated by Client on its Corporate Call Repetitive agreement or Retail PIN Repetitive agreement, remains constant, but the date and dollar amount vary; Transfers are initiated using a Repetitive Code.

i. "Standing Order Transfers" mean Transfers made as ordered by Client on a Standing Order Wire agreement, in which the debit and beneficiary information remain constant, and the frequency and amount of the Transfer are according to the instructions on the Standing Order Wire agreement.

j. "Drawdown Wires" mean Transfers made as ordered and agreed to by Client on a Drawdown Wire agreement, authorizing another institution to transfer funds from Client's account at the Bank.

k. "Statement" means Client's periodic Account statement.

l. "Transfer" means a transfer of funds by Fedwire, SWIFT, CHIPS, telex, computer terminal, electronic, or other means, but excluding transfers made through the ACH network or Real-Time Payments network.

2. Authorized Sender. Authorized Senders may provide Payment Orders and Instructions to Bank.

3. Client Signature. A Wire Document may be signed manually or electronically according to Bank's instructions. A duplicate or copy of any manually or electronically signed Wire Document delivered to Bank through facsimile or email attachment shall be as effective and enforceable as an original manually signed agreement. A digital, electronic or photostatic image of any such signed Wire Document maintained in Bank's record retention system shall be as effective and enforceable as an original manually signed agreement. Client consents to the use of electronic records and signatures with respect to Client's use of any Wire Service.

4. Form of Instructions. Bank may act upon Payment Orders or Instructions. Any Payment Order or Instruction which does not comply with Bank's procedures, or which exceeds the available balance of the funds on deposit in an Account may be canceled from Bank's wire system without notice to Client or liability to Bank.

   a. Special Instructions. Client may elect to authorize Repetitive Transfers for Retail PIN Wire Service by executing a Retail PIN Repetitive agreement, or for Corporate Call Wire Service by executing a Corporate Call Repetitive agreement. Bank's assignment of a Repetitive Code for Repetitive Transfers is not a security procedure as such term is used herein. Client may also elect to authorize a Standing Order Transfer by executing a Standing Order Wire agreement. Client may make arrangement with another financial institution to debit an Account by means of a drawdown instruction by executing a Drawdown Wire agreement. Bank shall be under no obligation to comply with any drawdown request or make any transfer which would exceed the balance of available fund on the deposit in the Account. Client agrees that any drawdown request must be received by Bank prior to Bank's established cut-off time; drawdown requests received after that time may be refused.

   b. Electronic Instructions. If Bank accepts Client's election to initiate Payment Orders and Instructions from Client's electronic access system, Client shall be responsible for the security and confidentiality of Client's system and for the accuracy and completeness of any data received by Bank.

5. Processing Transfers. Bank may select any means for the transmission of funds which it considers suitable, including but not limited to Bank's own internal systems. Bank may use any of its domestic or foreign correspondent banks to facilitate or effect payment. Bank may also substitute or insert a routing number of an intermediary or beneficiary bank provided by Client in a Payment Order, if such substitution is necessary for the means of transmission used, provided that the substituted or inserted routing number identifies the same intermediary or beneficiary bank included in the Payment Order.

   Bank may, in its sole discretion, verify or authenticate any Payment Order or Instruction by contacting Client by telephone or by any other means deemed reasonable by Bank, but Bank is under no obligation to do so. If Bank is unable to verify or authenticate a Payment Order or Instruction, it is within the Bank's sole discretion to either effect or refuse such Payment Order or Instruction.

   Bank may cancel the Transfer without notice or liability to Client if (i) the request does not comply with Bank's procedures, (ii) Bank reasonably believes the transfer is prohibited by applicable law, (iii) the Transfer exceeds the available balance of funds in the Account, (iv) Bank attempts to verify a Payment Order and is unable to do so, or (v) as otherwise provided in this Agreement.

6. Funding Obligations. Client is responsible for ensuring that there are sufficient collected and available funds in the Account to satisfy all Payment Orders and other debits which may be presented on a given day. Bank may handle Client's Payment Orders with other debits for the day in any order chosen by Bank, in Bank's sole discretion. If funds are insufficient to cover all debits, this may result in rejection or cancellation of the Payment Order, delay in execution until sufficient funds are available, or the creation or increase of an overdraft in the Account.

