Remote Deposit Service Manual

This Remote Deposit Service Manual ("Service Manual") and all amendments and revisions hereto, are incorporated as part of the Treasury Management Services Agreement ("Agreement"). In the event of conflict between the Agreement and this document, this document shall control. Unless otherwise provided herein, all defined terms shall have the meanings as set forth in the Agreement.

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

2. **Customer Service**.

    a. Telephone support is available at 877-516-2777 Monday through Friday from 8:00 a.m. to 7:00 p.m. CT. Company may also contact Commercial Services through electronic mail at commercialservices@midfirst.com. Bank will respond to electronic mail inquiries within one (1) Business Day of receipt. Do not include sensitive or personal Account information in emails.

    b. Bank will review Service with Company and assist with training of new Users. Company is ultimately responsible for training its Users, but Bank may assist as requested by Company. Bank will notify Company of changes to Service and provide notice to Company of updated, modified or amended Agreement, Service Manual, and User Guides as necessary.

3. **The Service**. Company may use the Service to perform the following functions:

    a. Deposits. Company can create, capture, correct, balance and transmit deposits.

    b. Reports. Company can view and print reports.

    c. Account History. Company can view and print Account and deposit history.

    d. Users. Company can manage its Users and their respective accesses.

4. **Definitions**. As used in this Service Manual:

    a. "**Account Agreement and Disclosure**" shall mean the agreement and disclosure Company received when Company opened its MidFirst Bank account(s), which may be amended or updated from time to time by Bank, and which governs the terms and conditions of Company holding the Account(s).

    b. **"Administrator"** shall mean the individual authorized by the Company, that shall be the primary contact with the Bank on the use of the Services, and as designated on the Remote Deposit Implementation Form, to have full User access for the Services, on the Account(s), access to Account information, establish and direct Service features and options to be used by Company to establish authorized Users and their access rights, and to conduct selected transactions and Services on behalf of the Company.

    c. "**Failure Threshold**" shall mean the score set by the Service that must be met or exceeded or an Item will not be allowed.

    d. "**User Guide**" shall mean the information and guide provided by Bank to Company for the purposes of outlining the Services and Company's use of the Services.

5. **User Guide**. Bank will provide Company with a User Guide to assist Company in its participation in the Service.

6. **Endorsement of Items**. All Items must be properly endorsed and should contain the word "Processed" or "Scanned" on the face of the Item. The endorsement and notations should be clearly visible on the Imaged Item to prevent any delay in processing.

7. **Altered Items**. Altered Items are not to be deposited. Company should review all Items before processing to ensure accuracy and timely deposit of Imaged Items.

8. **Timing Specifications for Imaged Items**. Deposits transmitted to the Bank will be credited to the appropriate Account on the date of receipt if received before 7:00 p.m. local time on a Business Day (as defined in the Account Agreement and Disclosure). As referenced in the Account Agreement and Disclosure Funds Availability Policy section, Bank will make funds from Company's deposits available to Company on the first Business Day after the day Bank receives Company's deposit. If, for any reason, Company is unable to transmit to Bank or Bank is unable to receive the Imaged Item, the deposit must be delivered to Bank by Company, at Company's expense, and Bank will process the deposit item as a paper transaction credited in accordance with Bank's "Funds Availability Policy" outlined in the Bank Account Agreement and Disclosure, which were provided to Company at the time of Company opening the Account and available to Company at any time upon request.

9. **Image Inspection**. The system has forty-nine (49) Image Quality Assurance ("IQA") fields. Fields are weighted individually and rolled up into a Failure Threshold. If an image does not pass the Failure Threshold, the Service will not allow that Item into the deposit.

10. **Scanner Failure**. As described in the Agreement, if Company's Scanner should fail, Company will process Items in one of the following manner:

a. US Mail. Company may mail all items with the appropriate deposit slip and other required documents to:

MidFirst Bank, P.O. Box 76149 Oklahoma City, OK 73147-2149.

b. Banking Center. Company may deliver the Items for deposit directly to a banking center.

