



Treasury Management Master Agreement

This **Treasury Management Master Agreement**, including attachments, governs your use of **business digital banking and related products and services** (all of which is referred to herein as “Business Digital Banking”, “Services” or “BDB”). This document and all agreements and attachments that are a part thereof will be referred to as the “Master Agreement” which by using **Business Digital Banking**, you agree in all respects and as to all provisions. As such, please read this Master Agreement carefully and keep a copy of this Master Agreement for your records.

Business Digital Banking

Definitions – These apply to all provisions and sections of this Master Agreement:

You, Your or Customer – The person(s) subscribing to or using **Business Digital Banking**.

We, Us, Our or Bank – Refers to First Bankers Trust Company, N.A. and any agent, [independent contractor], designee, or assignee thereof that may be involved in the provision of **Business Digital Banking**.

Business Day - Any calendar day other than a Saturday, Sunday, or federal holiday recognized by the Bank. Transactions are processed by the Bank only on all Business Days that the Federal Reserve Bank is operating and open for business.

Business Day Cut-Off- The Bank’s primary banking offices are located in Illinois and its Business Day is based on the Central Time zone. For posting purposes, the Bank will process all transactions successfully completed by 4:00 P.M. on that Business Day. Transactions completed after 4:00 P.M., including transfers, will be processed on the following Business Day. Transactions requiring earlier processing, i.e., ACH Payroll, may require earlier posting time requirements. You may wish to inquire as thereto.

Confidential Information means all “non-public personal information” (as defined in the Gramm Leach Bliley Act) regarding a Customer which may include social security numbers, credit scores and income.

Services means any and all of the programs, services or Customer offerings the Bank makes available to its Customer, including those list for BDB (below), as now or hereafter amended or supplemented.

About Business Digital Banking

The Bank’s **Business Digital Banking** provides a complete array of financial services to its customers. Among other things, BDB allow you to access 24/7 your data with full statements and complete transaction detail.

The **Business Digital Banking** platform that is accessible to our customers via the internet, currently consists of the following:

Account inquiries, balances, rates, etc. Wire Transfer Requests

Historical transactions View Detailed Transactions

Secure E-mails & File transfers DDA or Savings Statements

Transaction Downloads Various bookkeeping services

Account transfers Payments to our loan accounts

ACH Credit Origination Direct Deposit Originations

ACH Debit Origination [EFTPS] Credit Origination

Participation or use of some of these systems will require that you sign a specific agreement that governs those particular Services. Those Agreements are part of this Master Agreement.

Registration Process

To avail yourself of our **Business Digital Banking** services require that you complete an initial registration process. This involves signing this Master Agreement, our online acceptance of the Master Agreement, and completing a Treasury Management Master Application (“Application”) which will identify all the information that will be needed to enable the services. In addition,

should you utilize the wire transfer and ACH features of **Business Digital Banking** you will be required to complete and sign the Bank's Wire Transfer and ACH Agreements. As part of this process, Bank personnel will verify the information you submit for accuracy and authorizations. Any changes to your initial Application must be made in writing by an authorized Customer representative. It is the Customer's responsibility to notify the Bank of any account, employee and/or transaction authorization changes.

Log-On Security

Security is very important to the **Business Digital Banking** system. At the time you request the service, you will select a unique "Client ID" that will be used to gain access to the system. In addition, each employee that has been given the right to access account information will be given his/her own "Employee ID" and "Password". The right to access account information and/or transfer funds is Employee ID dependent. Prior to system activation, Bank personnel will verify your identity and authorizations to information associated with the accounts that you requested be tied to the service.

To help prevent unauthorized access and ensure the security of your accounts, the Bank will end your online session if we have detected no activity for 10 minutes. This is to protect you in case you leave your computer unattended after you have logged on. When you return to your computer, you will be prompted to re-enter your Employee ID and password.

Because your Employee ID and password are used to access accounts, you should treat it as you would any other sensitive personal data. You should carefully select a password that is hard to guess. Keep your password safe. Memorize your password, keep it to yourself, and never tell it to anyone else. You should change your password periodically, such as every 90 days.

PFM (Personal Financial Manager) Statement

The Bank is not responsible for the security, accuracy, or reliability of 3rd party personal financial managers or online financial management account services that require our Customers to provide their account login ID and password or any other personally identifiable information to access information held by the Bank. The Bank recommends that you not provide account login ID and passwords to any third party.

eWarning

The Bank will NEVER request from a Customer, by e-mail, text, or phone call, any Confidential Information such as an account number, social security number, PINs or passwords. Never give out Confidential Information unless you have originated a voice or in-person conversation and we are requesting this information for identification purposes. Also, never give your PIN or password to anyone, including Bank staff. Emails from presumably legitimate sources such as a bank or the FDIC can be fraudulent. When accessing our website, only enter directly at www.firstbankers.com in your browser. Never allow another website (such as a search engine, other website or bookmark) to transfer you to our website. Websites can be fake if not entered directly.

