This Service Description is part of the Treasury Services Master Agreement (the "*Master Agreement*") currently in effect between you and BMO Bank N.A. ("*we*" or "*us*" and *"our"*). This Service Description is part of the Master Agreement and is subject to all of the terms and conditions contained in the Master Agreement. Any references herein to the Master Agreement shall be deemed to include the terms of this Service Description, including any User Guide and set-up form. Any capitalized terms not defined herein shall have the same meaning as set forth in the Master Agreement.

1. Services.

With our Financial EDI Services, we will process wire transfers or ACH credit entries ("*Fund Transfers*"), or create paper checks, as instructed by you, and based on entry data ("*Entry Data*") contained in electronic data interchange ("*EDI*") files transmitted or directed to us by you (the "*Service*"). We will process (i) ACH entries only if you have signed up for and implemented our ACH Origination Services, (ii) wire transfers only if you have signed up for and implemented our Wire Transfer Services and (iii) paper checks only if you have signed up for and implemented our Positive Pay Service. The underlying transactions for the Service including Fund Transfers and checks are sometimes referred to as "*Transactions*."

2. Transmissions.

Entry Data may be (a) transmitted directly to us through our File Transfer Facility Service (subject to your acceptance and implementation of our File Transfer Facility Service) ("*FTF*"), or (b) directed to us through the facilities of a value added network ("*VAN*") identified by you in the setup process, provided we are permitted to access the VAN to retrieve your files. We may also agree to accept transmissions through other communication systems. When using FTF or another direct communication system, you must comply with the security procedure and transmission requirements, including formatting for that system. You are responsible for complying with the requirements and procedures of the system you choose to transmit Entry Data to us.

3. Payment.

You agree to pay us for the amount of each Funds Transfer (i) in the case of ACH entries, as provided in the ACH Origination Service Description, and (ii) in the case of wire transfers, as provided in the Wire Transfer Service Description. We will add checks to the Positive Pay files for which you have completed all service documentation required for the Positive Pay service. Checks will be processed to your Account designated in the setup process and charged to that Account as provided in the Positive Pay Service Description. You agree to maintain in the Account as of the applicable settlement date and time immediately available funds sufficient to pay for each Funds Transfer. You authorize us to debit your Account for the amount of the Funds Transfers requested in the Entry Data file even if it creates an overdraft. If an overdraft exists, you agree to pay to us, upon our demand, in immediately available funds the amount of any overdraft, plus the amount of related fees and charges. We, in our sole discretion, may (i) require you to deposit immediately available funds in the Account for the Funds Transfers requested in the Entry Data file ("*prefund*") and (ii) delay processing the Funds Transfers requested in the Entry Data file if the aggregate amount of Funds Transfers requested in the Entry Data file is not prefunded. In the event you are subject to a line of credit and your request exceeds any available amount of the line of credit, you must obtain the prior approval of your relationship manager before the Transaction can be processed. We are not obligated to make or originate any Funds Transfers without such approval. We are not obligated to continue to originate any Funds Transfer without having first been paid by you if we have requested you to prefund an Account. We are not required to give notice to you that we will no longer continue to make Funds Transfers without prefunding, or credit approval, regardless of whether we may have done so previously. We may, in our sole discretion, initiate reversals of Funds Transfers for which you have not paid us or for which there is not adequate prefunding or credit approval.

4. Rules.

You agree to comply with all laws, regulations, and rules applicable to the Services, including, without limitation, the rules and regulations of the National Automated Clearing House Association and any other clearing house used in connection with any Fund Transfers, and the Fedwire System.

5. Processing of Transactions Based on Entry Data.

Subject to the terms of this Service Description, we will process Transactions based on your Entry Data and effect settlement for Funds Transfers in accordance with applicable rules and industry practices. Except as specifically provided in this Service Description, we will accept, process and handle (a) Entry Data for ACH entries in accordance with and on the terms of the ACH Origination Service Description, (b) payment orders contained in Entry Data for wire transfers in accordance with the terms of the Wire Transfer Service Description, and (c) paper checks~~,~~ in accordance with the Positive Pay Service Description. We will prepare and print paper checks based on the Entry Data as required, affix the authorized signature you provide to us solely on your behalf and mail the checks in our normal processing schedule. We will create a Positive Pay file of issued and outstanding checks to reflect the checks identified on the Entry Data file. We will originate Funds Transfers before the applicable deadlines, provided that you transmit or deliver the Entry Data to us in compliance with (i) the applicable security procedures and (ii) the format requirements and cut-off hours established by us from time to time. You agree that you are solely responsible for the accuracy and completeness of all Entry Data you or your Vendor transmit or direct to us. We are not responsible for detecting errors contained in any of your Entry Data, and we are entitled to rely on the information contained in the Entry Data. We may treat Entry Data received by us after our cut-off hours as received on the following Business Day.