7. Confirmations and Duty to Report Errors. The date and amount of each Transfer are described on the applicable Statement. Bank may also deliver Confirmations to Client in writing, electronically, or by a report produced by one of Bank's information reporting services, and/or as otherwise described in the applicable Wire Document. Bank will not deliver next day notice of

receipt of incoming Transfers. Client shall examine upon receipt, but in no event later than 30 days after receipt, any Statement or Confirmation (whichever first occurs) and notify Bank of errors or discrepancies in connection with a Transfer shown on the Statement or Confirmation. Failure to notify Bank of any error within such 30-day time period shall relieve Bank of all liability for the any unauthorized or erroneous Transfers reflected in such Statement or Confirmation.

8. Corporate Call and Retail PIN Wire Services. Corporate Call and Retail PIN Wire Services are funds transfer services that are available through the use of a phone to an interactive voice response (IVR) solution. Corporate Call is offered to business Accounts, and Retail PIN is offered to consumer Accounts. The terms of the applicable Wire Document(s) for Corporate Call or Retail PIN govern the use of the service in addition to the terms of this Agreement.

9. Amendment or Cancellation of Payment Orders. Any Instruction canceling or amending a Payment Order is not effective unless Bank has received such Instruction at a time and in a manner affording Bank a reasonable opportunity to act before processing the Transfer. Client may not be able to cancel or amend a Transfer after it is processed by Bank. However, Bank may, at its discretion, use reasonable efforts to act on an Instruction for cancellation or amendment. If Client requests that Bank attempt to recover a Transfer, Client may be required to deposit funds with Bank or provide other payment assurances that are satisfactory to Bank to cover the cost, expense, charges, and/or attorneys' fees incurred by Bank in its recovery attempt, and Client agrees to indemnify and hold Bank harmless from any and all liabilities, costs and expenses Bank may incur in attempting to recall or amend a processed Transfer. Bank's attempt to recover funds shall not be an acceptance of responsibility for the completed Transfer. Bank does not guarantee the recovery of all or any part of a Transfer, and any expenses of Bank or its correspondent bank relating to the recall or return of funds shall be deducted from the amount of the returned funds. In the event Bank receives the return of funds in a currency other than U.S. Dollars, the funds will be converted by Bank into U.S. Dollars at Bank's current buying rate for that currency on the date of return. Bank shall not be liable for any resulting exchange losses.

10. Deadlines. Bank maintains deadlines for the receipt of Payment Orders and Instructions, including cancellations and amendments, and such deadlines are subject to change at the sole discretion of Bank. Payment Orders and Instructions received after the deadline shall be treated as received on the next banking day. Bank may, in its sole discretion, execute Payment Orders received after the deadline on that same banking day only as an accommodation to Client.

11. Security Procedures. The security procedures Bank offers to Client are designed to control access to the Wire Services and verify the authenticity of instructions provided to Bank. The security procedures are not designed to detect errors in the content of Payment Orders or Instructions transmitted to Bank, including but not limited to intended account numbers of Client, account numbers not belonging to the name of recipient, and erroneous or fraudulent instructions provided to Client by another party. The security procedures for Wire Services are described below. Client agrees that use of the applicable Wire Service constitutes acceptance of the below security procedures and agrees that the security procedures are commercially reasonable for Client's use of the Wire Service, including the size, type and frequency of any possible Transfers that may be initiated from an Account that is associated with the Wire Service now or in the future. Client agrees to be bound by, and Bank is authorized to rely and act upon, all Payment Orders accepted by Bank in good faith and in compliance with the applicable security procedures, whether or not Client (or a user, administrator, or Authorized Sender of Client) actually gave Bank those instructions. Client agrees to comply with additional security procedures that may be implemented by Bank for a particular Wire Service from time to time.

