

DIGITAL BANKING BASIC ACCESS AGREEMENT (INCLUDING MOBILE SERVICES)

I. INTRODUCTION TO THE SERVICE

Thank you for choosing Midland States Bank to assist you in meeting your deposit account needs through Digital Banking Basic (the "Service"). By executing the Enrollment and Execution Form provided herewith, Customer and Bank agree as follows:

1) **Definitions.** The following terms used in this Agreement have the meanings set forth below. Where appropriate, terms defined in the singular are deemed to include plural and those defined plural are deemed to include the singular.

- a) "Account" means each of Customer's deposit accounts at Bank that is accessed via Digital Banking Basic.
- b) "Account Agreement" means the terms and conditions for Bank deposit accounts as provided at account opening and as it may be modified from time to time.
- c) "Agent" means the person(s) Customer appoints by resolution to execute this Agreement, who will have the authority provided in this Agreement.
- d) "Applicable Law" means any federal and state law (to the extent not considered to have been preempted by federal law) that applies to a party or the Service and the applicable rules and regulations.
- e) "Business Day" means any day during which Bank is open to the public for conducting all banking functions. None of Saturdays, Sundays, federal or state holidays or any day recognized by a Federal Reserve Bank as a holiday are considered Business Days, even if Bank's offices are open.
- f) "Check" means a draft, payable on demand and drawn on or payable through or at an office of a bank, whether or not negotiable, that is handled for forward collection.
- g) "Check Image" means a digitized image of the front and back of a Check and associated MICR Data provided to Bank in lieu of the original Check.
- h) "Confidential Service Information" means all Account numbers, identification data, and Login Credentials provided to or used by Customer in connection with any Service as well as information concerning access to any Service or to Customer's Account, including the Security Protocol.
- i) "Customer" means the business customer entering into this Agreement and any individual that Customer has authorized to use the System or Services according to the rules and procedures described herein.
- j) "Cut-off" means the deadline for delivery of certain information through the System. Cut-off times are posted on the Digital Banking Basic website or otherwise made available by Bank.
- k) "Digital Banking Basic" means the Internet banking system provided by Bank through its Website that enables Users to view Account information and perform certain transactions in Accounts.
- l) "Implementation Documents" means the enrollment and set-up materials and any supplement thereto required by Bank to implement the Service.
- m) "Internal Transfer" means a transfer of funds from a

Customer Account to another Customer Account at Bank.

- n) "Internet Service" means any Service that is or may be offered by Bank that is accessed on the Internet, including via Digital Banking.
- o) "Login Credentials" means company and User IDs, personal identification numbers ("PINs"), passwords, digital certificates/signatures, private keys or other security devices required by Bank to log into Digital Banking Basic and view Accounts and execute certain transactions in Accounts.
- p) "Mobile Device" means a smart phone or tablet enrolled in Digital Banking Basic for access to Account information.
- q) "Mobile Service" means a Service that accesses Accounts via a Mobile Device.
- r) "MICR Data" means Magnetic Ink Character Recognition, the line of numbers and letters on the bottom of the front of a Check that facilitates processing.
- s) "Primary Administrator" means the representative or Customer employee named by Customer to be responsible for coordinating and monitoring use of Digital Banking Basic.
- t) "Security Protocol" means the use of Login Credentials and additional procedures, including challenge questions, out-of-band authentication, encryption and other systems and software that Bank utilizes from time to time to protect Customer's information and mitigate against fraud.
- u) "Service Provider" means the third party providing the System.
- v) "System" means the software, systems and other applications that comprise Digital Banking Basic.
- w) "Token" means an electronic device that will permit Users to generate a one-time use numeric code to provide authentication to effect transactions in connection with certain Services. Tokens may be "hard" (tangible) or "Soft" (electronic on a User's device).
- x) "User" means those representatives and Customer employees designated to access one or more Accounts through the System. Any Agent or Primary Administrator, if set up in the Implementation Document or online, may be a User. This Agreement acts as Customer's authorization to allow the Users to access Accounts and process transactions which may directly affect the Accounts and Customer's liability to Bank.

2) **Other Agreements, Laws and Regulations.** The Digital Banking Basic Service is provided to Customer subject to the following other agreements, laws and regulations, which are hereby incorporated into and made part of this Agreement: (a) the Implementation Documents and User Guides; (b) the most current fee and availability schedule and other disclosures provided to Customer, including periodic Account statements; (c) the provisions of the then current Account Agreement and accompanying disclosures, which govern standard deposit accounts and other depository services; and (d) Applicable Law.

3) **Change of Terms/Amendments to Agreement.** From time to time, Bank may amend any of the terms and conditions contained in this Agreement. Such amendments shall become effective upon the date stated in Bank's notice to Customer. Bank reserves the right to notify Customer of changes electronically, by Internet posting, mailing or other means permitted by law. Using the Service following the effective date of the amendment shall be deemed

evidence of Customer's acceptance of and agreement to the amendment. This Agreement may not be amended or modified by Customer unless agreed to in writing by Bank.