6. Security Procedures.

(a) We offer the security procedures described in **Appendix A** attached hereto and those provided in the Master Agreement or separately agreed upon as a means of authenticating Entry Data (including amendments or cancellations) transmitted or delivered to us by you or your Vendor. Entry Data is effective as your instructions, whether or not authorized and regardless of the actual identity of the signer, sender, or transmitter of the Entry Data, if the Entry Data is received in accordance with the applicable security procedures, and if we accept such Entry Data in good faith and in accordance with any written agreement between us.

(b) If any Entry Data (including amendments or cancellations) is transmitted or delivered to us by you or on your behalf other than in compliance with the security procedures described in **Appendix A** attached hereto, and if we accept such Entry Data in good faith, then you agree to be bound by such Entry Data whether or not it was authorized, and you will be deemed to have refused the security procedures that we offer and recommend as "commercially reasonable." However, we have no obligation to accept any Entry Data that is not transmitted in compliance with the security procedures described in **Appendix A**, and we will not be liable for any losses or costs suffered by you as a result of our refusal to act upon any Entry Data transmitted to us if not in accordance with the procedures described in **Appendix A**.

7. Rejection of Transactions or Entry Data.

Except as otherwise expressly provided in a written agreement signed by us, we have the right to reject, and refuse to accept, any Entry Data for any reason, including your failure to maintain a sufficient balance of immediately available funds in the deposit Account specified in the Entry Data. We will have no liability to you based on our rejection of any Entry Data or Transactions. If we reject any Entry Data or Transactions, we will notify you by phone, electronic transmission, or other reasonable means no later than the Business Day that we would otherwise have originated the Transactions based on such Entry Data. We will have no liability to you based on the fact that we did not notify you earlier.

8. Cancellation or Amendment of Entry Data.

You have no right to cancel or amend any Entry Data after it has been received by us. However, we will make a reasonable effort to act on your request to cancel or amend Entry Data before we process your instructions, but we will have no liability if we are unable to effect such cancellation or amendment.

9. Remittance Advice.

As an optional service for Transactions, we will provide your trading partner with a remittance advice containing remittance detail as instructed by you. Our delivery methods include electronic data transmission, facsimile transmission, and email to an address provided by you.

10. Notice of Returned Transactions.

We will use reasonable efforts to notify you by mail, electronic transmission, phone, or other reasonable means of the receipt of a returned Funds Transfer no later than one Business Day after the Business Day of your receipt. We will have no liability to you based on the fact that we did not notify you earlier.

11. Delay.

We are not responsible for any delay or failure to effect your Entry Data and Transactions due to circumstances beyond our control including disruptions in communications facilities, power or equipment failures and the neglect, action or failure to act of any other bank, intermediary or ACH processor or funds transfer system.

12. Limitation of Liability.

We will be liable to you for use of the Services as set forth in the Master Agreement and this Service Description.

13. Notices.

Except as otherwise provided in the applicable security procedures, any written notice or other communication required or permitted to be given under this Service Description will be delivered or sent by United States mail, postage prepaid, or by express carrier, and if sent to us, addressed to:

BMO Bank N.A.
Supervisor, Automated Payments Unit (311/8)
P.O. Box 755
Chicago, Illinois 60690

THIS SERVICE DESCRIPTION HAS BEEN EXECUTED AS PROVIDED IN THE SCHEDULE OF SERVICES FORMING A PART OF THE MASTER AGREEMENT.

APPENDIX A TO COMPREHENSIVE PAYABLES/EDI SERVICE DESCRIPTION

Financial EDI and Funds Transfer Procedures

Our Financial EDI Service includes several features designed to verify the authenticity and integrity of data transmissions to us.

Verification of Payments Procedure (Recommended). This procedure ensures that a transmission received by us purporting to be from you was in fact sent or directed to us by you. We will contact your designated contact to verify: 1) the fact that you sent a transmission to us; 2) the total number of payments included in the transmission; and 3) the total dollar amount of the payments contained in the transmission.

- This procedure, used alone, will not protect against payments made to an unauthorized party nor will it protect against payments made to an authorized party, but for the wrong amount.
- This procedure, combined with the Trading Partner Profile procedure, will protect against payments made to an unauthorized party, but will not protect against payments in the wrong amount made to authorized parties.

We recommend the use of this security procedure. We also recommend that this procedure be combined with other security procedures to provide additional security.

Trading Partner Profiles Procedure (Recommended). This procedure assures that only payees that are authorized by you ("*Authorized Payees*") to receive payments can be sent electronic payments. You will provide us a file of Authorized Payees. Whenever we receive instructions to send a payment from you, the payee of the payment will be compared to the list of your Authorized Payees and if the payee is not on that list, we will reject the payment.

