Business Online Banking Service Manual

This document and all amendments and revisions hereto, are incorporated as part of the Treasury Management Services Agreement and applies to Company Accounts. Modification, updates, or changes may be made to this Service Manual at any time by Bank and such shall become binding on Company upon Company's continued use of the Services. Bank may amend the Agreement, including this Service Manual from time to time upon notification to Company, as specified in the Agreement and the Account Agreement and Disclosure. Any modifications, updates, or changes to the Agreement will be effective as of the date of posting the revised terms on the System. Unless otherwise provided herein, all capitalized terms shall have the meanings as set forth in the applicable Agreement.

1. **Hours of Operation.** The Service hours of operation for the System are generally twenty-four (24) hours a day, seven (7) days a week. However, access to the System may be restricted on Sundays between the hours of 3:00 a.m. central time ("CT") and 10:00 a.m. CT, so that MidFirst Bank ("Bank") may perform routine system maintenance.

2. **Customer Service.** Telephone support is available at 877-516-2777 Monday through Friday from 8:00 a.m. CT to 7:00 p.m. CT.. Company may also contact Customer Service through email at commercialservices@midfirst.com. Sensitive and confidential information should NOT be transmitted via email, as email is a non-secure method of transmission of information. Notwithstanding anything to the contrary, Bank may rely on any communication from Company, (or Company's Administrator, Administrative User(s), or Users), regardless of form or means of communication, as authorized communication and authority for Bank to act.

3. **The Services**. Company may use the System to perform the Services identified in the Agreement.

4. **Definitions**. Capitalized terms not defined below and used in this Service Manual shall have the meanings given to them in the Agreement or the Rules, as applicable.

   "Alert" shall mean the alerts from the System as further defined in section 14d.

   "Code" shall have the meaning given to it in section 14e (i) (2).

   "Limited Transaction Accounts" shall mean accounts with a specified or limited number of transactions per a designated time period.

   "Tokens" shall have the meaning given to it in section 14e (i) (2).

5. **Balance Inquiries**. Account balances will be current as of the date and time Company signs onto the System or as set forth in notices, updates, or terms of use available on the www.MidFirst.com website from time to time. The balance displayed by the System may include deposits still pending and subject to verification by Bank. The balance shown may differ from Company records because it may not include deposits in progress, check card authorizations, outstanding checks, or other withdrawals, credits, payments, or charges. Any funds transfers will be made available in accordance with the "Funds Availability Policy" as set forth in the Account Agreement & Disclosure. All Accounts enrolled in the System for Services, (as designated on the Business Online Banking Implementation Form), will be available for viewing and balance inquiries using the System. If Company does not wish to view information on a particular Account, Company may contact Commercial Services at 877-516-2777 to edit Company's viewing capabilities.

6. **Timing Specifications**

   a. Multiple Account Transfers, Internal Transfers, Loan Payments, Loan Advances, Bill Payments, and Wire Transfers initiated on any Business Day before the Service cutoff time shown below will be processed on the same Business Day. Service cutoff times are as follows:
      i. Multiple Account Transfers, Internal Transfers, On-Us ACH Entries, Loan Payments, or Loan Advances initiated prior to 10:00 p.m. central time ("CT") on a Business Day will be effective as of the close of that Business Day. Multiple Account Transfers, Internal Transfers, On-Us ACH Entries, Loan Payments, or Loan Advances initiated after 10:00 p.m. CT on a Business Day, or on a non-Business Day, will be effective as of the close of the following Business Day.
      ii. Domestic Wire Transfers initiated prior to 5:00 p.m. CT on a Business Day will be effective as of the close of that Business Day. Domestic Wire Transfers initiated after 5:00 p.m. CT on a Business Day, or on a non-Business Day, will be effective as of the close of the following Business Day.
      iii. International USD Wire Transfers initiated prior to 4:00 p.m. CT on a Business Day will be effective as of the close of that Business Day, unless otherwise provided in an amendment to the Agreement. International USD Wire Transfers initiated after 4:00 p.m. CT on a Business Day, or on a non-Business Day, will be effective as of the close of the following Business Day, unless otherwise provided in an amendment to the Agreement.
      iv. International FX Wire Transfers initiated prior to 2:00 p.m. CT on a Business Day will be effective as of the close of that Business Day, unless otherwise provided in an amendment to the Agreement. International FX Wire Transfers initiated

after 2:00 p.m. CT on a Business Day, or on a non-Business Day, will be effective as of the close of the following Business Day, unless otherwise provided in an amendment to the Agreement.