    Client is responsible for controlling access to and maintaining the confidentiality of the details related to the security procedures and Client must immediately report to Bank as soon as Client becomes aware of any (i) suspected breach of that confidentiality, (ii) compromise of any security procedure, or (iii) need to revoke any access credentials or authorization codes. Client's failure to control access to and maintain confidentiality of the security procedures, or failure to notify Bank as required herein, may result in improper use of the security procedures to initiate or access a Wire Service or initiate Transfers. Subject to applicable law, Client shall be responsible for any transaction or losses relating to access to a Wire Service resulting from such improper use of security procedures, provided Bank has complied with its obligations herein, and Client agrees that Bank shall have no liability for any loss, claim or damage Client sustains as a result of the improper use of the security procedures.

    a. Security Procedures for Transfers initiated via a Treasury Management Service. For Transfers initiated via a treasury management service governed by this Agreement, the security procedures applicable to logging on to/accessing the service (such as valid access credentials and/or authorization codes or tokens), as well as security procedures applicable to wire transactions within the service (such as dual approval and/or authorization codes or tokens required to release a transaction for processing) apply to Transfers initiated via that treasury management service.

    b. Security Procedures Applicable to Corporate Call and Retail PIN. Transfers initiated via Corporate Call or Retail PIN Client require the following verification elements items (i), (ii), (iii) and if required by Bank in Bank's discretion or by Client per elections made within the applicable Wire Document, item (iv).

i. Profile ID – 6-digit numerical ID emailed to Client's Authorized Representatives by Bank,

ii. Personal Identification Number (PIN) - assigned by Bank's system to Client (temporary PIN will be sent via U.S. Mail to each Authorized Representative; the PIN must be activated and changed to a confidential PIN within 90 days after receipt),

iii. Dynamic Passcode via Email or Mobile Phone – one-time verification passcodes, and

iv. Wire Verification via Telephone Call Back – by Client to Bank may be required.

If the Dynamic Passcode delivery method selected is mobile phone, applicable to US dialing only, then one SMS message containing a dynamic passcode is sent per Payment Order. Client may call 800-774-8179 for additional information or help with the mobile phone Dynamic Passcode delivery option, including to obtain instructions to stop enrollment in SMS messages.

12. Recording. Client consents to Bank recording telephone calls, including, without limitation, Payment Orders and Instructions. Client assumes the responsibility for obtaining the consent of the Authorized Senders for these recordings. The recordings made shall be conclusive confirmation of Payment Orders and Instructions. Client acknowledges that not all calls will be recorded.

13. International Transfers. If the amount transferred is of a currency other than that of the country to which it is transferred, it shall be payable to the payee (beneficiary) in the currency of the specified country at the then buying rate, unless the payee arranges otherwise with the paying bank and/or deposit bank and pays all its charges in connection therewith.

a. For International Transfers (Remittance Transfers) From a Consumer Account. Bank may in its discretion decline to comply with Client's request to use a particular intermediary or pay through bank and may substitute a correspondent bank of Bank's choosing. Client may cancel a transfer for a full refund within 30 minutes of payment for the Transfer, provided that the Instruction to cancel enables Bank to identify the sender's name and address or telephone number and the particular transfer to be canceled, and the transferred funds have not been picked up by the recipient or deposited into an account of the recipient. Other than this thirty-minute right of cancellation, Client may not be able to recall or amend a Transfer after it is processed by Bank and other applicable provisions of this Section shall apply. If Client believes there is an error with respect to the Transfer, Client must notify Bank (by calling 844-4TRUIST / 844-487-8478) within 180 days of the Availability Date set forth on the receipt provided to Client. Failure to notify Bank within the 180-day time period shall relieve Bank of all liability for the Transfer. Client can also contact Bank for a written explanation of Client's rights.

b. For International Transfers from a Non-Consumer Account. Bank or any correspondent or intermediary bank reserves the right to convert the amount of any Transfer to a local (generally beneficiary's country) currency prior to executing the Transfer. In the event Client designates an Intermediary Bank in Client's Payment Order, Bank will first send the Transfer to Bank's correspondent bank, and such correspondent bank will then route the Transfer to Client's designated Intermediary Bank. Bank may not offer foreign currency Payment Orders in a particular foreign currency, at Bank's discretion.