4) Representative Persons of Customer.

a) Agents. In order to enter into this Agreement and access Digital Banking Basic, Customer must provide to Bank (or there must be on file with Bank) a signed and completed company resolution in the form provided by Bank or other form acceptable to Bank. The resolution must evidence the proper authority of the named Agents(s) to execute this Agreement, the applicable Implementation Documents and any authorization forms. Agents may act on behalf of Customer under this Agreement, including, without limitation, appointing the Primary Administrator for Digital Banking Basic, signing additional documentation that may be necessary to implement the Service and giving Customer's instructions with regard to Digital Banking Basic.

b) Bank Rights. Bank is entitled to rely on such authorizations according to their terms until Bank receives properly authorized written notice in the form provided by Bank or other form acceptable to Bank that the existing authorization is changed or terminated and Bank has a reasonable opportunity to act on such notice.

5) Administration.

a) Primary Administrator. Customer agrees to designate one Primary Administrator for Digital Banking Basic.

i. The Primary Administrator is responsible for setting up Digital Banking Basic and for establishing internal security procedures, including, without limitation, system-wide configuration of Accounts, assigning Users, establishing authority levels, establishing authorization requirements, distributing and re-setting Login Credentials and other internal security devices related to the Service.

ii. Customer acknowledges that the Primary Administrator may receive email notifications from Bank from time to time and that the Primary Administrator is responsible for sharing pertinent information regarding updates to Digital Banking Basic and notices regarding the availability of services with other users at Company.

b) Users. Bank has no control over the establishment of Users or the identity of such Users, the personal information of such Users, or such Users' Login Credentials.

c) Intercompany Authority to Transfer or Commingle Funds. In the event that Customer requests Bank to provide the Service to a parent company, subsidiary, affiliate, or other commonly owned company, Customer agrees that it shall be jointly and severally liable for such company's obligations under this Agreement. Customer hereby represents and warrants to Bank that any and all transfers and commingling of funds required or permitted by any Service or requested by Customer, and all other aspects of the performance hereby by Bank and Customer, have been duly authorized by all necessary parties, including, without limitation, the account holder of each account, and that Customer has obtained and shall maintain in its regular business records and make available to Bank upon reasonable demand, for a period of two years after termination of the Service, adequate documentary evidence of such authorization from the account holder of each account,

executed by the duly authorized officer(s) of each such account holder in accordance with that account holder's bylaws and/or board resolutions. Customer further represents and warrants that each transfer or commingling of funds authorized hereunder is not in violation of any agreement, bylaw or board resolution of Customer or any of its affiliates or subsidiaries, nor is it in violation of any applicable federal, state, local law, regulation, of any decree, judgment, order of any judicial or administrative authority. Each representation and warranty contained herein shall be continuing and shall be deemed to be repeated upon Bank's effecting each transfer and commingling of funds authorized hereunder.

6) Security Protocol. Access to Digital Banking Basic will be controlled through the use of Login Credentials. Bank will assign unique codes which may include a Customer identification number ("Company ID"), a User identification number ("User ID") and password ("User Password"). Login Credentials that are assigned to individual Users shall not be shared with any other person, including other Users, and Customer shall not disclose any information regarding the Service that an unauthorized User would find helpful to obtain access to all or part of Digital Banking Basic. Bank reserves the right to issue new Security Protocol requirements and/or to cancel or change any Security Protocol by giving verbal or written notice to Customer.

a) Enhanced Multi-Factor Security. Access to Digital Banking requires the use of a Token or Out-of-Band Authentication/Biometrics. Each enhanced security device delivers a Security Access Code to be entered before accessing the applicable Service. One-time passcodes may be used in lieu of Tokens for customers who have view-only access to Account activity.

b) Tokens. Each tangible Token at all times remains Bank's exclusive property. Customer may not export, directly or indirectly, the Tokens or any technology inherent in the Tokens. Customer is responsible for communicating to the Bank any employees that have been assigned a Token. Customer is responsible for notifying Bank of the termination of an employee's Token access and the reassignment or return of Token.

c) Access and Security. Customer agrees to use the Internet Services in accordance with the Security Protocol established by Bank. Without limiting the foregoing, Customer shall at all times use a Web browser that supports the level of encryption used by Bank as part of its Security Protocol. Due to emerging technologies and ensuing changes in security practices, Bank reserves the right to supplement or change its Security Protocol from time to time upon reasonable notice to Customer.