v. Bill Payments initiated prior to 8:00 p.m. CT on a Business Day will be effective as of the close of that Business Day. Bill Payments initiated after 8:00 p.m. CT on a Business Day, or on a non-Business Day, will be effective the close of the next following Business Day.

vi. Payroll Services must be funded through a "funding account" set up with the third party payment processor, (SurePayroll, Inc.) and the funding account(s) must be funded by 2:00 p.m. local time, at least two (2) Business Days prior to the payroll ACH transmission date. The funding amounts must be sufficient to cover Payroll Services deductions. Company must have sufficient funds in their Bank Account for any processing or transactions to be completed and cleared.

vii. Expedited Payments must be scheduled prior to 6:45 p.m. CT on a Business Day for overnight checks; for non-Business Days or after 6:45 p.m., such Expedited Payments by overnight check will be processed the next Business Day. Same day ACH Expedited Payments are dependent on the Payee and will be processed same Business Day, provided the "pay it faster" or "same-day payment" option is still available through the Payee.

b. ACH Entries or External Transfers initiated on any Business Day after 5:00 p.m. CT may not be processed until the next Business Day or such Effective Entry Date as specified in the ACH Entry, whichever is later. It is recommended that Company initiate ACH transactions at least two (2) Business Days prior to the Effective Entry Date to allow ample time for Bank and Company to work through any processing errors or issues.

c. Unless agreed by Bank and Company in writing, Company may originate ACH Entries under only the following Standard Entry Class (SEC) Codes: CCD (Corporate Credit or Debit), PPD (Prearranged Payment and Deposit), and CTX (Corporate Trade Exchange).

d. Same Day ACH Credit Entries may be originated by Company subject to Bank's prior approval. Same Day ACH Entries will be processed on the Effective Entry Date. Notwithstanding the foregoing, Same Day ACH Entries must be received by Bank no later than 1:15 p.m. CT on the Effective Entry Date for same-day processing. If Company has enrolled in Same Day origination services, Entries that are submitted prior to 1:15 p.m. (whether on that same day or after hours the preceding day) with a stale or current-day Effective Entry Date may be transmitted as Same Day Entries, regardless of Company's intent. Same Day ACH fees will apply in such scenarios. Same Day ACH Entries are transmitted in Bank's sole discretion. Company's Same Day ACH Entries are subject to Company's pre-existing ACH limits, the Rules, and Bank's right to require pre-funding. Bank shall not be liable for any loss, claim, costs, or damages incurred by Company for any Entry that is not transmitted as a Same Day Entry due to Company's failure to comply with the Rules, Company's ACH limits, or other ACH file requirements.

e. Bank may, in its sole discretion, permit Company to originate Same Day ACH Entries on an urgent and expedited basis, subject to Company's acceptance of Bank's Same Day ACH terms and conditions, which Bank may communicate to Company through such means Bank deems acceptable. To request such service, Company should contact Commercial Services.

f. Check Issue File (and Check Issue Items) must be submitted to Bank by 6:00 a.m. CT on a Business Day.

g. Positive Pay, Payee Positive Pay, and Reverse Positive Pay decisions must be remitted to Bank on each Business Day between 8:00 a.m. CT and 2:00 p.m. CT. Any Positive Pay Exception decisions not remitted in the System to Bank by 2:00 p.m. CT on a Business Day will result in Bank applying the Default Decision, designated by Company on the Business Online Banking Implementation Form. Positive Pay requires User set-up and training. Until such set-up and training are completed, all items will be paid in accordance with the Bank's standard policies.

h. ACH Positive Pay decisions must be remitted to Bank on each Business Day between 7:00 a.m. CT and 5:00 CT. Any ACH Positive Pay Exception decisions not remitted in the System to Bank by 5:00 p.m. CT on a Business Day will result in Bank applying the Default Decision, designated by Company on the Business Online Banking Implementation Form.

