Digital Banking Service Agreement

April 2026

TABLE OF CONTENTS

NOTICE TO ALL DIGITAL BANKING CUSTOMERS: Unless specifically stated otherwise, applying for one or more deposit products and/or agreeing to this Agreement automatically enrolls you in all Digital Banking services (if, and when each service becomes available, for example online banking will become available after mobile banking), including, but not limited to, the eDocuments Service (as set forth in Section 29 below). This means that you will not be able to unenroll in one or more Digital Banking services; however, except for the eDocuments Service, you may choose not to use one or more Digital Banking services.

For example, you are automatically going to receive electronic deposit account statements that can be accessed via Digital Banking. We do not offer paper deposit account statements. You cannot unenroll in the eDocuments Service and continue to use other Digital Banking services. In the event you instruct us that you do not want electronic deposit account statements, notices and/or tax documents, we will close all your deposit accounts and terminate your Digital Banking services.

Another example, if, and when, Mobile RDC Service becomes available, you can choose not to deposit check images through Mobile Banking.

Consent to Receive Communications to Your Mobile Device

By accepting these terms, you consent to receiving text messages and autodialed, prerecorded or artificial voice ("PAV") calls to any number(s) you provide, and you acknowledge that, in any event and to the extent not prohibited by applicable law, by voluntarily providing your telephone number(s) to us, you expressly agree to receive autodialed, PAV messages and texts from us, including from our affiliates and third-parties calling on our behalf. You further certify that you are the owner of the mobile device and specified account. The frequency of messages sent via SMS text will vary depending on the type and frequency of transactions you initiate via Digital Banking. Message and data rates may apply. Mobile carriers are not liable for delayed or undelivered messages.

Right to Opt Out. You generally may opt-out of autodialed, PAV calls or text messages from us at any time, subject to applicable law. To opt-out of autodialed and PAV calls (but not text messages), call Client Support as set forth in Section 3 below. Except as expressly agreed with respect to the Traditional SMS Messaging and Transactional, One-Time Passcode SMS Messaging services (which concern identity verification, authentication, fraud prevention and/or compliance related SMS messages) subject to (and as defined in) the ZiFi SMS Terms of Use available on the Website, you may opt-out of certain text messages by replying STOP to any text message you receive. For help, text HELP. You acknowledge and agree that you may receive a text message confirming your opt out.

Please see the ZiFi SMS Terms of Use on the Website for additional terms (including opt-out information or instructions) applicable to Traditional SMS Messaging and Transactional, One-Time Passcode SMS Messaging services, which shall control with respect to ONLY THOSE SERVICES OR COMMUNICATIONS -- EXCEPT AS PROVIDED THEREIN, YOU MAY NOT BE PERMITTED TO OPT OUT OF OTHER, NECESSARY SERVICE, AUTHENTICATION OR PAV CALLS OR TEXT MESSAGES.

Our Privacy Notice can be found within the ZiFi Digital Privacy Statement web page, which can be accessed at https://zifi.com/agreement-center.

PART A – GENERAL TERMS AND CONDITIONS

PART A sets forth the general terms and conditions that apply to all Digital Banking services, including services that are provided through Online Banking and/or Mobile Banking, offered to customers of ZiFi, a division of Zions Bancorporation, N.A.

1. CONSENT, COMMUNICATIONS AND RECORDS; SYSTEM REQUIREMENTS

Consent to Electronic Disclosures. You have and/or now consent: (i) to electronic delivery and/or execution of disclosures, agreements, and other information ("Electronic Documents"); (ii) to the use of electronic records; and (iii) that the foregoing shall govern all of your Digital Banking services, including services that require you to also accept or that you may later self-enroll or otherwise accept as part of the Digital Banking services. You agree and acknowledge that your consent to electronic records is being provided in connection with a transaction affecting interstate commerce that is subject to the federal Electronic Signatures in Global and National Commerce Act ("Act"). Also, you acknowledge and agree that you and the Bank both intend for the Act to apply to the fullest extent possible to validate the Bank's ability to conduct business with you by electronic means.

Further, you agree and acknowledge that permissible electronic delivery by us includes: (i) by email to any address you have provided for use with Digital Banking, including attaching documents to the email, or providing links to or instructions within the email for navigating to documents posted online; (ii) by display on your screen or other "in-product" message or alert during your Digital Banking activity; (iii) by posting it to our Website, within the Secure Messages feature of the Digital Banking, or in our Mobile Banking Software; (iv) by message printed on the statement for your Eligible Accounts; (v) any other electronic means that you have authorized now or later; (vi) any other electronic means that is commercially reasonable and within the system requirements described; or (vii) requesting that you download a PDF file containing an electronic record.

Canceling. If you are a ZiFi deposit account customer, then you may at any time withdraw your consent to electronic delivery instead of paper by calling Client Support. ZiFi is then required to close your deposit account(s) and terminate this Agreement along with your ongoing use of Digital Banking (and not process any previously scheduled future transfers or payments). For withdrawing your consent to eStatements, eNotices and/or eTax Documents, please see Section 29 entitled, "eDocuments Service" for further information.

The Client Support phone number is set forth below in Section 3.

Paper Copies. We do not charge for electronic delivery. We do not send paper copies of electronic communications; however, we may provide you an electronic copy of an electronic communication upon request.

Hardware and Software Requirements. **The following are the hardware and software requirements that apply for Digital Banking:** (i) you must have a computer and/or a Mobile Device; (ii) a current operating system; (iii) a printer (if you want to be able to print your Electronic Documents); (iv) sufficient memory to download and retain Electronic Documents; (v) your computer and/or Mobile Device must use commonly accepted and recently updated software for reading and saving PDF and HTML documents; (vi) you must have an internet service provider and/or mobile communications data service provider; (vii) your computer or Mobile Device must use a commonly accepted and recently updated version of an HTML compliant web browser that supports the latest protocols for encryption; (viii) you must maintain, provide and update us with your active and valid email address(es) for use in sending, receiving and retaining disclosures and other communications; and (ix) you must be able to connect to websites via hyperlinks in email.

Also, for Mobile Banking you must also have: (i) the most recent version of our Mobile Banking Software installed on your Mobile Device that has a camera; (ii) your Mobile Device and/or mobile phone number registered with Digital Banking; and (iii) your Mobile Device enabled for SMS text messaging. Finally, you must regularly install updates as they become available to your computer's and/or Mobile Device's operating system, web browser and PDF reader (and, if applicable, your mobile banking software).