Accounts

You may request access to any account of which you are a signer or owner. If you desire Services that allow you to initiate payments or transfers from your account, you will need the required withdrawal authority over the account to do so. By using Business Digital Banking Services, you agree to maintain one or more accounts with us and to keep sufficient balances in any account to cover any transaction and fees that are ultimately approved by or related to BDB. If any accounts added to the Services are jointly held or have multiple signers, you agree that access to the information and all transactions initiated by the use of your [Employee ID] and passwords are authorized unless we have been notified to cancel the Service.

Fees for the Business Digital Banking

A Fee Schedule is attached to this Agreement and may be modified from time to time at our discretion. You will be notified of any changes in the Business Digital Banking Fee Schedule at least 30 days prior to the effective date of the change.

Limitation of Liability

Neither the Bank or its affiliates, nor any party involved in creating, producing, or delivering BDB Services is liable for any direct or indirect, incidental, special, consequential, punitive or other damages of any kind resulting from access to BDB. Neither the Bank nor its service providers will be responsible for any direct or indirect, special, incidental, consequential, punitive or other damages arising in any way due to the installation, use, failure, malfunction or maintenance of the equipment, software, online access software or service, or Internet browser or software associated with the Services. The Bank is not responsible for any electronic virus or viruses that you may encounter in using any of the Services. We encourage all of our Customers to install on their computers reliable virus protection products to detect, block, and remove viruses.

Customers have the ability to access information about their Bank accounts through electronic means (Telephone Banking, Online Banking, ATMs, etc.). Although the Bank tries to provide accurate and timely information to its Customers via electronic means, there may be inadvertent technical occurrences beyond the Bank's control which would cause electronic access to be unavailable from time to time. The Bank is not responsible for any losses resulting from the inability of Customers to access their accounts and/or perform transactions during any such force majeure events. Similarly, the Bank is not responsible for any losses during periods when its electronic systems are shut down for maintenance, repairs, upgrades, or other necessary actions.

Cancellation of Business Digital Banking

Your Business Digital Banking Services may be cancelled at any time by the Bank in whole or in part without prior notice for any reason or for no reason at the sole discretion of the Bank. You will remain responsible for all transactions approved pursuant to the Services prior to cancellation, and for any other transactions associated with the Services. The Bank's right to termination includes the right to terminate any and all of the Services being provided by the Bank to the Customer for any reason or no reason at all.

Balance Inquiries and Transfers Limitations

You may use **Business Digital Banking** to check the balances of your accounts and to transfer funds among your accounts. According to Federal regulations, you may not make more than six (6) pre-authorized or automatic transfers or debit transactions from a Money Market Deposit Account or Savings Account during a given monthly statement period. There are no limits on the number of transfers or debits you can make from a Checking Account.

Balances shown in your accounts may include [deposits subject to verification by us]. The balance may also differ from your records due to deposits in progress, outstanding Checks or other withdrawals, payments or charges. A transfer request may not result in immediate availability because of the time required to process the request. If you have questions as to the foregoing, please contact us.

Errors and Questions

In cases of errors or questions concerning transactions completed with **Business Digital Banking** call **Business Digital Banking** Service Support at (877) 228-8000.

Compliance

All bill payments, transfers and other services provided by the Bank will be subject to and will comply with applicable law, including without limitation, any applicable federal and state laws, codes, rules and regulations, such as the Internal Revenue Code and the operating circulars of the Federal Reserve System (collectively, "Applicable Law"), the operating rules of networks, associations and systems, such as the rules of the National Automated Clearing House Association and any regional ACH (collectively, "Applicable Rules") that we may use from time to time to provide the Services, as well as Office of Foreign Assets Control (OFAC*) requirements ("OFAC Requirements"), each as amended from time to time. You acknowledge that no bill payments, transfers or other Services will be initiated by you that violate any Applicable Laws, Applicable Rules, or OFAC Requirements.

[*OFAC is a division of the United States Treasury Department and is mandated to implement and enforce economic sanctions imposed by the U.S. Government against hostile foreign countries, their nationals, or other "specially designated" individuals or entities. These sanctions restrict banks and other businesses from doing business with those designated countries and entities.]