i. If Bank is unable to process a transaction as requested, Bank may notify Company through an Alert sent via the Business Online Banking secure mail system, Internet email, or through alternative methods, or contacting Company by telephone by 9:00 p.m. CT on the Business Day the Bank received the request. Company may not and has no right to cancel or amend an On-Us ACH Entry, originated ACH Entry, Bill Payment, External Transfer, or Wire Transfer request after its receipt by the Bank. If, however, Bank receives a request to cancel or amend an External Transfer, ACH Entry, Wire Transfer, or Bill Payment, Bank, at its sole option, may make a reasonable effort to attempt to cancel or amend the transaction, if Bank has not yet acted upon the request. Bank may, in its sole discretion, engage in discussions with Company on Exception matters for follow-up and resolution, but Bank shall have no liability for its reliance on information provided to it or for Bank's reliance on Company's designation of Default Decision.

j. If required by Bank, ACH prenotes must be initiated at least three (3) Business Days prior to the initiation of an ACH Entry pursuant to the Rules.

7. **Payee Positive Pay**. For Payee Positive Pay selected Services, Bank will provide Company with a "Payee Positive Pay Best Practices" document with guidelines to follow, to minimize Exceptions from not capturing the Payee name information from checks presented for payment accurately. The Payee Positive Pay Best Practices document is available to Company in the Administration/Download Documents section of the System. The Payee Positive Pay Best Practices document may be updated from time to time by Bank and Company should periodically check for updates to the document on the System. The Payee Positive Pay Best Practices document is incorporated by reference into this Service Manual and is part of the Company Agreement with Bank.

8. **Bill Payments.** Using the Bill Payment Service, Company may electronically schedule Bill Payments in any amount of not less than one dollar ($1.00) or any amount exceeding twenty-five thousand dollars ($25,000), (unless otherwise agreed in writing by Bank). Total Bill Payments for any given business day shall not exceed fifty thousand dollars ($50,000), (unless otherwise agreed in writing by Bank). The Bill Payment Service will be processed through the System, (in accordance with Company's specifications), to any Payee that generates a bill or invoice for products or services provided to Company or on Company's behalf and that has a U.S. payment address. All transfer limits are subject to temporary reductions to protect the security of Company Accounts and/or the transfer system. Bank reserves the right to refuse any electronic bill or Bill Payment request based on the limitations of the

Agreement, this Service Manual, Applicable Law, and the Account Agreement & Disclosures. Company may include up to two thousand five hundred (2,500) Payees on Company's Payee list. Company may schedule Bill Payments on the same date (by 8:00 p.m. CT on Business Days) of its request or on a future date up to three hundred sixty-four (364) days in the future. For each, the funds will be withdrawn from Company's designated Account and sent to the Payee for delivery, within two (2) Business Days, after the scheduled "send-on date," unless the payment is otherwise suspended, rejected, or refused for any reason in accordance with the Agreement, this Service Manual, Applicable Law, or the Account Agreement and Disclosure. In order to provide sufficient time for Bill Payments to be received by Payees, Company should schedule Bill Payments five to ten (5-10) Business Days before the Bill Payment due date, excluding any applicable grace periods (the "Due Date"). If Company schedules a Bill Payment for the same day, it must be submitted to the Service by 8:00 p.m. CT on a Business Day in order to be scheduled the same day Company submitted the information. If information is submitted after 8:00 p.m. CT on a Business Day, the payment will be scheduled for the next Business Day. Company may use the System to electronically change the amount or date of a scheduled Bill Payment, or to electronically cancel a Bill Payment prior to 8:00 p.m. CT on the "send-on date" scheduled for the Bill Payment. If Company is unable to stop or cancel a Bill Payment through the System, Company may call Commercial Services at 877-516-2777 Monday through Friday from 8:00 a.m. CT to 7:00 p.m. CT. Bank may make a reasonable effort to attempt to stop or cancel a Bill Payment; however, Bank makes no guarantee that any Bill Payment can be stopped or cancelled and Bank shall not be liable for any inability to stop, cancel or amend a Bill Payment. Electronic funds transfer payments cannot be stopped after 8:00 p.m. CT on the issue date.

9. **Expedited Bill Payments**. For same Business Day processing of overnight check payments, Company must schedule the Bill Payment prior to 6:45 p.m. CT on a Business Day. If Company schedules an overnight check payment as an Expedited Payment after 6:45 p.m. CT on a Business Day or on a non-Business Day, then the Bill Payment will be processed and sent the next Business Day. ACH Expedited Payments and time frames are subject to Payee system processing.