c. Foreign Currency Conversion Opt Out. If an Opt Out election is not made for an Account per an applicable Wire Document, Bank reserves the right, at its option to convert or instruct Bank's correspondent (a bank with which Truist has a relationship for the purpose of sending international wires) to convert any U.S. Dollar- denominated international Payment Order from the Account to the currency of the country in which the beneficiary's bank is located. If the Opt Out election is made for an Account, international Transfers initiated from the Account will be sent by Bank in the currency specified in Client's Payment Order (but note that funds may be converted to another currency by a subsequent intermediary bank or the beneficiary bank). If Client does not specify a currency for international Payment Orders, the Transfer will be processed in U.S. Dollars. If an Opt Out election is made for an Account, this election will apply to all Transfers from such Account, by any initiation method or channel. If Client desires to ensure that Bank executes an International Payment Order in a currency other than U.S. Dollars, then Client should denominate that International Payment Order in the desired currency.

d. Payment Protection - Bene-deduct (debit) Exemption. It is customary for correspondent banks (banks with which Truist has a relationship for the purpose of sending international Transfers) and/or additional intermediary banks which facilitate the delivery of Transfers to the beneficiary's bank to assess and deduct charges from the principal amount of the Transfer. If Client selects the Exemption for an Account per an applicable Wire Document, Transfers from the Account will be exempt from the deduction of charges by Bank's. However, note that an intermediary bank or the beneficiary's bank may still take a deduction from the payment to the beneficiary, so the Exemption selected for an Account may not prevent all deductions from the payment to the beneficiary. If the Exemption is selected for an Account, it will apply to all Transfers from such Account, by any initiation method or channel.

e. Conversion Cap. For foreign currency international Payment Orders that exceed an amount (the "Conversion Cap") set by Bank, Client must obtain a Contract ID before the Transfer can be processed. Contract IDs are offered at Bank's discretion and may not be available for all foreign currency Payment Orders. Client can obtain a Contract ID or request the current Conversion Cap amount by contacting Bank at the following numbers:

   i. For Retail PIN Wire Service: 844-4TRUIST / 844-487-8478

   ii. For all other Wire Services: 800-774-8179

14. Name and Account Number Inconsistency; Erroneous Instructions. Client acknowledges and agrees that Client is solely responsible for the accuracy of Payment Orders provided to Bank. If a Payment Order inconsistently describes the beneficiary, beneficiary's bank, or intermediary bank by name and number, payment might be made by the intermediary or beneficiary's bank on the basis of the number even if the number identifies a person or bank other than the named beneficiary or bank. Client shall be responsible for any loss associated with such inconsistency and agrees that its obligation to pay the amount of the Transfer to Bank is not excused in such circumstances.

15. Liability.

    a. Duty of Reasonable Care. Bank shall exercise good faith and reasonable care in performing the Wire Services. Client shall exercise good faith and reasonable care in observing and maintaining security procedures, in communicating Payment Orders and Instructions to Bank and in reviewing Statements and Confirmations for errors. Client is responsible for ensuring the accuracy of all information contained in a Payment Order, and Bank has no duty whatsoever to verify the accuracy of any Payment Order, nor will Bank be liable for losses or damages arising out of Payment Orders containing inaccurate or incorrect information.

    b. Limitation of Liability**.** Bank's liability for a Transfer shall be limited to errors or delays in the Transfer per applicable law and Bank shall not be liable in any case for any special, indirect, exemplary, or consequential damages (including lost profits) of any kind. Bank is not responsible for performance failure as a result of an interruption in transfer facilities, labor disputes, power failures, equipment malfunctions, suspension of payment by another bank, errors by another bank, refusal or delay by another bank to accept the Transfer, acts of war or terrorism, regulatory or emergency conditions, fire, earthquake, or other circumstances outside of Bank's control.

    Client will hold Bank harmless (a) if Bank acts in accordance with Payment Orders and Instructions, including, but not limited to, amendments or cancellations; (b) if Bank attempts to recover funds upon Client's request; (c) for any loss resulting from the unauthorized access to or use of applicable security procedures; or (d) for any matters referenced in this Agreement for which Client has responsibility.

    Except as otherwise required by applicable law, any damages or other compensation due Client resulting from Bank's negligence shall be limited to interest on the funds at issue at the federal funds rate paid by Bank at the close of business on each day the error or delay remains uncorrected; provided, however, if Bank is unable to recover the funds from the transferee who has no claim to all or any portion of the funds erroneously transferred as a result of the Bank's negligence, Bank shall be liable for Client's actual loss, not to exceed the amount of funds which Bank is unable to recover, plus interest at the rate described above.