7) Data Security Breach Notice. If Customer has reason to believe that a Security Protocol or Login Credentials have been or may become known by unauthorized persons (whether or not employed by Customer) or if Customer believes its network or computer systems have been compromised or its computers infected, Customer shall immediately notify Bank by calling 855-696-4352 and confirming such verbal notification in writing to Bank within 24 hours. If Customer believes there has been a security breach or that someone has transferred or may transfer money from Customer's Account without Customer's permission, Bank will replace the Login Credentials in accordance with Bank's procedure. Bank may also deny Customer access to the System in its sole discretion in order

to protect Accounts. Customer shall be solely responsible for instructions and other communications or transactions initiated before Bank received Customer's notice and had a reasonable time to act on such notice. Customer agrees to defend and indemnify Bank against any claims, losses, damages, costs, expenses, fines and other liabilities arising out of Customer's failure to maintain the security and confidentiality of the Login Credentials or arising out of the unlawful use of any website or portal by Customer or any person who obtains access to a website or portal using the Login Credentials.

8) Computer Equipment and Software. Customer shall ensure that computers and other equipment have the necessary compatibility and format to interface with the System, including, without limitation, the ability to support the Bank's Security Protocol. Customer agrees to install upgrades including software patches and other system enhancements within ten (10) Business Days of being requested to do so by Bank. License agreements for necessary software shall either be embedded in the software or separately documented in the Service Documentation. Customer agrees to comply with all applicable software license agreements. Customer has no rights or ownership in any software provided by or through Bank and shall not transfer, copy, alter, modify, reverse engineer, reproduce, or convey in any manner, in whole or in part, any such software. Customer shall return all software and User Guides associated with any software upon request.

9) Antivirus Protection. Customer must ensure that the software (excluding software provided by Bank), listed websites and related materials Customer uses in accessing Digital Banking Basic are free of defects, bugs and virus, software problems and other Items of a destructive nature. Bank is not responsible for any of these problems. Customer agrees to run antivirus scans before transmitting data to or through any website. Customer may use any commercially available, industry recognized antivirus software of the type that detects and disinfects viruses automatically, without the need for Customer to execute virus scanning for each file manually. Customer shall update its antivirus software on a regular basis and in no event less often than once every month or as updates become available.

10) Third-Party Networks. Some Services and features are provided by Bank through access to a third-party network or Service Provider. Such Services and features are dependent upon the availability of the third-party network on conditions acceptable to Bank. Bank reserves the right to discontinue the Service or feature provide the Service or feature through an alternative third-party network and shall have no liability should such network become unavailable. Bank does not warrant and shall not be responsible for Services received by Customer from any third-party network.

II. DIGITAL BANKING BASIC FUNCTIONS AND FEATURES

1) Features. Digital Banking Basic provides direct access to Accounts online via the Internet. The features currently available through Digital Banking Basic are summarized in the following bullets and are described in more detail in the sections below and in the Digital Banking Basic User Guide, Quickstart Guides and Implementation Documents.

- **Balance and Information Reporting.** Customer may use Digital Banking Basic to access, view and receive information about Customer Account(s).

- **Internal Transfers.** Customer may transfer funds from one Account at Bank to another.
- **Stop Payment.** Customer may stop payment on a check using the System.
- **Mobile Banking.** Users may access Account information and deposit Checks via Mobile Devices, as provided in sections 6 and 7 below.
- **Online Statements.** Customer may elect to receive electronic periodic statements to be posted on the System each month through a separate consent form Bank provides online.
- **Alert Services.** Customer may elect to receive informational alerts for selected Services delivered to the Mobile Device, voicemail box or email address Customer designates.
- **Bill Pay.** Users may pay bills online, subject to electronic terms and conditions that must be accepted on first login.

2) Balance Viewing and Accuracy of Online Information. Digital Banking Basic allows Customer to view and receive information about Customer's Account balance, activity, transactions and other information electronically. Account information changes frequently and is subject to updating, verification, and correction. Since the information may change during the delay between when the information was last sent to Customer or posted by Bank and when Customer receives or accesses the information, Bank assumes no responsibility for Customer's reliance on such information which is subsequently updated, verified or corrected. If Customer identifies and reports to Bank any information which requires updating or correction, Bank will promptly make any required corrections.

3) Internal Account Book Transfer Services. Customer may execute an Internal Transfer of funds using Digital Banking Basic. Each Internal Transfer shall be deemed to be a payment order and Bank's liability for processing such payment order is subject to the limitations on liability as set forth in Article III of this Agreement. Customer must communicate instructions to initiate an Internal Transfer through the System by using the Security Protocol. Internal Transfers shall be subject to the Cut-off times Bank establishes and any of Bank's information or formatting requirements, and Customer may schedule Internal Transfers for future dates. Bank may reject any Internal Transfer order for any reason in Bank's sole discretion (including, but not limited to, an overdraft in Customer Account). Uncollected funds may be accessed for transfers and check clearing, subject to applicable fees. Customer agrees to be liable for any Internal Transfer communicated to and executed by Bank in compliance with the Security Protocol, whether or not they are authorized. Customer shall have no right to cancel an Internal Transfer order once Customer submits it to Bank for processing.

4) Stop Payment Services.