2. INTRODUCTION AND DISPUTE RESOLUTION

This Agreement governs our Digital Banking services for Business Customers.

Not all Digital Banking services and/or functions may be available even though they are described herein. However, you agree and acknowledge that if, and when, such services and/or functions are made available, you agree to and are bound by the terms and conditions for such services and/or functions as set forth in this Agreement and/or Related Document(s), as they may be amended from time to time.

Also, not all Digital Banking services and/or functions are available in all Channels. For example, remote deposit capture may only be available in Mobile Banking. Further, not all Digital Banking functions may be available for all product types. Features in Digital Banking or individual Channels may be added, deleted or changed without prior notice.

This Agreement is supplemented by the terms of your Deposit Account Agreement and other "Account Agreements" (see PART C entitled, "Definitions" below), but this Agreement governs over any conflicting terms therein with respect to Digital Banking.

Dispute Resolution; Jury Trial Waiver, Class Action Litigation Waiver, Private Attorney General and Public Interest Litigation Waiver. Except as may be prohibited by applicable law and subject to applicable dispute resolution provisions in the Deposit Account Agreement (including, but not limited to, mutually-permissive arbitration provisions set forth therein), you and we both hereby waive any rights to have a jury hear or decide any dispute between us, participate in a class action, and/or participate in a private attorney general and public interest litigation. You also hereby agree that such dispute resolution provisions found in your Deposit Account Agreement (including, but not limited to, mutually-permissive arbitration provisions set forth therein) and other Account Agreements between us (as may be amended from time to time) shall also govern the resolution of any disputes under or in connection with this Agreement, the Digital Banking service, any Related Document, or any Digital Banking transaction.

3. CLIENT SUPPORT

The telephone number for Client Support is (800) 341-7303. The address for Client Support is- ATTN: ZiFi, PO Box 26125, Salt Lake City, Utah 84126-0125.

4. ACCESSING YOUR ELIGIBLE ACCOUNTS

When you access Digital Banking, you will see a menu of functions (e.g., view balances; view or search for transactions; execute specific types of internal or external funds transfers; ; etc.). From time to time, with or without prior notice, we can add, modify, and delete particular access protocols, features and functionality, the menus, the Website, and the Mobile Banking Software.

We reserve the right to refuse to make any transaction that you may request through Digital Banking. Also, we reserve the right to honor any request by you to obtain your funds by issuing you a check, mailing it to the last known address in our records and making it payable to the name indicated in our records. You agree that such action will constitute rightful honor under the Uniform Commercial Code.

Information on transfers to or from your Eligible Accounts will be reflected on your account statements for those accounts and will be available to you online. We are not required to provide you with any other notice of the receipt, transmittal, execution or debiting of such transfers.

5. SERVICE AVAILABILITY

We use reasonable efforts to make Digital Banking available with minimal interruptions. Digital Banking may be temporarily unavailable for regular or emergency system maintenance. We will endeavor to have scheduled maintenance occur during non-peak hours, but we may conduct maintenance at any time. In addition, your accessibility to Digital Banking may be interrupted because of conditions or other causes beyond our control, including outages in internet or telecommunications availability, emergency conditions, or to allow emergency personnel to use the communication networks. We will use commercially reasonable efforts to re-establish service in those instances, but we do not promise Digital Banking will always be available for your use. We do not guarantee functionality of Digital Banking through all web browsers or on all Mobile Devices, on all communications networks, in all geographic regions, or at all times. In no event, regardless of cause, shall we be liable to you in any manner whatsoever for the unavailability of Digital Banking, or your inability to access the Service or to execute its functions.

6. NEW FUNCTIONS

We may, from time to time, offer and introduce new functions in Digital Banking. By using these functions when they become available, you agree to be bound by applicable law and all rules we communicate for those functions. Using the new function may require acceptance of a Related Document and/or reacceptance of this Agreement, as amended.

7. FEES

Fees may be assessed by your internet or mobile communications service provider. You are responsible for all fees and charges that you may incur to any communications service provider or any other third parties. <u>We reserve the right to add or change fees for Digital Banking after sending prior notice. See the Section below entitled "Changes to Fees or Other Terms."</u> You agree to pay the fees separately disclosed for enrollment in, or transactions in Digital Banking. Such disclosures may include, but are not limited to, the fee schedules governing your enrolled Eligible Accounts, applications for enrolling your business or any Eligible Account in Digital Banking, and notices displayed within the Digital Banking service itself.

8. EQUIPMENT AND COMMUNICATION PROVIDERS

You are responsible for obtaining your own equipment, software, and internet and/or mobile communications service providers. We are not a party to, and we have no duty, liability, or responsibility in connection with: (i) your internet or mobile communications service provider agreement; or (ii) any hardware, software or any other product or service you may purchase from others relating to your use of Digital Banking. This Agreement does not amend or supersede any agreements that you have with third parties (such as your Mobile Device supplier and your mobile communications service provider), and you remain subject to all terms, fees, costs, other charges, limitations, and restrictions in those agreements with third parties. Your hardware, software and communications providers are responsible for their products and services. You agree that any problems you may have concerning those companies' products, services or agreements shall be resolved by you directly with them, and without involving us.

Your hardware, software and/or communication services may become subject to unauthorized tracking, "hacking," data disclosure or other manipulation by malware such as spyware, viruses, or other malicious code (e.g., "Ghost" which can take control of infected Mobile Devices). We are not responsible for advising you of the existence or potential effect of any malware. Your choices of downloading, installing, and using your hardware, software and communication services are at your own risk. Except as may be prohibited by applicable law (such as Regulation E for certain consumer transactions), you agree that we have no liability for, and you shall indemnify and hold us harmless from, any losses suffered by you, us or by third parties as a result of compromises in the security of your hardware, software, or communication services.

At any time, we reserve the right (but shall have no duty) to limit access to any Digital Banking Channel or function to only those customers who use specific security procedures, hardware, software, or communication services (collectively "controls"). Our specification of required controls shall not constitute a representation or warranty that they: (a) are sufficient for your security needs or will prevent any particular security compromise; or (b) be compatible with your procedures, hardware, software, or communication services. We have no duty to review your security, identify deficiencies or make recommendations.