16. Fees. Client shall pay all fees and charges which Bank may, from time to time, impose for the performance of Wire Services subject to this Agreement. In addition, Client shall reimburse Bank for all out-of-pocket expenses incurred by Bank in effecting Payment Orders and Instructions, including cancellations, amendments and attempted recoveries, and Client shall be responsible for payment of all fees and charges of each correspondent or intermediary bank which facilitates a Transfer or payment. It is customary that such fees and charges are assessed and withheld from the amount of the Transfer or if assessed to Bank, passed on to Client. Client hereby authorizes Bank to instruct any correspondent or intermediary bank to obtain payment of its charges by withholding such charges from the amount of the Transfer.

17. Notices. For Wire Services subject to this Agreement, notices shall be provided pursuant to the notice provisions in this Agreement. For Standing Order Wire, Drawdown Wire, Corporate Call, and Retail PIN, notices shall be provided pursuant to the notice provisions in the BSA or CBSA, as applicable.

18. Amendment and Termination. This Agreement may be amended by Bank from time to time by prior written notice to Client. Any use of Wire Services subject to this Agreement Client's receipt of the notice shall constitute acceptance of the terms of the amendment. Either party may terminate this Agreement by giving 30 days prior written notice to the other party. Bank may terminate this Agreement immediately, without prior notice to Client, if (a) the Account(s) has no annual activity or has been closed; or (b) in the good faith opinion of Bank, Client is involved in potentially illegal or unethical business practices or is financially unstable, or the prospect of Client's payment or performance has been impaired.

19. Miscellaneous**.** This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, successors, and assigns, by merger or otherwise. If any provision of this Agreement shall be declared invalid or unenforceable, said provision shall be ineffective to the extent it is invalid, without in any way affecting the remaining provisions of this Agreement. In addition to the applicable law provisions of the BSA or CBSA, the rights, duties and liabilities of Bank and Client shall be subject to, and Client agrees to comply with, as applicable, federal laws, Federal Reserve Bank operating circulars, Federal Reserve Board regulations, Consumer Financial Protection Board regulations, regulations and requirements of the Clearing House Interbank Payments System (CHIPS) and/or the Society for World Interbank Financial Telecommunication (SWIFT).

Zelle® Disbursements

1. **Service Description.** Zelle® Disbursements is a service of Early Warning Services, LLC ("EWS"), a digital payments network and company. Zelle and related marks are wholly owned by EWS and are used herein by permission. This Service allows you to send payment instructions to Bank for submission to Zelle for payments to a consumer or small business recipient. For each payment, the payee must be enrolled in Zelle (enrolled payees are referred to as "Users") and you must provide the alias registered by the User, such as an email address or mobile phone number. EWS does not provide deposit account or other financial services. Zelle neither transfers nor moves money. Client may not establish a financial account with Zelle of any kind. All money will be transmitted by Truist and/or another financial institution that has partnered with EWS (each, a "Network Financial Institution").

2. **Service Functionality.** Details regarding Zelle Disbursements functionality and technical requirements that Client must follow when using the service are provided in the applicable reference materials. You understand that use of this Service by you will at all times be subject to (i) this Agreement, and (ii) your express authorization at the time of the transaction for us to initiate a debit entry to your deposit account. We or Zelle are entitled to impose transaction limits on your payments. If this occurs, transaction limits will be disclosed in the applicable reference materials. You understand that when you send the payment, you will have no ability to stop, cancel, or reverse the payment. The payment is sent directly to the User's bank account (except as otherwise provided below) and may not be canceled or revoked. We therefore recommend that you use the Service to send money only to people you know and trust. In most cases, the transfer will occur in minutes; however, there are circumstances when the payment may take longer. For example, in order to protect you, us, Zelle, the other Network Financial Institutions, and Users, we, Zelle, or the receiving Network Financial Institution may need additional time to verify the identity of the person receiving the money. The money may also be delayed or the transfer may be blocked to prevent fraud or to comply with regulatory requirements. If we or Zelle delay or block a payment that you have initiated, we will notify you. Neither we nor Zelle have control over the actions of other Network Financial Institutions that could delay or prevent your money from being delivered to the intended User (for example, the receiving Network Financial Institution may decline to apply a payment if they find a mismatch between the User's Zelle profile and the Network Financial Institution's account records) .