- a) Customer may use Digital Banking Basic to transmit an order for Bank to stop payment on a check that Customer issued (each a "Stop Payment") on a Customer Account, and Bank agrees to provide such Service relating to Stop Payments subject to the terms herein.
- b) Bank is authorized to rely on Stop Payments received through the System and Customer agrees that a Stop Payment placed under this Service constitutes a writing pursuant to Section 4-403 of the UCC. Prior to Customer submitting a Stop

Payment order to Bank, Customer agrees to access the appropriate Account and database information through the System, review the applicable periodic statement for the Account, and determine whether the check to which the Stop Payment order relates has or has not already been paid. Customer acknowledges that a transaction search through Digital Banking Basic will not necessarily reveal whether a check has been paid until the Business Day after the Business Day on which the Stop Payment order is received by Bank. To place a Stop Payment, Customer must provide all information Bank requires (the "Required Information") and the Required Information must precisely identify a check Customer has issued on a Customer Account or the Stop Payment shall be void and not processed.

c) This Service is available only for checks drawn on a Customer Account and will not apply to cashier's checks, certified checks, drafts or other similar cash equivalent Items.

d) Bank will not be obligated to honor any Stop Payment and such Stop Payment will be void if the Item to which it relates has been paid or Bank has become otherwise obligated to pay such Item.

e) Unless otherwise set forth on the request for a Stop Payment, each stop payment placed hereunder will automatically expire six (6) months after the date submitted unless customer renews it for a similar period. Bank has no obligation to comply with any expired stop payment and shall have no liability for payment of a check on which the Stop Payment order has expired. No notice will be provided to Customer that an order is expiring.

5) **Alerts.** The types of alerts are described in the Implementation Document or a specific Service to which the alert applies. Customer is solely responsible for the selection, security, accuracy and accessibility of the email addresses and phone numbers provided for the alerts. Alerts are provided for Customer convenience and are based on Customer Account information, which may be updated throughout the day. Bank shall not be liable for any failure or delay or inaccuracy in any alerts. Customer is solely responsible for User use and reliance on such alerts.

a) Customer is not permitted to reply to any alerts by means of the mobile or online address to which such Alerts are delivered or otherwise. Customer acknowledges and agrees that alerts are sent without encryption or any security codes and that Bank shall not be responsible or have any liability for unauthorized access to an alert or the information therein.

b) Customer acknowledges and agrees that alerts are provided as a courtesy and do not have any effect on the validity of transactions initiated using any other Service or information provided to Customer as part of a Service or in connection with an Account, including periodic statements or information provided by other means and Customer obligations to monitor activity on Customer Accounts is not modified by Bank's providing, or failure to provide, alerts. Customer further acknowledges and agrees that Customer is responsible for accessing each Service as applicable to administer Customer transactions and information, notwithstanding whether an alert is provided, and alerts do not relieve Customer of Customer's responsibilities under the terms of any Service.

6) **Business Mobile Banking.** Based on the permissions established in Digital Banking Basic, Customer may use Mobile Banking in the

same manner Customer uses Digital Banking Basic, to: (a) view current balance information for Accounts linked to the Service; (b) review available transactions for Accounts; (c) view Account alerts and notifications; and (d) view payment history.

a) Customer will not use the Mobile Services in or for any illegal, fraudulent, unauthorized or improper manner or purpose and will only use it in compliance with all Applicable Laws, including all applicable state, federal, and international Internet, data, telecommunications, telemarketing, "spam," and import/export laws and regulations, including the U.S. Export Administration Regulations. Without limiting the foregoing, Customer will not use the Mobile Services to transmit or disseminate: (i) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom Customer does not otherwise have a legal right to send such material; (ii) material that infringes or violates any third party's intellectual property rights, rights of publicity, privacy, or confidentiality; (iii) material or data that is illegal, or material or data, as Bank determines (in Bank's sole discretion), that is harassing, coercive, defamatory, libelous, abusive, threatening, obscene, or otherwise objectionable, materials that are harmful to minors or excessive in quantity, or materials the transmission of which could diminish or harm Bank's or Bank's Service Provider's reputation; (iv) material or data that is alcoholic beverage-related, tobacco-related (e.g., cigarettes, cigars, pipes, chewing tobacco), guns or weapons-related (e.g., firearms, bullets), illegal drugs-related (e.g., marijuana, cocaine), pornographic-related (e.g., adult themes, sexual content), crime-related (e.g., organized crime, notorious characters), violence-related (e.g., violent games), death-related (e.g., funeral homes, mortuaries), hate-related (e.g., racist organizations), gambling-related (e.g., casinos, lotteries), specifically mentions any wireless carrier or copies or parodies the products or services of any wireless carrier; (v) viruses, Trojan horses, worms, time bombs, cancelbots, or any other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or personal information; (vi) any material or information that is false, misleading, or inaccurate; (vii) any material that would expose Bank or any of Bank's Affiliates or Bank's Service Provider, or any other third party, to liability; or (viii) any signal or impulse that could cause electrical, magnetic, optical, or other technical harm to the equipment or facilities of the Service Provider or any other third party.