EXCEPT AS SPECIFICALLY PROVIDED IN THIS AGREEMENT OR THE AGREEMENTS GOVERNING THE TERMS OF ANY LICENSE RIGHT RELATING TO THE USE OR OPERATION OF THE DIGITAL BANKING SERVICES OR MOBILE BANKING SOFTWARE, THE DIGITAL BANKING SERVICES AND MOBILE BANKING SOFTWARE ARE PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF PERFORMANCE, OR MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, OR SECURITY, OR ANY OTHER WARRANTY AS TO PERFORMANCE, ACCURACY, COMPLETENESS OR SECURITY. YOUR USE OF THE DIGITAL BANKING SERVICE AND MOBILE BANKING SOFTWARE, AND ANY MATERIAL OR SERVICES DOWNLOADED OR OTHERWISE OBTAINED VIA THE DIGITAL BANKING SERVICE, IS AT YOUR OWN DISCRETION AND RISK, AND YOU ARE SOLELY RESPONSIBLE FOR ANY DAMAGE RESULTING FROM THEIR USE.

9. EXPORT CONTROLS

Software programs, materials, tools, and technical data may be subject to U.S. export controls or the trade laws of other countries. You agree to comply with all export control regulations. You, not we, have the responsibility to obtain any applicable licenses to export, re-export or import. You agree not to export or re-export to entities on the most current U.S. export exclusion lists or to any country subject to U.S. embargo or terrorist controls as specified in the U.S. export laws.

10. PROTECTING YOUR ACCOUNTS

Reporting Errors. In case of errors or questions about your electronic transfers: call Client Support at the number referenced in Section 3 above as soon as you can if you think your statement or receipt is wrong, or if you need more information about a transfer listed on a statement or receipt.

Protect Your Access Credentials. References to "your Access Credentials" include Access Credentials that are issued to or by your Authorized Users. You are responsible for the use and confidentiality of Access Credentials issued to your Authorized Users.

Note: Some software may store Access Credentials to facilitate future access to websites or mobile applications. For security reasons, you agree to disable those features. You may, however, store data required by biometric identification systems (e.g., fingerprint or facial recognition) that may be supported by our Digital Banking service.

You warrant that you have not and will not: (1) use any software, computer or Mobile Device whose security features have been modified or disabled (including using any "jail broken" mobile device); or (2) use any disposable mobile device (e.g., "burner phone"). Such use can cause security and other problems, and you agree to indemnify and hold us harmless from any damage or loss suffered by us, you or any third person that results from such use.

If you use a third-party service to access Digital Banking on your behalf (e.g., a third-party aggregation service for downloading account data), and for which you share your Access Credentials, that third-party service shall be your agent (not ours). You and your agent shall be solely responsible for, and you shall indemnify and hold us harmless from, all use, misuse, loss or disclosure of your Access Credentials or personal data, and any transactions by that service, its employees or subagents or unauthorized persons.

For Mobile Banking. Your Online Banking Access Credentials are also your primary Access Credentials for Mobile Banking. For Mobile Banking, we may also permit you to use "other " Access Credentials that we make available. Other Access Credentials may include but are not limited to: (1) a simplified passcode for limited functionality (e.g., viewing) that does not include transferring funds; and/or (2) biometric identification (e.g., fingerprint or facial recognition) that may include any Mobile Banking functionality, including funds transfers.

Commercially reasonable types of other Access Credentials methods can be added, removed, substituted or changed by us from time to time without prior amendment of this Agreement. Other Access Credentials may not be available for all Mobile Devices, functionalities, types of accounts, or classes of Mobile Banking.

If you elect to use an optional biometric identification procedure that is performed on your Mobile Device or via a third-party service selected by you, then we can accept and act upon identity authentication communicated to us from that Mobile Device or service, and we can grant access to your Mobile Banking without further action or responsibility on our part to confirm your identity.

Important Note: If any other person's biometric information becomes associated (with or without your knowledge) with a Mobile Device that you or your agent have registered for biometric identification, then that other person's biometric information shall be one of your Access Credentials and you are authorizing that person to transact in your Mobile Banking service. Enabling biometric identification on a Mobile Device that is shared with or may be used by another person is strongly discouraged.

Please see also the Sections of this Agreement entitled "Your Primary Administrator" and "Your Authorized Users," located below.

11. ACCESS CREDENTIALS; SECURITY PROCEDURES; RESPONSIBILITY TO UTILIZE ALL SECURITY PROCEDURES; AGREEMENT TO ALTERNATIVE SECURITY PROCEDURES

Access Credentials. You agree and acknowledge that Digital Banking requires entry of valid Access Credentials. For initial sign in to Digital Banking, Access Credentials generally consists of either: (a) your Username and Password; and/or (b) your biometric identification , such as fingerprint or facial recognition, in a Mobile Banking Channel.

You agree and acknowledge that: a) you will not use personally identifiable information (such as, Taxpayer Identification Number, date of birth, maiden name and etc.) or private financial information (such as, account number, debit card number, and etc.) as part of your Access Credentials; and b) we implement certain character lengths, capitalization and/or symbols for passwords. Further you agree and acknowledge that if we deem, in our sole discretion, that any part of your Access Credentials or credentials do not conform to the foregoing standards, then we may request that you reset your Access Credentials accordingly before accessing Digital Banking, regardless of how long you have been accessing and/or using Digital Banking with any non-conforming Access Credentials or credentials.

Finally, you agree and acknowledge that you bear sole responsibility for maintaining strict secrecy and security of all Access Credentials, Security Procedures, any codes used for MFA or transaction-based authentication services, and any other identifiers, codes, tokens, passwords, or the like (collectively "Identifiers") that we issue to you or allow you to select for purposes of security, identification, or transaction authentication, including Identifiers issued to or selected for your agents. You must immediately notify us of any loss or suspected compromise in the security of any Identifier, and of any termination of an Authorized User.

Security Procedures. You agree and acknowledge that the Access Credentials and any other authentication method or tool we offer or otherwise make available through one or more Related Documents and/or through Digital Banking are the Security Procedures. Also, you agree and acknowledge that we may use the Security Procedures to verify access to Digital Banking, whether it be through the Online Banking or Mobile Banking Channel, and/or to authenticate Communications, which includes, but is not limited to, any Order made in your name delivered to us through Digital Banking.

More specifically, you agree and acknowledge that your agreement to the Security Procedures for Digital Banking is for purposes that include, but are not limited to, Uniform Commercial Code Article 4A, Funds Transfers, as it may be amended from time to time. Consequently, you agree and acknowledge that: (a) the authenticity of Orders issued to us in your name will be verified by us pursuant to the Security Procedures; and (b) Orders in your name delivered to us through Digital Banking authenticated using the Security Procedures may be relied on by us as your effective Order and you will be obligated on the Order, whether or not authorized.