3. **Content Standards.** You agree that you will not use the Service in any way, or upload or provide content or otherwise post, transmit, distribute, or disseminate through the Service any material that: (a) is false, misleading, unlawful, obscene, indecent, lewd, pornographic, defamatory, libelous, threatening, harassing, hateful, abusive, or inflammatory; (b) encourages conduct that would be considered a criminal offense or gives rise to civil liability; (c) breaches or infringes any duty toward or rights of any person or entity, including rights of publicity, privacy, or intellectual property; (d) contains corrupted data or any other harmful, disruptive, or destructive files; (e) advertises products or services competitive with Zelle, as determined by Zelle in its sole discretion; or (f) in the sole judgment of Bank or Zelle, is objectionable, restricts or inhibits any person or entity from using or enjoying any portion of the Service, or which may expose us, Zelle, or our respective affiliates or customers to harm or liability of any nature. Although neither we nor Zelle have any obligation to monitor any content, both we and Zelle have absolute discretion to remove content at any time and for any reason without notice. We and Zelle may also monitor such content to detect and prevent fraudulent activity or violations of this Agreement. We and Zelle are not responsible for, and assume no liability, for any content, including any loss or damage to any of your content. We and Zelle make no representation or warranty that content uploaded to a User profile accurately identifies a particular User of the Service.

4. **Consent to Emails and Automated Text Messages.** In the case of any messages that you may send through either us or Zelle or that we may send or Zelle may send on your behalf to an email address or mobile phone number, you represent that you have obtained the consent of the recipient of such emails or automated text messages to send such emails or text messages to the recipient. You understand and agree that any emails or text messages that we send or that Zelle sends on your behalf may include your name.

5. **Payees that are not Users.** As of the date of this Agreement (as indicated in the footer), the Service does not allow payment attempts to persons that are not yet enrolled in Zelle. If this capability is added and you then attempt to send money to someone who has not enrolled as a User with Zelle, they will receive a text or email notification instructing them on how to enroll to receive the money. You understand and acknowledge that a person to whom you are sending money may fail to enroll with Zelle, or otherwise ignore the payment notification, and the transfer may not occur.

6. **Payments on behalf of Third Parties.** You will not use this service to send money on behalf of a third party unless (i) you have disclosed the circumstances to Bank; (ii) the third party is domiciled in the United States; and (iii) Bank has approved. Bank may withhold or condition its approval in its sole discretion. You agree that Bank is entitled to rely on your instructions and you will be solely responsible to the third party if there is any dispute or loss.

7. **Private Health Information (PHI) Exclusion.** Certain terms used in this paragraph are defined in the Business Associate Agreement terms incorporated above in this Agreement. Bank states that the Zelle Disbursements service is not designed to process PHI in compliance with HIPAA and Bank assumes no obligations of a Business Associate in connection with the IR service. If Client is a Covered Entity, Client acknowledges the foregoing statement and agrees that (i) it will ensure that it does not enter PHI in any fields in its payment initiation file. Any transmission of PHI by Client, whether inadvertent, incidental, or otherwise, must be communicated to Bank immediately upon discovery. Bank accepts no liability arising from its receipt of PHI in connection with the Zelle Disbursements service.