b) Neither Bank nor the Service Provider will be liable for any errors in the content of information obtained or transmitted through the Mobile Services, or for any actions taken in reliance thereon (including, but not limited to, the type of alerts and other preferences Customer select).

c) Customer is responsible for any and all charges, including, but not limited to, fees associated with text messaging or data usage rates imposed by Customer's telecommunications carrier. Bank is not responsible for any damages resulting from Customer's failure to comply with any terms and conditions provided by any telecommunications carrier or any app store. Any losses or charges incurred through the loss of a Mobile Device or the safeguarding (or failure to adequately safeguard) of Login Credentials will remain Customer's sole responsibility.

d) In connection with Customer's use of Mobile Banking, Bank and its Service Provider may receive and may share with one another names, domain names, addresses, passwords, telephone and device numbers, the content of messages, data files and other data and information provided by Customer or from other sources in connection with the Mobile Services. Bank and the Service Provider will maintain reasonable safeguards to protect the User information from unauthorized disclosure or use, but Bank reserves the right to use and disclose the User information as reasonably necessary to deliver the Mobile Services and as otherwise permitted by law, including, without limitation, compliance with court orders or instructions from a government agency, to protect the personal safety of subscribers or the public, to defend claims, and as otherwise authorized by Customer. Bank and the Service Provider also reserve the right to monitor the use of Mobile Banking for purposes of verifying compliance with Applicable Law, this Agreement and any applicable license, but disclaim any obligation to monitor, filter, or edit any content.

e) It is important that Customer understands the limitations of the Mobile Services, including but not limited to the following: (i) because Mobile Banking is accessible only through Customer's Mobile Device, Customer's access to the Mobile Services may be limited by the service provided by Customer's telecommunications carrier; (ii) there may be technical or other difficulties related to Mobile Banking. These difficulties may result in loss of data, personalized settings or other the Service interruptions. Bank does not assume any responsibility for the timeliness, deletion, or misdelivery of any user data, failure to store user data, communications or personalized settings in connection with Customer's use of a Mobile Banking; nor for the delivery or the accuracy of any information requested or provided through Mobile Banking; (ii) Bank reserves the right to block access or delete the Mobile Banking software from Customer's Mobile Device if Bank or Bank's Service Provider has reason to believe Customer is not complying with this Agreement, or has reason to suspect Customer's Mobile Device has been infected with malicious software or virus.

7) Business Mobile Remote Deposit Capture. This Mobile Service ("Mobile Deposit") is designed to allow Customer to make deposits to Accounts from remote locations by capturing Check Images and delivering the Check Images and associated deposit information to Bank or its Service Provider. Once Customer has requested and enrolled in Mobile Deposit, identified a Primary Administrator and set-up Users, Customer will be able to take pictures of Checks for deposit. Customer will need to provide an image from both the front and the back of the Check and provide the information required. Notifications will be sent to let Customer know Customer's transaction was successful.

a) Check Requirements. In order to be eligible to be transmitted to Bank through Mobile Deposit, a Check must meet all of the following requirements:

- i. The Check must be a paper Check made payable only to Customer's business;
- ii. The paper Check must be payable on demand and drawn on or payable in U.S. dollars at a financial institution whose corporate headquarters is located in the United States;

iii. The paper Check must not have been previously deposited with any financial institution, or deposited to the Account or any other account or used as a source document for any electronic image that has been transmitted to any financial institution; and

iv. The paper Check cannot be future or postdated.

b) Impermissible Checks. Customer will not transmit any Checks that violate any of the terms of this Agreement or the Account Agreement. Customer may not image and deposit any of the following types of Checks:

i. Checks payable to any person or entity other than the person or entity that owns the Account that the Check is being deposited into;

ii. Checks containing an alteration on the front of the Check, or which Customer knows or suspects, or should know or suspect, are fraudulent or otherwise not authorized by the owner of the account on which the Check is drawn;

iii. Checks previously converted to a substitute check, as defined in Regulation CC;

iv. Checks drawn on a financial institution located outside the United States;

v. Checks that are remotely created checks, as defined in Regulation CC;

vi. Checks not payable in United States currency;

vii. Checks dated more than six (6) months prior to the date of deposit;

viii. Checks that have previously been submitted through the Mobile Service or through a remote deposit capture service offered at any other financial institution;

ix. Checks that are drawn or otherwise issued by the U.S. Treasury Department.

c) Endorsements and Procedures. **Customer must restrictively endorse any Check transmitted through Mobile Deposit as "For mobile deposit only, Midland States Bank"** or as otherwise instructed by Bank. Customer agrees to follow any and all other procedures and instructions for use of the Mobile Service as Bank may establish from time to time.

d) Receipt of Items. Bank reserves the right to reject any Check Image transmitted through Mobile Deposit, at Bank's discretion. Bank is not responsible for items Bank does not receive or for images that are dropped or intercepted during transmission. An image of a Check will be deemed received when Customer receives a confirmation from Bank that Bank has received the image. Receipt of such confirmation does not mean that the transmission was error free or complete.