10. **Limited Transaction Accounts.** Company understands that, for Limited Transaction Accounts, such as savings and money market accounts, the number of transfers which can be made on a monthly basis is subject to Applicable Law and by the terms of the Account Agreement & Disclosure. Company agrees that it will comply with the limitations, and understands that exceeding the limitations will result in excess transaction fees and/or conversion of Company's Account to a non-interest bearing account.

11. **Loan Advance**. Company understands and agrees that if it uses or requests a loan advance through the Loan Advance Service using the System, any loan advance shall be subject to all other terms and conditions of Bank for the issuance and performance of loans in compliance with Bank's underwriting, verification, agreements, and other lending requirements and the timing and performance thereof. A Loan Advance may be denied at anytime by Bank without liability. Company must comply with all lending terms in connection with the Loan Advance Service and any default by Company on the terms of the loan agreement, shall allow Bank to seek, in addition to the remedies available under this Agreement, all other available remedies at law or in equity.

12. **Account Agreement & Disclosure.** The MidFirst Bank Account Agreement & Disclosure, which Company received when Company opened its MidFirst Account(s) or received as an updated replacement disclosure from the Bank, governs and sets forth the terms and conditions of Company's MidFirst Account(s), of which may be amended from time to time by Bank. The terms and conditions referenced in the MidFirst Bank Account Agreement & Disclosure, and any amendments to that document, shall continue to apply to the transactions, which Company initiates using the System.

13. **Security Measures and Operating Procedures.** Company agrees not to disclose any confidential and/or proprietary information regarding the System, Services, or other procedures or operations of Bank or its third party providers, to any third parties. Company further agrees to comply with all Security Procedures set forth in section 14 below, to maintain the confidentiality of all User ID's, passwords, security Codes, or other User identifications, which Company, Administrator, Administrative User(s), or User adopts or which are assigned to Company and Users, and to take such other security and protective measures as may be appropriate to prevent unauthorized access to the System and Service(s). Company agrees to notify the Bank immediately by phone, email or otherwise, if Company believes that Company's, Administrator's, Administrative User(s)', or other User's user IDs, passwords, authentication, access, Tokens, devices, or security Codes have been compromised or that an unauthorized person has gained access to the System or Company Service or to Company's system and operations. Company recognizes that the System and Services are the property of Bank or a third party contracted with by Bank, and agrees to comply with such Security Procedures and other requirements as agreed to by Company and as may be established from time to time by the Bank. As to Company's use of the System and any Service in connection with any Account, Company acknowledges and agrees that it has reviewed and selected on the Business Online Banking Implementation Form the Security Procedures as described in section 14 below and has independently determined that the Security Procedures (1) are a commercially reasonable method of providing security against unauthorized payments, access, transfers, and other intrusions, and (2) are adequate based on the size, type and frequency of payment orders and/or transfer requests and Services, which Company anticipates. Company further agrees that it is primarily responsible for ensuring that the Security Procedures selected by Company continue to be commercially reasonable and adequate, at all times and in the future for Company, and that Company shall notify the Bank immediately in writing if Company's security fails to meet the minimum standards set forth by the Security Procedures or commercial reasonable standards. Bank shall have no liability for Company's failure to maintain adequate and reasonable security measures, precautions and procedures and Company agrees to indemnify, defend, and hold harmless Bank, its shareholders, officers, directors, employees, agents, representatives, parent company, affiliates, subsidiaries, and divisions from any claims or damages from a third party for Company's failure to maintain a secure system and follow the Security Procedures. Company acknowledges and agrees that the Security Procedures are commercially reasonable with industry practices and Company agrees to work with Bank in updating and maintain reasonable ongoing Security Procedures. **COMPANY AGREES TO ASSUME FULL LIABILITY AND RESPONSIBILITY FOR ANY ALTERNATIVE**

SECURITY PROCEDURES IT OPTS TO USE, AS AGREED UPON AND SIGNED BY COMPANY WITH AN ALTERNATIVE SECURITY PROCEDURES AGREEMENT THAT DO NOT FOLLOW THE BANK RECOMMENDED SECURITY PROCEDURES.