8. **No Warranty.** EXCEPT AS OTHERWISE PROVIDED HEREIN, AND SUBJECT TO APPLICABLE LAW, NEITHER BANK NOR ZELLE MAKES ANY EXPRESS OR IMPLIED WARRANTIES, REPRESENTATIONS OR ENDORSEMENTS WHATSOEVER WITH RESPECT TO THE SERVICE. BANK AND ZELLE EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, WITH REGARD TO THIS SERVICE. BANK DOES NOT WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE, OR THAT DEFECTS WILL BE CORRECTED. THE SERVICE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. EXCEPT AS OTHERWISE PROVIDED HEREIN AND SUBJECT TO APPLICABLE LAW, IN NO EVENT WILL BANK OR ZELLE BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, OR OTHER INDIRECT DAMAGES ARISING OUT OF (I) ANY TRANSACTION CONDUCTED THROUGH OR FACILITATED BY THE SERVICE; (II) ANY CLAIM ATTRIBUTABLE TO ERRORS, OMISSIONS, OR OTHER INACCURACIES IN THE SERVICE, (III) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA, OR (IV) ANY OTHER MATTER RELATING TO THE SERVICE, EVEN IF BANK OR ZELLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF YOU ARE DISSATISFIED WITH BANK'S SERVICE OR WITH THESE TERMS, YOUR SOLE AND EXCLUSIVE REMEDY IS TO DISCONTINUE USING THE SERVICE. IN THOSE STATES WHERE THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES MAY NOT APPLY, ANY LIABILITY OF BANK OR ZELLE AND ITS OWNERS, DIRECTORS, OFFICERS, AGENTS, AND NETWORK FINANCIAL INSTITUTIONS IS LIMITED AND WARRANTIES ARE EXCLUDED TO THE GREATEST EXTENT PERMITTED BY LAW. Client is responsible for carefully reviewing the applicable reference materials and limiting its Zelle Disbursement transactions to those that present only a level of risk determined by Client to be acceptable.

Zero Balance Account Service

1. Description of Zero Balance Account Service. The Zero Balance Account ("ZBA") service allows Client to manage cash flow by aggregating debit and credit entries from one or more zero balance or "subsidiary" accounts to a master account on a daily basis.

2. Daily Posting and Funding. Designated subsidiary accounts, their associated master accounts, and any super master accounts (if any) will be reflected in the Treasury Request Confirmation for ZBA service. Client may designate a target ledger balance for a subsidiary account, and such designation will also be reflected in the Treasury Request Confirmation. At the end of each banking day, Bank will transfer all debit and credit entries that were posted to a subsidiary account that banking day to the master account associated with that subsidiary account, so that each subsidiary account will have a zero ledger balance (or the target ledger balance, if applicable) at the end of each banking day. Bank will post to the relevant master account a single entry equal to the net debit or credit activity in each subsidiary account. When Bank posts these entries to a master account, offsetting entries will also be posted to the relevant subsidiary account. Client agrees to maintain sufficient available balances at all times in each master account to cover any debit activity (and any target ledger balances) of all subsidiary accounts funded by that master account as well as any debits presented directly against that master account. At its option, Bank may pay, but is not obligated to pay checks, drafts, withdrawal requests or other debits presented against a master account or a subsidiary account unless the applicable master account contains sufficient funds. At its option, Bank may, but is not obligated to, return any debits presented against a subsidiary account in the event Bank reasonably believes

that the applicable master account does contain sufficient funds. In the event payment of any debits presented against a subsidiary account results in an overdraft in a master account, or if the master account does not contain sufficient funds to bring the balance of the subsidiary account(s) to zero at the end of a banking day, Client is obligated to immediately submit funds to Bank to repay any overdraft amount pursuant to the terms of the CBSA, without notice or demand. If Bank receives a writ of garnishment or levy seeking funds in a subsidiary account, Client agrees that Bank shall have the right, in its sole discretion, to (a) freeze and/or place a hold on any master or super master account(s) in an amount equal to the amount sought by the garnishor until the writ of garnishment is satisfied or in an amount as otherwise required by law, and/or (b) pay the full amount sought by the writ of garnishment using funds from any master or super master account(s); provided, further, that Bank may take these actions whether or not the ownership and/or designated representatives of the subsidiary account are the same as those for the master account. Regarding a garnishment or levy, Client further agrees that (c) Bank may collect its fees for garnishment or levy against any master, super master, or subsidiary account when the garnishment or levy is received and may offset these fees before honoring any garnishment or levy, and (d) Bank will not be liable for any hold or freeze placed on any master, super master, or subsidiary account.

3. Super Master Accounts. If Client has identified one or more "super master accounts", any master account funded by the super master account will be treated as a subsidiary account of that super master account.

4. Duration and Changing of Options. Once Bank has implemented the ZBA service according to Client's instructions, Bank will post the net amount of all debits and credits from each subsidiary account to the relevant master account in accordance with such instructions until (a) Client's use of the ZBA service is terminated or (b) Client provides modified instructions to Bank and Bank has had had a reasonable time to act on such instructions.