Notwithstanding the foregoing, you agree and acknowledge that we shall have no liability to you if, despite authentication by the Security Procedures, we delay or do not process a Communication (including an Order) that we in good faith believe or suspect might not be authentic or authorized.

Also, you agree and acknowledge that if one or more Communications, including any Orders, were authorized by you and/or you are bound by the Communications under the law of agency, then you will be obligated on the Communications even if we did not authenticate the Communications using the Security Procedures and even if the Security Procedures would have prevented error. You agree and acknowledge that the Security Procedures are intended to authenticate Communications and not to detect error. You are solely responsible for the accuracy of your Communications.

Further, you agree and warrant that you have: (a) assessed the risks presented by the possibility of unauthorized access to Digital Banking and/or unauthorized instructions to move money through Digital Banking; (b) reviewed the Security Procedures in consideration of the risks; and (c) determined that the Security Procedures are commercially reasonable security procedures for your needs, including, but not limited to, the size, type and frequency of Orders that you use Digital Banking to accomplish. You agree and acknowledge that the Security Procedures are a commercially reasonable method of providing security against unauthorized Orders after considering the risks.

Also, you agree and acknowledge that we, acting in good faith, are entitled to receive, act upon, execute, and rely upon any Orders that are authenticated by the Security Procedures. And you agree and acknowledge that such authenticated Orders shall be effective as your Orders and we shall have no obligation to further investigate the authenticity of any Orders that are authenticated by the Security Procedures.

Additionally, you agree and acknowledge that each subsequent use of Digital Banking by you shall constitute a reacceptance and a reaffirmation of your ongoing agreement and warranty that the Security Procedures, which are a menu of Security Procedures that may be added to or modified from time to time, remains commercially reasonable for the size, type and frequency of Communications that you use Digital Banking to accomplish.

Finally, you agree and acknowledge that in your current and ongoing review of the Security Procedures in connection with your use of the services offered by Digital Banking, now and in the future, you will notify us immediately in the event your use of Digital Banking, including any Digital Banking service that allows for the movement of money, would necessitate or be better served by a level of security that exceeds that offered by the Security Procedures. In the event of such notification, you agree and acknowledge that we reserve the right to suspend any service within Digital Banking that allows money movement. If you fail to notify us immediately, then you agree and acknowledge that the Security Procedures made available by us for each service offered within Digital Banking are appropriate for your needs and will provide you with a commercially reasonable degree of security against unauthorized use.

Responsibilities to Utilize all Security Procedures. You agree and acknowledge that any additional or modified authentication tool or method we make available, now or in the future, to authenticate any Communications (including Orders) received by us in your name are part of the Security Procedures and it is your responsibility to use these additional or modified authentication tools or methods when we make them available to you. Specifically, you agree and acknowledge that this responsibility, which requires you to regularly review all types of additional or modified tools or methods for authentication of Communications we make available, as they may be updated or modified from time to time, requires specific action on your part, such as, but not limited to, enabling or enrolling for additional or modified authentication tools or methods through your Primary Administrator's self-administration functionality within Digital Banking.

For example, Digital Banking may make available, depending on your type of business entity structure and/or whether you have multiple Authorized Users, the ability to have a Security Procedure that would require that certain Orders must be initiated and approved using the separate Access Credentials of two Authorized Users ("Dual Control"). If, and when, Dual Control is made available by us as an additional tool or method for authentication of certain Orders, then you agree and acknowledge that: (a) you will utilize Dual Control with or without any specific separate request by us; and (b) Dual Control is a commercially reasonable security procedure for the size, type and frequency of Orders that you use Digital Banking to accomplish.

Agreement to Alternative Security Procedures. If you choose not to use a Security Procedure other than Access Credentials that we make available to you (such as Dual Control or an updated MFA method) and/or later discontinue utilizing a Security Procedure other than Access Credentials, then you understand and acknowledge that you are **expressly** agreeing to "alternative security procedures." You understand and acknowledge that we highly recommended that you utilize all Security Procedures that we make available to you, in particular Dual Control (when it is available for utilization by you), and that by not using any or all Security Procedures in addition to the Access Credentials that we make available to you constitutes your refusal of one or more Security Procedures that are commercially reasonable.

Also, you agree and acknowledge that by agreeing to "alternative security procedures" you have made a voluntary decision that the Security Procedures you are using, such as single control, are commercially reasonable methods of providing security against unauthorized payment orders for the size, type and frequency of Orders that you use Digital Banking to accomplish. Specifically, you agree and acknowledge that the "alternative security procedures" are the "Security Procedures" and any Order in your name delivered to us through Digital Banking authenticated using the "Security Procedures" may be relied on by us as your effective Order and you will be obligated on the Order, whether or not authorized.

Further, you agree and acknowledge that by agreeing to "alternative security procedures" as the "Security Procedures" you cannot shift the risk of loss associated with unauthorized Orders to Zions Bancorporation, N.A. Furthermore, you agree to indemnify and hold us harmless from and against any and all liabilities, obligations, losses, damages, penalties, actions, judgments, suits, costs, expenses or disbursements of any kind whatsoever that you or we may suffer to the extent that such loss: (a) could have been detected, prevented, reduced or recovered by your use of one or more additional or modified authentication tools or methods we made available to you in order to authenticate Orders and/or other Communications that you declined or refused to utilize; (b) in any way relates to or arises, directly or indirectly, out of your express agreement to use the "alternative security procedures" as the "Security Procedures" to authenticate Orders in your name delivered to us through Digital Banking; and/or (c) in any way relates to or arises, directly or indirectly, out of your failure to effectively use any Security Procedure (e.g., you provide an erroneous unique email address or mobile phone number for purposes of receiving one-time passcodes as part of an MFA protocol).