14. **Security Procedures.**

a. Only authorized Administrator Administrative User(s), and Users may access the System and use the Services. Company, Administrator or an Administrative User(s), (or a User with the administration role), has the responsibility to and may limit each User's access by Account and/or by function (e.g., account information, Account Reconciliation, Wire Transfers, express transfers, book transfers, funds transfers, stop payments, ACH Entries, Check Issue File maintenance, Exception maintenance, Positive Pay, Payee Positive Pay, Reverse Positive Pay, ACH Positive Pay, Bill Payment, etc.). Bank may require an Administrator and an Administrative User(s) (i.e. two Approvers) for establishing new Users, deleting Users, or changing Users and functions available to those Users. In order to access the System or use the Services and view Account information, Users must have an operating system that is capable of supporting the minimum security standards and procedures:

i. Secure Socket Layer ("SSL") protocol and digital certification and authentication with a 128-bit, or higher, encryption.
ii. One or more firewall servers or devices to control the flow of traffic into the Service.
iii. Virus prevention/detection software for continuous protection against infection.
iv. Secured router used in accessing the System.

b. Login to the System is not possible without 128-bit encryption.

c. Call back conversations, if applicable and in Bank's sole discretion, may be recorded for quality control purposes.

d. The System offers a feature whereby Company may request that Bank send Company an Alert upon the occurrence of certain specified events, such as when Company's Account reaches a specified minimum or maximum balance, when a transfer has failed, or when certain deposits to or checks drawn on Company's Account have posted. These Alerts may be received by Company via the System's "Received Mail and Alerts," section to an Internet email address and/or SMS text message to a mobile device. By registering a mobile device, Company certifies that Company has proper authorization to request text alerts to such device. Wireless carrier charges may apply to alerts delivered by text message. To assure text message alerts are received, device settings should be reviewed to ensure proper notifications are enabled on the device. In order to request this feature, Company must complete the appropriate online form specifying method of notification and Company's email Alert preferences. If Company has specified an email address or mobile phone number for receipt of Company's Alerts, Company is responsible for informing Bank of any changes. Company acknowledges and agrees that Alerts may be delayed or prevented by a variety of factors, and although Bank will attempt to transmit Alerts in accordance with the specifications, Alerts are not guaranteed to be accurate, nor are they guaranteed to be sent by Bank or received by Company on a timely basis. Company agrees that Bank will not be liable or responsible in any manner for any delays, failure to deliver, or misdirected delivery of any Alert, for any errors in the content of an Alert, or for any actions taken or not taken by Company or any third party in reliance on an Alert, and specifically disclaim liability for any costs, damages or losses associated with any such failures. Company agrees to take appropriate steps to verify and confirm Alert information independently. Company acknowledges and agrees that Alerts may contain Company's name and certain information about the Account, according to the type of Alert selected, and that persons having access to Company's email will be able to view the content of the Alerts. The information provided on Alerts is intended to complement the Security Procedures selected by Company and serve as an additional fraud prevention tool for Company. Company shall be accountable and responsible for timely reviewing and responding to all Alerts, and Bank will have no liability to Company or any third parties for Company's failure to process Alerts timely.

e. The Security Procedures offered to Business Online Banking customers consist of multiple levels of access methods, authentication, User ID's, and individual passwords, which shall be kept confidential by Company and not shared. To mitigate the risk of monetary losses from unauthorized access and unauthorized transactions, and to reduce the risk of online identity theft, the Bank will recommend a specific Security Procedure Company should consider based on the types of functions performed and the transaction amounts initiated by Company. Bank reserves the right to recommend two or more Approvers or additional security controls for various functions and/or transaction initiations depending on the type and dollar amount of the transaction. The Security Procedures currently available are and can be used in various combinations:

i. Access Procedures. Company recognizes that, as between Company and Bank, the System and the Services are the property of Bank and Company shall comply with such procedures and requirements as may be established from time to time by Bank. Company must select one of the two following Security Procedures to access the System.