e) Disposal of Checks. Customer must mark each Check "VOID", or otherwise render it incapable of further transmission, deposit, or presentment and put the Checks under lock and key until Customer's business destroys them.

f) Promises Customer Makes to Bank. In addition to any warranty Bank must make in connection with collection of the Checks, Customer warrants to Bank:

i. Customer will only transmit eligible Checks;

ii. Check Images will meet Bank's image quality standards in effect from time to time and the image of the

MICR Data will be clear and easily readable;

iii. Customer will not store or make a back-up copy of any electronic item;

iv. Customer will not transmit an image or images of the same Check to Bank more than once and will not deposit or negotiate, or seek to deposit or negotiate, such Check with any other party;

v. Customer will not deposit or re-present the original Check to any other party;

vi. All information Customer provides to Bank is accurate and true, including that all images transmitted to Bank accurately reflect the front and back of the Check at the time it was scanned.

g) **Deposit Limits.** Bank may establish limits on the dollar amount and/or number of Checks or deposits from time to time. If Customer attempts to initiate a deposit in excess of these limits, Bank may reject the deposit.

III. GENERAL TERMS OF THE SERVICE

1) **Fees and Charges.** Unless otherwise agreed by Bank in writing, Customer shall pay Bank the fees, charges and assessments set forth for the Service stated in the most current fee schedules and other fee disclosures provided to Customer (including periodic Account statements). The fee schedule shall be deemed accepted by Customer upon provision of the Service to Customer. Bank may change the amount or type of service charges from time to time. Customer authorizes Bank to debit Customer's Account(s) with Bank for any and all fees, expenses or other charges owed by Customer to Bank under this Agreement.

2) Confidentiality.

a) **Data Security.** Bank shall maintain physical, electronic, and procedural safeguards to keep Customer's Confidential Service Information secure.

b) **Use of Confidential Service Information.** All uses of the Service in accordance with the Security Protocols will be deemed to be authorized by and binding on Customer. Customer's failure to protect Login Credentials and Account numbers may allow an unauthorized party to (i) use the System; (ii) access Customer's electronic communications and financial data; (iii) send orders and transfer funds from Accounts; or (iv) receive confidential information from Bank.

3) **Compliance.** Bank and Customer will each comply with all Applicable Law in connection with use of the System. Unlawful Internet Gambling Notice: Restricted transactions as defined in Federal Reserve Regulation GG are prohibited from being processed through the Account(s). Restricted transactions generally include, but are not limited to, those in which credit, Electronic Funds Transfers, checks, or drafts are knowingly accepted by gambling businesses in connection with the participation by others in unlawful Internet gambling.

4) Instructions and Communications.

a) Customer may elect to send or receive instructions or reports from Bank related to the Service via email or other electronic transmission ("Electronic Transmission"). Customer acknowledges that such Electronic Transmissions are an inherently insecure communication method due to the possibility of error, delay and observation or receipt by

unauthorized personnel. Bank may rely in good faith on Customer's instructions regarding how and to what number or email address Electronic Transmissions should be sent and may rely on any Electronic Transmission that it reasonably believes to have been initiated by Customer. Should Customer elect to send or receive Electronic Transmissions to or from Bank, Customer assumes all risks, and Bank shall not be liable for any loss, that results from the nonreceipt, disclosure or alteration of any such Electronic Transmission.

b) Bank may provide Customer the option of entering into this Agreement or any Implementation Documents with a digital signature. Customer hereby agrees that Customer's use of such digital signature shall bind Customer to the terms and conditions of the applicable agreement, addendum or form.

c) In addition, in order for Bank to service the Account, mitigate fraud or to collect any amounts owed to Bank, Bank or its Service Provider may from time to time make calls and/or send text messages to Customer at any telephone number(s) associated with the Account, including wireless telephone numbers that could result in charges to Customer. The manner in which these calls or text messages are made may include, but is not limited to, the use of prerecorded/artificial voice messages and/or an automatic telephone dialing system.

d) Customer may have Accounts that require multiple signers to execute transactions. Customer agrees that Bank is authorized to complete each transaction initiated electronically by one User using the Security Protocol, including but not limited to, transfer of funds, credit payments and issuances of Checks or electronic payments.

5) **Transactions on Non-Business Days/Cut-off Times.** Transactions, deposits, Payment Orders, Entries or other requests by Customer received by Bank on a non-Business Day or after established Cut-off may be treated by Bank as received on the next Business Day unless otherwise required by Applicable Law. Bank may change any Cut-off time or other deadline at any time.