Finally, you agree that we are making various digital funds transfer and payment methods available to you under this Agreement, the nature of which may generally increase risks or losses associated with unauthorized or fraudulent funds transfers, payment orders or Communications. In exchange for the convenience and versatility inherent to such capabilities offered through Digital Banking, you agree and acknowledge California Commercial Code, Section 11202, as it may be amended from time to time, as the law governing the subsections entitled, "Security Procedures," "Responsibilities to Utilize all Security Procedures," and "Agreement to Alternative Security Procedures," as set forth above in this Agreement, without regard to conflicts of laws principles and notwithstanding any other provision in this Agreement, the Deposit Account Agreement or any other Account Agreements or Related Documents; **EXCEPT TO THE EXTENT THE APPLICABLE LAW FOR YOUR ACCOUNT(S) (AS DETERMINED BY YOUR DEPOSIT ACCOUNT AGREEMENT) PROVIDES FOR THE USE OF A RECORD STORED IN AN ELECTRONIC OR OTHER LIKE MEDIUM FOR PURPOSES OF ESTABLISHING OR DOCUMENTING AGREEMENTS UNDER ANY SUCH STATES' ADOPTION OF UNIFORM COMMERCIAL CODE ARTICLE 4A-202.**

12. YOUR PRIMARY ADMINISTRATOR

You hereby fully authorize your Primary Administrator to act as your designated agent in all matters regarding Digital Banking itself and transactions using Digital Banking. You must have at least one Primary Administrator and that Primary Administrator may designate others to have the same or less than same entitlements as the Primary Administrator in Digital Banking. Each Primary Administrator and any person authorized by your Primary Administrator will be deemed to be an authorized agent. In all matters regarding your Digital Banking service, we shall be entitled to accept, rely upon and act upon, without further inquiry, any written, electronic or oral instructions, directions, consents, waivers and agreements that are received by us from your authorized agents.

Your Primary Administrator's authority includes, without limitation, the power to:

a. engage in functionality and/or authorize entitlements;

b. designate Eligible Accounts accessible via your Digital Banking;

c. designate one or more Authorized Users, and request the timely setup of Access Credentials for using Digital Banking, which may be subject to limits configurable by the Primary Administrator;

d. designate one or more Authorized Users with the same exact entitlements of the Primary Administrator, which would allow the Authorized User(s) to do any of the foregoing without the Primary Administrator's knowledge, including, but not limited to, entitling any person to have access to Digital Banking as an Authorized User with the same entitlements as the Primary Administrator; and

e. receive on your behalf, as your designated agent, any legal notices (including notices of amendment to or termination of this Agreement), transaction notices or disclosures from us in connection with Digital Banking.

Your Primary Administrator's authority also includes the power to designate, on your behalf, one or more additional Authorized Users for your Digital Banking service, and issue additional Access Credentials for performing Primary Administrator functions. You are responsible for ensuring that Access Credentials for your Digital Banking service's self-administration functions are not issued to an Authorized User whom you do not intend to have access and/or use of Digital Banking and/or to have the same control and power with entitlements as the Primary Administrator.

Your Primary Administrator's authority and Access Credentials shall remain in place until: (a) you deliver formal written notice of revocation to us through the Secure Messages feature of Digital Banking indicating revocation and who is the new Primary Administrator (who must be an existing Authorized Principal); or (b) you notify us by calling Client Support at (800) 341-7303 indicating revocation and who is the new Primary Administrator. However, other Authorized User's authority and Access Credentials, including, the same control and power of entitlements as the Primary Administrator can only be revoked online by the Primary Administrator using Digital Banking's self-administration functionality. In each case we shall have a commercially reasonable time and opportunity to act upon that notice or online revocation. In addition, we may revoke or refuse to accept your Primary Administrator's authority and Access Credentials in connection with Digital Banking at any time without prior notice.

13. YOUR AUTHORIZED USERS

Through his or her or their Access Credentials, an Authorized User can access Digital Banking's functions, subject however to restrictions imposed by Digital Banking itself or by your Primary Administrator (as permitted by Digital Banking's self-administration functionality). Limits on an Authorized User's access may include restricting an Authorized User to or from particular Eligible Accounts; to or from particular functions; dollar limits; viewing but not transacting in Eligible Accounts; transactions requiring prior or secondary authorization by another Authorized User. We may from time to time change the available types of limits.

An Authorized User is your agent for receiving notices from us regarding any transfer, transaction or other instruction submitted to Digital Banking by that Authorized User or another Authorized User. That agency includes, but is not limited to, receiving any disclosures that we may be required by law to provide to you in writing.

You represent that each individual who is issued Access Credentials by your Primary Administrator or by an authorized agent given the power to issue Access Credentials to others has general authority from you to view and transact in the Eligible Accounts associated with that person's Access Credentials (unless those credentials are limited to view only) and to otherwise exercise the capabilities associated with that person's Access Credentials.

An Authorized User's Access Credentials shall remain in place until those Access Credentials are revoked online by your Primary Administrator using Digital Banking's self-administration functionality; but in each case we shall have a commercially reasonable time and opportunity to act upon that revocation. In addition, we may revoke or refuse to accept any Authorized User's Access Credentials at any time without prior notice. Authorized Users may be allowed to change their Access Credentials.

14. MONITORING YOUR DIGITAL BANKING ACCOUNTS

You agree to exercise ordinary care in monitoring your Eligible Accounts in Digital Banking (including reviewing the transactions reported in Digital Banking on each Business Day), and to immediately notify us of any discrepancies. Also, you agree and acknowledge that in order for us to comply with our requirements under the Nacha rules, you must notify us of an unauthorized or erroneous ACH debit transaction before 5:00 p.m. Eastern Time on the Business Day after the posting of the transaction to your account. If you fail to notify us of the unauthorized or erroneous ACH debit transaction within this time frame, we shall have no liability to you for the transaction.

In that event you miss this deadline, we will provide reasonable non-financial assistance to you in making appropriate claims (which may include breach of warranty claims) under applicable payment system rules (e.g., Nacha Rules or Article 4A of the Uniform Commercial Code) against the receiver/beneficiary and the receiver/beneficiary's financial institution. However, while such claim is pending, and if such claim is unsuccessful, you covenant to not assert any claim against us for that loss. Without limiting the foregoing standard of daily review, in no event shall we be liable for any discrepancy that is not reported to us within thirty (30) days of it first appearing in Digital Banking.

15. DUTY TO REVIEW ACCOUNTS AND REPORT DISCREPANCIES

In addition to your duties under the law, your Account Agreements, and your Related Documents, you agree to use Digital Banking to frequently review activity in your Eligible Accounts, and to IMMEDIATELY notify us of any discrepancies, including, but not limited to, any erroneous or unauthorized transactions.

We often can stop or recover transactions that Digital Banking reports as still pending or processing, return or recover transactions that are still in the process of final settlement, or recover funds that have been sent but not further transferred by the recipient (but we do not promise we can or will do so).

Therefore, your duty to exercise ordinary care may includes using Digital Banking to review your Eligible Accounts on a daily basis. We may deem your failure to frequently review and immediately notify us as a proximate cause of an experienced loss. You also agree to frequently check Digital Banking's Secure Messages feature for notices from the Bank.