Separation of Duties

The [System] enables you to require that certain Services or [transactions] be pre-approved before they can be processed. In order to increase your internal security, we recommend that you put in place dual controls to initiate transactions such as Funds Transfers, ACH Originations, Wire Transfers, and Bill Pay.

Commonly Controlled Entities

You represent and warrant that each of the entities listed on your Application is under common ownership and/or control with you (each, a "Commonly Controlled Entity"), and each Commonly Controlled Entity has signed a [Business Digital Banking] Application and has agreed to the terms of Digital Banking. You acknowledge and agree that, by including an entity on the Application as a Commonly Controlled Entity, (i) your Accounts will be accessible by the Commonly Controlled Entities and you will have access to the Accounts of the Commonly Controlled Entities, and (ii) your (and your Commonly Controlled Entities') Primary Administrator, [Secondary Administrators, and Authorized Users] will be able to transfer funds among the Accounts of

each of the Commonly Controlled Entities, and (iii) all Checks issued to payees thru the Bill Pay function for any of the Commonly Controlled Entities will have printed on the Check the name of the entity in which the Account has been established. You agree that your Primary Administrator will be the same individual for each Commonly Controlled Entity (which individual shall be an officer of your company and of each Commonly Controlled Entity). You also agree that such Primary Administrator will only designate Secondary Administrators and Authorized Users who are officers or employees of your Company and of each Commonly Controlled Entity. You agree to defend, indemnify and hold us harmless from and against any and all actions, losses, liabilities, claims, damages or expenses (including, without limitation, attorneys' fees, court costs and expenses) arising from or related to (i) your designation of an entity as a Commonly Controlled Entity, (ii) a Commonly Controlled Entity's designation of you as being commonly owned/controlled with it, or (iii) the transfer of funds from an Account maintained by you to an Account maintained by a Commonly Controlled Entity, or vice versa. You and all Commonly Controlled Entities shall be jointly and severally liable for this indemnity obligation which shall survive termination of this Master Agreement.

Liability for Business Customers

You represent and warrant that all of your Accounts that can be accessed under Business Digital Banking are not Accounts established primarily for personal, family or household purposes, but, rather, for business or commercial purposes.

Additional risk is associated with Customer's use of Online Banking and Business Digital Banking. More specifically, in using these Services you will not have the benefit of any consumer laws limiting liability for the unauthorized [use of your Business Digital Banking]. You accept and agree to assume this additional risk and the greater measure of liability associated with the use of Business Digital Banking. Unless otherwise provided by Applicable Law, you are liable for transactions you did not authorize if we processed the transaction, with due care, in good faith and in compliance with commercially reasonable security procedures to which we both agreed. You agree to defend, indemnify and hold us harmless from and against any and all actions, losses, liabilities, claims, damages or expenses (including, without limitation, attorneys' fees and court costs and expenses) arising from or related to your access or use of any Services.

If you have reason to believe that your Primary Administrator User ID, Password, or [token] has been lost, stolen or otherwise compromised (or may be compromised) or that a bill payment, funds transfer or other Service has been or may be made with your Primary Administrator User ID and Password without your permission, you must call us at (217) 228-8018 to so advise us. In such an event, you should also immediately change your Primary Administrator User ID and Password. You will not be liable for any unauthorized transaction that occurs after we receive your notice and have had a reasonable opportunity to act on it, unless we can establish that your failure to comply with this Agreement or to otherwise exercise ordinary care contributed to the unauthorized transaction.

If you have reason to believe that any User ID has been lost, stolen or otherwise compromised (or may be compromised) or that a bill payment, funds transfer or other Service has been or may be made with your User ID without your permission, you must contact your Primary Administrator or any Secondary Administrator as soon as this information comes to your attention. Upon being so notified, your Primary Administrator or Secondary Administrator, as applicable, must deactivate, and has the sole responsibility for deactivating, any such User ID. You acknowledge and agree that, except as otherwise provided by Applicable Law, we will not be liable for any transaction that occurs through the use of any User ID (including Secondary Administrator) which you may or may not have authorized.

Disclosure of Account Information to Third Parties

Information will only be given to third parties about your Account(s) or the transaction(s) you make if at least one of the following applies:

It is necessary to complete the transaction,
to verify the existence and condition of your Account or comply with a governmental agency or court order.
If you give permission to the Bank, which we may require to be in writing.
To collect information for internal use or for the use of the Bank's service providers, servicingagents and contractors concerning the Bank's electronic funds transfer service.
It involves a claim by or against the Bank concerning a deposit to or withdrawal from your Account.
Where otherwise required or permitted under Applicable Law.