11. **Right to Inspect**. Pursuant to the Agreement, Bank reserves the right and Company agrees to allow Bank to conduct periodic on-site inspections of Company's Scanner, other related equipment and security procedures to ensure compliance with the requirements of the Service. Onsite inspection of Company's check processing location may be required prior to Service initiation to ensure Company's check storage and its destruction facilities are adequate and have the appropriate controls in place. Bank may choose to periodically inspect these facilities to ensure compliance.

12. **Level of Care**. It is recommended to exercise care and implement a review process for the following:

    a. Manually or hand-keyed items. Company should take extra care when manually processing Items to avoid unnecessary errors and delays in processing. Company is solely responsible for any losses or errors associated with manual or hand-keyed items.

    b. Duplicate Items. Company should be cautious when processing duplicate Items so that Items are not processed multiple times. Company may receive an error when depositing a duplicate Item; however, Company may reset the duplicates allowing Company to run the Item again. Bank will check for duplicate Items once the deposit has been received.

    c. Amount Field. Company should exercise caution with regard to changing the amount field on the applicable system.

13. **Hardware, Software and Scanner Minimum Requirements**. In order to properly utilize the Service, the following hardware, software and Scanners are required:

    a. Hardware.

        i. Pentium 4 2.0 GHz or Core 2 Duo 1.86 GHz processor (Recommend 3.0 GHz due to processing required for CAR/LAR)
        ii. 512 MB RAM
        iii. 250 MB free hard drive space
        iv. Network card
        v. Broadband Internet access vi. USB 2.0
        vii. Screen resolution (Recommend 1024 x 768)
        viii. Remote Deposit scanner

    b. Software. Software requirements vary based upon the version of the Service Company selects and the volume of Imaged Items per deposit Company runs through the Service.

        i. Windows 8 or 8.1 (32 or 64 bit)
        ii. Windows 10 (32 or 64 bit)
        iii. Apple OS X Yosemite
        iv. Internet Explorer 9 10 and 11
        v. Edge
        vi. Chrome (minimum version 40)
        vii. Safari (minimum version 8)

    c. Scanner. Scanner requirements will vary depending on the version of the Service Company selects.

        i. Remote Deposit - Basic version uses a single-feed scanner.
        ii. Remote Deposit - Premium and Premium Plus versions use a multi-feed scanner.
        iii. Digital Check (TS 215, TS 220, TS 220e, TS 230, TS 240, TS 4120 and CheXpress)
        iv. Panini (iDeal, MyVisionX)
        v. Epson
        vi. RDM (ec8000)

    d. Monitoring. Company will monitor and check all hardware, software and scanners on a regular basis to ensure it is functioning properly.

    e. Non-Web customers only (Remote Deposit - Custom version). Company must have hardware capacity sufficient to store Imaged Items for a minimum of fifteen (15) Business Days. Company has the option to request Bank establish the retention of Imaged Items for longer than fifteen (15) Business Days, which will be at Company's cost.

14. **Email Verification**. Bank will send Company communications, notifications, and verifications via electronic mail. Company is solely responsible for ensuring that Bank has a valid email address on file for all such communications, notifications, and verifications.

    a. Company will receive email notifications when Bank receives deposits; receipt for purposes of processing checks shall be effective only when the Company receives an email acknowledgement of receipt from Bank.

    b. Company should verify that it received email verification from the Bank confirming a successful deposit transmission and, if Company does not receive such email notification for deposits, Company should immediately notify Commercial Services at the number provided above.