16. YOUR INTERNAL SECURITY

You bear sole responsibility for establishing, maintaining, implementing and updating policies, procedures, equipment and software ("**Internal Security Controls**") that ensure the security and integrity of your computer systems, Mobile Devices and information, protect them from any unauthorized use, intrusion, takeover or theft, and prevent your Access Credentials from any unauthorized discovery or use (collectively "**Internal Security Breaches**"). You bear all risk of fraudulent transfers and other losses or disclosures arising from your Internal Security Breaches or from the interception of your communications prior to their receipt by us (collectively "**Internal Security Losses**"). We will not reimburse your Internal Security Losses. You are encouraged to consider purchasing insurance to cover your Internal Security Losses.

To help protect your system from Internal Security Breaches, your Internal Security Controls program should consider including:

a. Verifying all instructions from your payees (e.g., ensure new or changed payment addresses were not communicated by an imposter);

b. Limiting and controlling who has access to your computer systems and Mobile Devices;

c. Protecting and frequently changing your Access Credentials;

d. Adopting dual authorization and/or transaction-based authentication procedures for financial transfers;

e. Employing up-to-date security software such as anti-virus, anti-malware and anti-spyware programs, as well as up-to-date software patches for all your software programs, internet browsers, email programs, and the like;

f. Prohibiting the disabling or modification of the security features of any software or hardware (e.g., "jailbreaking" of mobile devices); and prohibiting the use of "burner" mobile devices.

g. Using effective, up-to-date firewalls;

h. Procedures to avoid infection by malware and malicious code, such as: controlling what software and applications are downloaded to your computers and Mobile Devices; controlling what websites are visited by your computers and Mobile Devices; controlling the connection of other devices (e.g., flash drives) to your computers and Mobile Devices; controlling what documents, email attachments, programs and other files are opened or installed on your computers and Mobile Devices; and limiting which of your computers and Mobile Devices are used for Digital Banking or other financial matters;

i. Reconciling all accounts on a daily basis, and immediately reporting any discrepancies;

j. Prohibiting your Authorized Users from leaving a computer or Mobile Device unattended while connected to Bank's systems, or from communicating or accessing sensitive information from insecure locations (e.g., terminals or networks at Internet cafes or airports);

k. Allowing Digital Banking to be accessed only from secure locations; and

l. Adopting such other recommendations that we may (but are not obligated to) make from time to time to help promote safe use of our services.

This is not a complete list of the Internal Security Controls that you may need. You are solely responsible for determining and implementing all of the Internal Security Controls necessary to prevent your Internal Security Breaches and Internal Security Losses. We have no duty to review your Internal Security Controls, identify deficiencies or make recommendations. We do not represent or warrant that any or all of the above recommendations or any future recommendations are adequate for your needs or will prevent Security Losses.

We may at any time (but are not required to) limit access to any Digital Banking Channel or function to only those customers who have adopted specific Internal Security Controls. Our specification of any required Internal Security Controls shall not constitute a representation or warranty that they: (a) are adequate for your security needs or will prevent any Internal Security Breach or Internal Security Losses; or (b) will be compatible with any computer system or other Internal Security Controls.

You remain at all times solely responsible for your Internal Security Controls, Internal Security Breaches and Internal Security Losses. Although we may employ various systems and procedures from time to time to prevent losses by us, we assume no obligation for your Internal Security Losses.

17. LIMITATION OF LIABILITY

Except as specifically provided in this Agreement, or where the law requires a different standard, you agree that we shall not be responsible for any loss, whether caused by us, by equipment or software, by internet service providers, by mobile communications service providers, or by any agent or subcontractor of any of the foregoing. **We shall not be responsible for any direct, indirect, special or consequential, economic or other damages in connection with the Digital Banking service, or arising in any way** out of the installation, use or maintenance of equipment or software, even if you have notified us or we are aware of the possibility of such damage.

Our obligations and your rights and remedies with respect to Digital Banking are set forth in this Agreement, and are exclusive, and any related services or products are provided "AS IS." WE HEREBY DISCLAIM AND EXCLUDE ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LMITATION ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, SECURITY OR NON-INFRINGEMENT.

18. CHANGES TO FEES OR OTHER TERMS

We reserve the right to change (amend, add or delete) fees for Digital Banking, any term of this Agreement, and the Digital Banking service itself. We will send you such notice, which may include sending such notice through the Secure Messages feature of Digital Banking, of those changes as may be required by law or by our other agreements with you.

Notices of new or increased fees will be provided at least twenty-one (21) days before the effective date of the change. Notice of other changes, if presenting an adverse impact to you or otherwise required by law, will be provided in advance and, if there is a legal requirement to give a certain amount of advance notice before the change's effective date, then we will give at least that amount of time or more, unless an immediate change is necessary in our discretion for exigent circumstances (e.g., maintaining the security of the system). If an immediate change cannot be disclosed before it is effective, we will provide any required notice within a reasonable time thereafter. You agree and acknowledge that by continuing to access and/or use one or more of the Digital Banking services after a change (or after the effective date of any prior notice), you are accepting the changes regardless of whether you are using the service or feature that is subject to the change. Changes to fees applicable to specific Eligible Accounts are governed by their separate Account Agreements. Features and functionality may be amended without prior notice unless required by law.

19. SUSPENSION AND TERMINATION

We reserve the right to suspend or terminate this Agreement, your access to Digital Banking, or Digital Banking itself, in whole or in part, at any time without prior notice except as required by law.

If all your enrolled Eligible Accounts are closed, or if you have a zero or less balance in any of your Eligible Accounts for any consecutive thirty-day (30) period, your access to Digital Banking (including related services that you access through Digital Banking such as the eDocuments Service) may be terminated or suspended without prior notice. However, if we terminate Digital Banking, your eStatements can be viewed online after closure for 30 days. If you need to access your eStatements after your access has been disabled, you may still obtain electronic copies of your eStatements by calling Client Support.

You may terminate your Online Banking or Mobile Banking services at any time by contacting Client Support (800) 341-7303. We shall have a reasonable time of two Business Days to act upon your notice of termination. For Mobile Banking, you must also un-register your Mobile Device and remove the Mobile Banking Software.

If you or we terminate your Digital Banking for any reason, any unprocessed transfers that you have scheduled through Digital Banking (or related services that you access through Digital Banking) will be cancelled without notice.