1. Secure Sign On Technology. "Secure Sign On Technology" adds a layer of security to help protect Company from fraudulent transactions. Secure Sign On Technology may include, but is not limited to the following:
   - User ID
   - Company ID
   - Individual Password
   - Out-of-band authentication or other industry required authentication techniques

2. Secure Token Approval Technology. "Secure Token Approval Technology" adds an additional security feature to help protect certain transactions. The Secure Token Approval Technology requires secure tokens ("Tokens") which display

a six (6) or eight (8) digit code ("Code") that changes every thirty (30) seconds. A User- created PIN and the Code is required each time a User with Approval authority approves an ACH Entry, Wire Transfer, and other designated transaction on the System. Any user entitled to ACH Entry and Wire Transfer Service from the System is required to use Secure Token Approval Technology to approve an ACH or Wire transaction, unless the Company signs an Alternative Security Procedures Agreement, and Bank agrees and allows otherwise. .

ii. Safeguarding Information. Company, Administrator, and all other Users are solely responsible for safeguarding and protecting their User IDs, passwords, security Codes, Tokens, and other authentication techniques, which allow them access to the System and Services. Company, Company shall be fully liable for all Administrator, Administrative User(s), Approvers, and Users transactions made using their User IDs, passwords, security Codes, Tokens, and/or authentication techniques.

iii. Approval Procedures. Company must select one of the following approval procedures to perform certain functions or transactions through the System. The recommended Security Procedures identified in the Agreement and this Service Manual and otherwise provided by Bank, are intended to be minimums and Company may choose to set up more Approvers and approved limits for various functions and transactions, (depending on type and dollar amount of the transaction), than are recommended by Bank and may do so through the System.

1. Single Approver. This option allows the Administrator to designate one person to approve various functions or transactions initiated by Company.

2. Multiple Approvers. This option allows the Administrator to establish that two (2) or more Approvers are required for various transactions and the individual dollar limitations of those Approvers. The Bank also has the ability to establish the number of Approvers required for various functions or transactions depending on the type and dollar amount of the transaction. Two (2) or more Approvers may be required by Bank before a transaction is processed.

iv. ACH Origination. If required by Bank, Company must initiate ACH prenotes or prenotifications at least three (3) Business Days prior to the initiation of an ACH Entry. An ACH prenote or prenotification is a non-dollar ACH Entry that may be sent through the ACH network by an ACH originator to alert a RDFI that a live dollar ACH Entry will be forthcoming and that verification of the Receiver's account number is required. The purpose of an ACH prenote is to allow the RDFI to validate the accuracy of the routing number and account number of the Receiver.

v. Multiple Approvers and Secure Token Sign On Technology. For maximum protection against unauthorized transactions and persons, multiple Approvers may be required in conjunction with Secure Token Approval Technology. The Bank also has the ability to establish the number of Approvers required for various transactions depending on the type and dollar amount of the transaction, including but not limited to, use of Secure Token Approval Technology at the transaction level for ACH origination or Wire TransfersCompany Security Responsibility. Company accepts sole responsibility for monitoring the Administrator, Administrative User(s), and the Users to which the Company, Administrator, and Administrative User(s) grants access and authority.

f. Company is solely responsible for ensuring that its operating system and Internet browser meet the minimum standards and requirements to use the System and the Services, as suggested by Bank. The approved and/or recommended operating system and Internet browsers are listed in the Administration/Download Documents section of the System. This list is updated from time to time by Bank and should be checked by Company periodically to ensure continued compliance.

g. Company agrees to maintain the confidentiality of Confidential Information using the Security Procedures and other commercially reasonable security practices, set forth by the industry. Company shall only disclose Confidential Information on a need-to-know basis both internally and externally. If Company is required to provide any Bank Confidential Information to any external parties, then Company agrees to notify Bank first and seek Bank's approval and written consent prior to any such disclosure of Bank Confidential Information.

h. **Company shall notify the Bank immediately if it believes that its Administrator, Administrative User(s), or User numbers, passwords, security Codes, Tokens, any other authentication techniques, or any other Confidential Information has been compromised, or becomes known or suspected to have become known to an unauthorized person, or that an unauthorized person has gained access to the System, Company's system, or the Services. Telephone notice shall be given by calling 877-516-2777 Monday through Friday from 8:00 a.m. CT to 7:00 p.m. CT, or via email to commercialservices@midfirst.com.**

i. Company should continually monitor its access to the System and activity on the System and activity on its own system for unauthorized use, access, and intrusion. Company should seek qualified technical professional assistance to validate Company's security methods and procedures.