15. **Administrator**. Company will designate an Administrator on the Remote Deposit Implementation Form. The Administrator's duties include, but are not limited to the following:
    a. Creation and deletion of Users from the Service.
    b. Assignment and removal of User roles.
    c. Assignment and removal of Accounts from the Service.
    d. Assignment and resetting of passwords.
    e. Enabling and disabling of Users from the Service.
    f. Unlocking Users.
    g. Editing User emails.
    h. Resetting of duplicate history.
    i. Being point contact person with Bank.
    j. Oversees use of the Services and identifies any errors, defects, or problems with Company's use of the Services.

16. **Account Agreement and Disclosure**. The terms and conditions referenced in the MidFirst Bank Account Agreement and Disclosure, and any updates, changes, or amendments to that document, shall continue to apply to the transactions which Company initiates using the Service. However, to the extent that the MidFirst Bank Account Agreement and Disclosure conflicts with the Service Agreement or with this Service Manual (including any amendments) regarding a transfer made using the Service, the Service Agreement and/or Service Manual shall control. For any other conflicts between the Agreement or the RD Service Manual and the Account Agreement and Disclosure, the Account Agreement and Disclosure shall control.

17. **Security Measures and Operating Procedures**. Company agrees not to disclose any proprietary information regarding the Service to any third party. Company further agrees to comply with all Security Procedures set forth in this RD Service Manual and as may be established by the Bank, to maintain the confidentiality of all Account numbers, User numbers, ID's and passwords, which Company or Administrator adopts or which are assigned to Company, and to take such other measures as may be appropriate to prevent unauthorized access to the Service. Company agrees to notify the Bank immediately as set forth in this Agreement, if Company believes that Company's, Administrator's, or other User's user IDs, passwords or security codes have been compromised or that an unauthorized person has gained access to the Service. Company recognizes that the Service is the property of the Bank's and agrees to comply with such procedures and requirements as may be established from time to time by the Bank. As to Company's use of the Service in connection with any Account, Company acknowledges and agrees that it has reviewed and selected the Security Procedures as described herein and has independently determined that the Security Procedures (a) are a commercially reasonable method of providing security against unauthorized payments and (b) are adequate based on the size, type and frequency of payment orders and/or transfer requests which Company anticipates. Company further agrees that it is responsible for ensuring that the Security Procedures selected by Company continue to be commercially reasonable and adequate as described above in the future, and that Company shall notify the Bank immediately in writing if it determines anything to the contrary. If an Imaged Item received by the Bank purports to have been transmitted or authorized by Company, it will be deemed effective even if not so authorized, provided the Bank acted in compliance with the Security Procedures regarding the order or request. If an order or request was transmitted or authorized by Company, Company shall be obligated to pay the amount, whether or not Bank complied with the Security Procedures.

18. **Security Procedures**.
    a. Authentication. Bank provides multi-factor authentication for customers to log onto the Service via HTTPS.
    b. Building Security. Company must take the appropriate steps to secure its building, specifically the area that houses the Service Scanner and other Service-related equipment.
    c. Secure Transmission. Company must use a secure transmission authenticated by the Bank to use the Services.
    d. Check Storage. Company must implement check storage with the appropriate controls to prevent unauthorized access to store and maintain original Items for time specified in the Agreement.
    e. Equipment Controls. Company must have the appropriate controls in place to protect and secure all Service-related equipment, including but not limited to computers, Scanner equipment, and software.
    f. Security Controls. Company must implement reasonable security controls, consistent with Bank recommended security procedures and industry standards, for the protection against unauthorized access to Company passwords, IDs, login information, the Services, emails, and any other information, equipment, or data in Company's control, which is considered confidential and proprietary.

19. **The Company shall notify the Bank immediately if it believes an unauthorized person or that an unauthorized person has gained access to the Service or its related equipment. Telephone notice shall be given by calling 877-516-2777 Monday through Friday from 8:00 A.M. to 7:00 P.M. CT, or via email to commercialservices@midfirst.com.**

20. **The Company should monitor all Service activity for unauthorized use and access. The Company is responsible for and should seek qualified professional assistance to validate its security methods and procedures.**