All provisions of this Agreement which by their nature are intended to survive the termination of this Agreement shall survive such termination.

20. PAYMENT ACCOUNT

You agree to pay promptly all fees and charges for services provided under this Agreement and authorize us to automatically charge your designated Payment Account. If you close the Payment Account, you must notify us and identify a new payment account for the selected services. Until you designate a new payment account, you authorize us to debit any other deposit account.

21. HOLD HARMLESS AND INDEMNIFICATION

Except to the extent that we are liable under the terms of this Agreement or an Eligible Account's governing Account Agreement, you waive any claim against us and agree to indemnify and hold us, our directors, officers, employees, and agents harmless from all loss, liability, claims, demands, judgments and expenses arising out of or in any way connected with the performance of Digital Banking. This indemnification is provided without regard to whether our claim for indemnification is due to the use of Digital Banking by you or your agents.

Without limiting the generality of the preceding paragraph, you agree to indemnify, defend and hold harmless us, our parent company, and our respective directors, officers, employees and agents, from and against every claim, damage, loss, liability and cost (including without limitation attorney's fees) of any kind which results directly or indirectly, in whole or in part, from: (a) any authorized or unauthorized use of your Access Credentials; (b) your breach of this Agreement; (c) our actions or omissions, if they are in accordance with your instructions or the terms of this Agreement; (d) the actions or omissions of you, your agents or employees, including, but not limited to, inaccurate, ambiguous or incomplete instructions to us; (e) any warranty that we are required or deemed to make to a third party in connection with your transactions; (f) your use or distribution of any equipment or software that is inconsistent with the license or sublicense that you may receive; (g) actions, omissions, delays or failures to perform by third parties (including other financial institutions, the Federal Reserve, funds transfer systems, payment networks, beneficiaries/receivers, and service providers) none of whom shall be deemed our agent; and (h) any delay, alteration or corruption in the transmission of information to us. This Section shall survive the termination of this Agreement.

22. FOREIGN TRANSFERS

Digital Banking service does not support, and you will not attempt to use Digital Banking to make, foreign transfers or foreign currency transactions. Each time you use Digital Banking, you warrant that your transactions do not violate United States laws or regulations (including, but not limited to, laws administered by the U.S. Treasury's Office of Foreign Assets Control ("OFAC")).

23. EXCLUSIVE USE AND YOUR NON-ASSIGNMENT

Digital Banking is furnished for the exclusive use of you and your Authorized Users. You shall not sell, assign or transfer this Agreement or any materials furnished to you in connection herewith. You shall not resell any part of the Digital Banking service (including its related services) or use any of its features or functionality (e.g., External Transfers/ACH) for the benefit of anyone other than yourself. We may assign this Agreement without notice to you.

24. LEGAL NOTICES AND OTHER COMMUNICATIONS BY US TO YOU

We may send you any required or voluntary written legal notice, or any other communication regarding Digital Banking, by: (A) any method of delivery described above in the subsection entitled, "Consent to Electronic Disclosures;" (B) U.S. mail or commercial delivery service to your address as it appears in our records; (C) message printed on the periodic statement for any of your accounts; or (D) any other commercially reasonable method and manner. Electronic messages to you shall be effective upon posting or sending. Email notices to you shall be effective upon being sent, even if blocked or returned by your system or service provider.

Notices to you by U.S. mail or commercial delivery shall be effective upon the earlier of actual delivery or three (3) Business Days after the notice is sent. Other notices to you shall be effective a commercially reasonable number of days after sending. If this Agreement or law does not require us to provide you with written notice, then we can notify you by telephone.

You are responsible for notifying us and updating us of any change in your email address, your U.S. mail address, your physical address, or phone number. Please note: notice to a Primary Administrator (e.g., your Primary Administrator's email address or by electronic message accessible via your Primary Administrator's Access Credentials) shall be effective notice to you; **your duty to update your contact information includes changes to any Primary Administrator's email address or phone number.**

25. NOTICES BY YOU TO US

Formal legal notices by you to us regarding Digital Banking must be made by commercial delivery service or U.S. Mail delivered to Zions Bancorporation, National Association, Attn: Corporate Legal Department, One South Main Street, #1100, Salt Lake City, Utah 84133.

Other types of notices by you regarding Digital Banking should be: (1) posted through Digital Banking's electronic Secure Messages feature; (2) telephoned to Client Support; or (3) delivered by commercial service or U.S. Mail delivered to Client Support. You authorize us to act on your oral notices, but we may require you to promptly confirm any oral notice via Digital Banking's Secure Messages feature or delivery to the ClientSupport address before such oral notice is binding.

You must IMMEDIATELY notify us of any unauthorized or unrecognized transaction appearing in your Eligible Accounts, or of any compromise or potential compromise of any Access Credentials, by calling Client Support.

26. GOVERNING LAW

Except as specifically stated otherwise in this Agreement and/or Related Documents, this Agreement will be governed by and interpreted in accordance with federal law and regulations, and by the laws of the State of Utah.

27. ENTIRE AGREEMENT

This Agreement, as supplemented by your Account Agreements and your Related Documents, constitutes the complete and entire agreement between you and us, relating to the subject matter of this Agreement.

This Agreement governs over any conflicting terms and conditions that you may have previously accepted for Online Banking, Business Online Banking or Mobile Banking services. When you enroll or we automatically enroll you in a new Channel or you obtain an additional service through Digital

Banking, we may require that you re-accept this Agreement or an updated version hereof, applicable to all Channels in which you become enrolled. This Agreement incorporates the Related Documents for your services, including agreements for services that are available within Digital Banking but require separate enrollment and acceptance of terms.

PART B – DIGITAL BANKING SERVICES

PART B sets forth the terms and conditions that apply to the applicable specific Digital Banking service.

With Digital Banking, you may access your Eligible Accounts, their balances, transaction history and other information. You may also conduct the types of transfers described below. You agree and acknowledge that your Eligible Accounts are established for business or commercial purposes and your use of the Services in connection with those business or commercial Eligible Accounts will only be for business or commercial purposes and not for any personal, family or household purposes. We may, from time to time, offer and introduce new electronic banking services. All current and future services will be governed by this Agreement.

28. VIEW

Digital Banking allows you, subject to system limitations, to view account balances, transactions, eStatements, and, if, and when available, images of checks paid and checks deposited using the Mobile RDC Service. You agree and acknowledge that balance and transaction information provided to you as part of the Digital Banking service is not the official record of your account or its activity. Your account statement furnished to you by us in electronic format is the official record.