No Signature Requirements

When any payment or other on-line service generates items to be charged to your account, you agree that we may debit the designated account, or the account on which the item is drawn, without requiring your signature on the item and without any

notice to you, unless we have agreed otherwise.

Virus Protection

The Bank is not responsible for any electronic virus or viruses that you may encounter. We encourage our Customers to routinely scan their system using a reliable virus product to detect, block, and remove any viruses. Undetected or unrepaired viruses may corrupt and destroy your programs, files and even your hardware. Additionally, you may unintentionally transmit the virus to other computers.

Wide Text Statements and other Special Printing Instructions

For certain accounts, the Bank's statement format may be wider than your default printer setting support and may not automatically print correctly or cut off the right-hand side of the page.

Termination

You may terminate the use of **Business Digital Banking** by contacting the Bank in writing by mail or personal delivery. If your account is closed or restricted for any reason, **Business Digital Banking** accessibility will automatically terminate.

Governing Law

This Master Agreement shall be governed by and construed in accordance with the laws of the State of Illinois.

Assignment

This Master Agreement may not be assigned to any other party by you. The Bank may assign or delegate this Master Agreement, in part or whole, to any third party.

Ownership of Material

The Bank's **Business Digital Banking** is a proprietary product. Its unauthorized reproduction or use in whole or part is prohibited.

Amendments

Terms and conditions of this Master Agreement may be amended by us, in our discretion, in whole or part at any time with 30 days written notification prior to the change taking effect. If you do not agree with the change(s), you must notify the Bank in writing prior to the effective date to cancel your use of Business Digital Banking. Amendments or changes to term(s) or condition(s) may be made without prior notice if the change does not result in higher fees, more restrictive service use, or an increase in your liability.

Alerts

Your enrollment in Business Digital Banking and/or Mobile Banking includes receiving transaction alerts and notifications ("Alerts"). Alerts are electronic notices from us to you that contain transactional information about your Account(s). "Account Alerts" and [Additional Alerts] must be managed and/or added online through the Services. We may [add] send new Alerts from time to time, or cancel old Alerts. We may notify you when we cancel Alerts, but we are not obligated to do so. The Bank reserves the right to terminate its Alerts service at any time without prior notice to you. However, you will be notified if such Service is terminated.

Methods of Delivery

We may provide Alerts through one or more channels ("**endpoints**"): (a) a mobile device, by text message, (b) a mobile device, by push notification; (c) an email account, by an e-mail message; or (d) your **Bank** Online Banking message inbox. You agree to receive Alerts through these endpoints, and it is your responsibility to determine that each of the service providers for the endpoints described in (a) through (c) above supports the email, push notification, and text message Alerts provided through the Alerts service. Please be advised that text or data charges or rates may be imposed by your endpoint service provider. Those charges are yours and not our responsibility. Alert frequency varies by Account [and preferences]. You agree to provide us a valid mobile phone number or email address so that we may send you Alerts. If your email address or your mobile device's number changes, you are responsible for informing us of that change. Your Alerts will be updated to reflect the changes that you communicate to us with regard to your primary and secondary email addresses or mobile device number.

Alerts via Text Message

To stop Alerts via text message, **text "STOP" to 99588 at anytime**. Alerts sent to your primary email address will be unaffected by this action. To restore Alerts on your mobile phone, just visit the Alerts tab in **First Bankers Trust Company, N.A.** Online Banking. In case of questions please contact Customer service at **877-587-8018**. Our participating carriers include (but are not limited to) AT&T, SprintPCS, T-Mobile®, U.S. Cellular®, Verizon Wireless, MetroPCS.

Limitations

The Bank provides Alerts as a convenience to you for information purposes only. An Alert does not constitute a bank record for the deposit or credit account to which it pertains. We strive to provide Alerts in a timely manner with accurate information. However, you acknowledge and agree that your receipt of any Alerts may be delayed or prevented by factor(s) affecting your mobile phone service provider, internet service provider(s) and other factors outside the Bank's control. We neither guarantee the delivery nor the accuracy of the contents of each Alert. You agree to not hold **the Bank**, its directors, officers, employees, agents, and service providers liable for losses or damages, including attorneys' fees, that may arise, directly or indirectly, in whole or in part, from (a) the non-delivery, delayed delivery, or misdirected delivery of an Alert; (b) any inaccurate or incomplete information in an Alert; or (c) your reliance for any purpose on, or use of, the information provided in an Alert.

Alert Information. Because alerts delivered via a short message service ("SMS"), email and push notifications are not encrypted, we will never include your passcode or full account number in such Alerts. You acknowledge and agree that Alerts will not be encrypted and may include your name and some information about your Accounts which anyone with access to your Alerts will be able to see.