6) **Account Communications and Review Period.** At Customer's election, Bank will either provide to Customer electronically through Digital Banking Basic or by mail at Customer's current address in Bank's files, periodic statements, notices and other information regarding the Account and Account activity.

a) Customer acknowledges that it is in the best position to discover erroneous charges, payments, missing or incorrect deposits, credits or debits or other entries to Customer's Account or other Account problems. Customer agrees to promptly examine each periodic statement, record, notice, canceled check and other items provided or made available to Customer (whether originals, images, copies or in other formats) and to promptly notify Bank of any error or Account problem.

b) Customer shall, within a reasonable time, which in no event shall be greater than thirty (30) calendar days following the day Bank first mails, electronically transmits or otherwise makes data available to Customer, notify Bank of any error or discrepancy between Customer's records and any Bank notice or periodic statement, or any transaction or transfer Customer believes was not authorized. Such notifications are to be made by calling Bank or writing to Bank at the telephone number or address listed on Customer's periodic statement. However, Bank encourages Customer to review periodic statements on a

regular basis and recommends that Customer report any inconsistencies with respect to such periodic statements within fifteen (15) calendar days of discovery.

c) If Customer fails to notify Bank of an unauthorized transaction within the review period, Customer agrees that the failure to report any such error or unauthorized transaction shall relieve Bank of any liability for the unreported erroneous or unauthorized transaction and Bank will not be obligated to re-credit or refund the amount of the error or Account problem.

7) Disclaimer of Warranties. BANK MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN LAW OR IN FACT, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE AND OF MERCHANTABILITY, EITHER TO CUSTOMER OR TO ANY OTHER PARTY, WITH RESPECT TO THE SERVICE PROVIDED BY BANK OR ITS SERVICE PROVIDERS OR WITH RESPECT TO SOFTWARE PRODUCTS PROVIDED OR MADE AVAILABLE TO CUSTOMER FOR ITS USE IN CONNECTION WITH THIS AGREEMENT AND DIGITAL ONLINE BANKING BASIC.

8) Standard of Care. Bank will use commercially reasonable care and will exercise good faith in providing the Service to Customer. Bank's care is to be evaluated based on reasonable commercial banking standards prevailing in Bank's industry and location for similarly situated commercial banks and Applicable Law. Occasional unintentional deviations by Bank from the procedures set forth in this Agreement shall not be deemed a failure to exercise reasonable care in respect to the transactions in which the deviations occur. Clerical errors or mistakes in judgment shall not constitute failure to exercise reasonable care. Further, reliance on any oral, telephonic, electronic, written or other communication believed in good faith to have been given by or on behalf of Customer will in no event constitute a failure to exercise reasonable care.

9) Limitation of Bank's Liability. Customer acknowledges that Bank's fee for the Service is very small and consequently Bank's willingness to provide Digital Banking Basic is based on the liability limitations contained in this Agreement.

a) Bank's liability related to Digital Banking Basic shall be limited exclusively to actual proven damages arising directly from its own gross negligence or willful misconduct or its failure to exercise good faith. Bank will not, under any circumstances, be liable for any special, incidental, indirect, consequential, punitive or similar losses or damages, whether or not the likelihood of such losses or damages was known by either party at the time Customer first obtains the Service from Bank, and whether such losses or damages arise from tort, contract or otherwise.

b) Bank's cumulative liability to Customer for all loss or damage arising from or relating to this Agreement and Digital Banking Basic, regardless of the form of action, is limited to direct losses attributable to Bank's gross negligence, willful misconduct or failure to exercise good faith and is limited to an amount not to exceed twelve (12) times the fees paid by Customer during the month immediately preceding the month in which the loss or damage was incurred.

c) Any claim known or unknown for liability arising under this Section shall be made within twelve (12) months after the date the claim arises.

d) Bank shall not be liable for any damage, cost, loss, liability or delay caused by Bank acting in accordance with Applicable Law, accident, strike, fire, flood, war, riot, terrorist act, pandemics and other national emergencies, cyber-attacks, cyber warfare, equipment breakdown, electrical or mechanical failure, acts of nature, any cause which is attributable to a third party, or any other cause or event that was beyond Bank's reasonable control. Bank has no responsibility and will incur no liability for any act or failure to act by any other Bank, intermediary or any other third party including any failure, delay or error by any Federal Reserve Bank or other intermediary bank in timely, presenting data or checks to Bank.

10) Dispute Resolution.

a) **Governing Law.** Except as otherwise provided herein; this Agreement shall be governed by the laws of the State of Illinois, without regard to conflicts of law principles, including the Uniform Commercial Code as in effect in the State of Illinois from time to time.

b) **Jury Trial Waiver.** To the fullest extent permitted by law, Bank and Customer hereby agree to waive trial by jury in any judicial proceeding involving, directly or indirectly, any matter (whether in tort, contract or otherwise) in any way arising out of, related to or connected with the Service or this Agreement. Bank and Customer represent and warrant to each other that this jury trial waiver is knowingly, willingly and voluntarily given.