- This procedure does not protect against making a payment in the wrong amount to any Authorized Payee.

We recommend that you separate the responsibility for designating Authorizing Payees from the responsibility of making or approving individual payments.

We *recommend* this procedure for all transmissions.

Unscheduled Payments Procedure (Required if Applicable). This feature detects missing transmissions when a regular schedule of transmissions cannot be established. The procedure is intended for use only where a regular schedule cannot be established.

Our Datapool software has the capability to detect when a scheduled transmission is late and report this information to the system operator for corrective action. However, if no regular schedule can be established, this feature cannot be used. Therefore, where no regular schedule can be established, you would notify us to expect a transmission, thereby guarding against missed transmissions.

This procedure *will only detect a missing or delayed transmission*. It does not address in any way the content of the transmission. We *require* that this procedure be used when a regular schedule of transmissions cannot be established.

Functional Acknowledgements Procedure (Recommended). The purpose of an acknowledgement is to report, at a minimum, that one or more messages have been received. The receipt of an acknowledgement assures the sender of a message that the receiver received the message(s). In the world of EDI, a special transaction set, the 997 Functional Acknowledgement, was defined for use as an acknowledgement. The 997 can be used both to confirm receipt of a functional group and the transaction set or sets within the group and to indicate whether or not the transaction sets contained in the group conform to ANSI X12 syntax.

The 997 Functional Acknowledgement only reports that we as the receiver have received the functional group and that the transaction sets within the group do or do not syntax check. It does not indicate whether we have actually processed the transaction sets within the group or acted on them in any way.

In addition, unless authentication is used for both the original transactions and the 997, the receipt of the 997 only indicates that the person who received the message acknowledged it, not that the person who you intended to receive the message actually received it.

To be effective, a method must be in place to cross-check acknowledgements received with the original functional groups that were sent. A receiver of acknowledgements is concerned more with those functional groups that have not been acknowledged than those that have. The groups that have not been acknowledged can only be determined by cross-checking.

We will generate 997 Functional Acknowledgements for all incoming ASC X12 functional groups unless you request that we not do so. We encourage you to acknowledge all functional groups received from us.

Message Authentication Procedure (Optional). The purpose of message authentication is to verify the source and integrity of a message. This technique uses a Message Authentication Code or MAC, calculated using three components: the contents of the message, a pre-defined cryptographic algorithm, and a secret key shared by the sender and receiver.

The integrity of a message is protected by having the sender calculate the MAC and send it, with the message, to the receiver. The receiver computes its own MAC and compares it to the MAC sent with the message. If the two MACs agree, the message has not been altered since the original MAC was computed.

The source of the message can be ascertained if the MACs agree because in order for the MACs to be equal, the same secret key must have been used in both calculations. Since the receiver knows who shares a given secret key with it, it therefore knows the identity of the sender.

Authentication provides data integrity from the time the original MAC is calculated up until the time the second MAC is calculated and the security information is deleted. In most cases, this means the data will only be protected during the transmission. Care should be taken to ensure that proper controls exist to protect the data prior to the original MAC being calculated. If the message is altered and the MAC is then calculated, the MAC functions as a seal of approval.

A person receiving an authenticated message is assured that it was sent by the person who shares the key with the receiver, providing the secret key was not compromised. In addition, message authentication of the type described here cannot be used to prove to a third party who sent the message. Since the receiver also has access to the key, the receiver could have constructed the message, not received it from the sender.

We *recommend* that this procedure be used if you do not use the Trading Partner Profile procedure. We may require this procedure for our own protection if you refuse to agree to use the Verification of Payments procedure.

Message Encryption Procedure (Optional). The purpose of encryption is to provide for the confidential transmission or storage of a message. Confidentiality is provided by the sender using a cryptographic algorithm and a secret key to transform the message from readable text (plaintext) to a meaningless form (ciphertext). The receiver, using the same algorithm and the same key, reverses the process and converts the ciphertext back into plain text.

Since this procedure requires the sender and receiver to share a secret key, this procedure also gives some assurance to the receiver that the person who sent the message was the same person who shares the key with the receiver.

Although the algorithm used for encryption is the same algorithm used for authentication, encryption does not, in and of itself, provide data integrity or protection from change. While any alteration of the message after it is encrypted will result in the decryption algorithm producing a result different than the original message, the new result could go undetected since there is no guarantee that the new result will be invalid. Therefore, if data integrity is required along with confidentiality, both authentication and encryption should be used.

However, encryption can protect against intentional changes since an intruder cannot determine the result of any change to the message and, therefore, could derive no direct benefit from the change.

With regard to verification of the source of a message, the same limitation regarding proof to third parties that was listed for authentication also applies to encryption.

This procedure should be used whenever you desire to maintain the confidentiality of your messages during the transmission from your computer system to our computer system.