c) **Arbitration.** Any dispute, controversy or claim arising out of or relating to this Agreement, including a breach of this Agreement, shall be decided by arbitration conducted in the United States of America (except as Customer and Bank expressly agree otherwise) in accordance with the United States Arbitration Act (Title 9, U.S. Code) under the Commercial Arbitration Rules of the American Arbitration Association. Under these procedures, the dispute, controversy or claim shall be submitted to a neutral person for determination in place of a trial before a judge or jury. Judgment upon the decision rendered by the arbitrator may be entered in any court having jurisdiction.

d) **Jurisdiction and Venue.** Customer consents to the jurisdiction of the courts of the State of Illinois, waives any argument that such venue is inconvenient and agrees to bring litigation commenced in connection with this Agreement in any state or federal court located in the State of Illinois.

e) **Adverse Claims.** If Bank receives an adverse claim against any Account, and Bank reasonably believes that it will not be protected if the claim is ignored, Customer agrees that Bank may place a hold on the affected Account. Any such hold will remain in place only so long as reasonably necessary to resolve the claim or employ legal remedies to allow a court to decide such claim. Assuming compliance with this Section, Bank shall have no liability for dishonored transactions due to the hold, and Customer agrees to reimburse Bank all costs, including attorney fees, incurred due to such adverse claim.

11) Notices.

a) All written notices to Bank shall be delivered or mailed to Treasury Operations at Midland States Bank, 1201 Network Centre Dr., Effingham, Illinois 62401-4602, or at such other address as Bank may specify in writing or they may be emailed

to customerservice@midlandsb.com, unless Electronic Transmission is not permitted.

b) Notices sent to Customer shall be delivered or mailed to Customer's current lead Account address or other known address if deemed more appropriate by Bank under the circumstances. Notices may be delivered in electronic format, including posting to Bank's Website, if requested or appropriate.

12) Termination.

a) The Service may be terminated by either party upon ten (10) Business Days' prior written notice to the other.

b) Bank may also terminate or suspend the Service without notice to Customer if any of the following occurs: (i) a material adverse change occurs in Customer's business or financial condition; (ii) Bank has reason to believe that Customer has engaged in fraudulent or illegal activity; (iii) Customer fails to maintain balances in Accounts sufficient to cover overdrafts; (iv) Customer violates the terms of this Agreement or any financing arrangement with Bank; (v) Customer fails to comply with Bank's Security Protocol or fails to provide financial information reasonably requested by Bank; (vi) Bank determines it is impractical or illegal to provide the Service because of changes in laws, regulations or rules; (vii) Bank, in good faith, is unable to satisfy itself that the Service has been properly authorized by Customer; (viii) Bank, in good faith, deems itself insecure, believes such Service may create a risk of financial loss for Bank or result in an unacceptable credit exposure to Bank; or (ix) Customer has not used the Service for ninety (90) days.

c) Upon termination, Customer will immediately return to Bank or destroy the originals and all copies (in all formats and media) of software programs, if any, that were licensed to it as part of the Service, all Quick Start Guides and User Guides, and security and access devices. Any licenses granted to Customer with respect to the terminated Service under the Service Documentation will automatically terminate.

d) Article III of this Agreement will survive any termination of the Agreement and the Service, along with any indemnification undertaking or limit of liability.

13) Miscellaneous.

a) This Agreement is binding upon and will inure to the benefit of the parties and their respective legal representatives, successors and permitted assigns. This Agreement is not for the benefit of any other person except as explicitly provided herein, and no other person shall have any right against Customer or Bank under this Agreement.

b) To the extent possible, each provision of this Agreement shall be interpreted in such manner as to be effective and valid under Applicable Law, but if any provision shall be held to be invalid, illegal or unenforceable, such provision shall be ineffective only to the extent of such invalidity, illegality or unenforceability, without rendering invalid, illegal or unenforceable the remainder of any such provision or the remaining provisions of this Agreement.

c) Bank may at any time assign or delegate its rights and duties under this Agreement. Customer may not assign or transfer its rights or obligations hereunder to any other person or entity without Bank's written consent, whose consent shall

not be unreasonably withheld. Any purported assignment of this Agreement or Digital Banking Basic without Bank's prior written consent is void.

d) A waiver by Bank or Customer of any term or provision shall not be construed as a waiver of such term or provision at any other time, or of any other term or provision. Bank's waiver of the enforcement of any of the terms of this Agreement with respect to any transaction or series of transactions will not affect Bank's right to enforce any of its rights with respect to other Customers or to enforce any of its rights with respect to later transactions with Customer.

14) **Third Party Information and Linked Websites.** Financial market data, quotes, news, research and other information developed by third parties and transmitted by Bank may be available on the Website (or sites linked to the Website). The posting of such information or data on the Website (or sites linked to the Website) will not be a recommendation by Bank that a particular service or transaction is suitable or appropriate for Customer. Although Bank strives to insure that information Bank obtains from third parties is reliable, Bank does not guarantee the accuracy, completeness or timeliness of third-party Information, nor is Bank in any way responsible for any decision Customer makes or action Customer takes in reliance on such information.