You agree and acknowledge that balance and transaction information is generally updated in real time; but is subject to adjustment and correction and therefore should not be relied upon by you for taking, or not taking, any action. Also, you agree and acknowledge that certain balances may not be subject to immediate withdrawal, may include deposits still subject to verification or other items in the process of being posted to the account, and may not include outstanding checks, debits, or credits. Please see "When Will Funds Be Available- Your Ability to Withdraw Funds" and "Posting Order" in the Deposit Account Agreement for additional information.

29. EDOCUMENTS SERVICE

You agree and acknowledge that we generally do not offer paper deposit account statements, notices and/or tax documents and that by applying for one or more deposit accounts with us and/or agreeing to this Agreement, you are automatically enrolled in our eDocuments Service as set forth in this Agreement. **This means that you will be automatically getting eStatements, eNotices and/or eTax Documents for your deposit accounts.**

You can access your eStatements, eNotices and/or eTax Documents by signing in to Digital Banking. Unless stated otherwise in this Agreement or we decide otherwise in our sole discretion, we will not also send you or any co-owner of the Eligible Account paper versions of your eStatements, eNotices and/or eTax Documents.

There is no fee for receiving eStatements, eNotices, or eTax Documents.

Reviewing eDocument Communications in Digital Banking. To view a new eDocument Communication sign in to Digital Banking. You can access all eDocument Communications via the homepage of your eDocuments Service. Also, you may be able to view prior eDocument e Communications via the homepage of your eDocuments Service.

Please note: All eDocument Communications, including eTax Documents, may be seen by all Authorized Users.

When eDocument Communications are Deemed Delivered. eDocument Communications are deemed given, received and effective upon being transmitted by us. We have no obligation to monitor whether you are receiving or reviewing your eDocument Communications. We have no obligation to send your paper versions of information from eDocument Communications, or to take any other response, if we learn that you are not receiving or reviewing eDocument Communications. If you are unable to review eDocument Communications, you are solely responsible for updating your software and/or hardware requirements in the manner described above in Section 1 under the heading, "*Hardware and Software Requirements*" and/or in your E-Sign Consent for Execution and Delivery of Electronic Documents.

Obtaining Electronic Copies. Again, we generally do not provide paper documents in connection with ZiFi digital banking products and services. In the event you need copies of your current or past eStatements, eNotices and/or eTax Documents, we can provide you electronic copies. Please call us at the number specified above in Section 3 entitled, "Client Support" to make your inquiry for electronic copies.

Cancelling your eStatements, eNotices or eTax Documents service. You may cancel receiving eStatements, eNotices and/or eTax Documents at any time in connection with your deposit accounts. However, if you cancel one or more of these services, then we will have to close all your deposit accounts that were opened through our digital deposit application process and terminate your services offered under this Agreement. To cancel receiving eStatements, eNotices and/or eTax Documents, please contact us by calling the phone number specified in Section 3 above, entitled "Client Support," or by using the Secure Messages feature within Digital Banking.

However, if we terminate Digital Banking, your eStatements can be viewed within Digital Banking after account closure for 30 days. If you need access to your eStatements and/or eTax Documents after your access has been disabled, you may still obtain electronic copies by calling Client Support.

Persons Able to Access eDocument Communications. On behalf of yourself and all other owners of the enrolled Eligible Account, you acknowledge and accept that anyone with access credentials (e.g., Username and Password) to log into your Eligible Account is able to read and copy any eDocuments Communications. You, any Authorized Principals, and/or Authorized Users, as those terms are defined in this Agreement, and any persons you or they entrust with Access Credentials, are responsible for protecting the secrecy of those Access Credentials and safeguarding them against misuse by authorized or unauthorized persons. If you suspect any unauthorized access to the eDocuments Service, other portions of Digital Banking or any account, then call us at the number specified above in Section 3 entitled, "Client Support."

Additional Terms for eTax Documents. For tax forms that are outside the scope of the eTax Documents service, you will continue to receive your tax forms by mail without further action by you. Your enrollment applies to all eTax Documents for current and future tax years, until consent is withdrawn by you, we terminate your enrollment in the eTax Documents service, or we terminate the eTax Documents service itself. We will provide you with reasonable notice before terminating your enrollment or the eTax Documents service.

eTax Documents will be made available through Digital Banking on or before the required federal and, if applicable, other state or local deadline. Please see IRS.gov for applicable federal tax form deadlines.

Tax forms for which Internal Revenue Service reporting thresholds are not met will not be created and will not be available through Digital Banking. (For example, checking account customers with aggregated interest amounts lower than $10.00 will not receive a tax statement. Please see IRS .gov for the various form reporting thresholds.)

You may request an electronic copy of your tax forms by calling us at the number specified above in Section 3 entitled, "Client Support."

Miscellaneous. We reserve the right to determine which account information will be provided by eDocument Communication rather than by paper, and the right to provide any information by paper in addition to (or instead of) eDocument Communication despite automatic enrollment in the eDocuments Service.

We may change those determinations, or suspend or terminate any eDocuments Service or enrollment, at any time for any or no reason, with or without prior notice. (In addition, if an account becomes delinquent, charged-off, blocked or frozen, it may no longer be accessible via Digital Banking, then it may no longer be accessible via Digital Banking and eDocument Communications may no longer be available for that account.)

These terms and conditions for the eDocuments Service supplement, but do not replace, your Account Agreements and other agreements that you may have accepted that apply to your account. For example, see your Account Agreements for information about your obligation to promptly review statements and report errors or unauthorized activity in your accounts; your rights and our duties when you report errors or unauthorized activity; limitations on our liabilities and your remedies applicable to products and services (including an eDocuments Service) that we provide in connection with Digital Banking.

30. INTERNAL TRANSFERS

Digital Banking allows you to transfer funds among your Deposit Accounts on a one-time basis. You agree and acknowledge that we have the right to establish, without prior notice unless required by law, limitations on the amount or number of Internal Transfers. Unless otherwise required by law, we may also without prior notice increase, decrease, or remove such limitations at any time, and we are not obligated to enforce our limitation of any Internal Transfer.

31. LOAN PAYMENTS

Digital Banking, if, and when, it is available, allows you to make a transfer from your eligible Deposit Account to one or more Loan Accounts ("Internal Payment"). Internal Payments will be credited to the designated Loan Account as regular payments. Please refer to your Loan Account's agreement(s) for information on how regular payments are applied. For some Loan Accounts you may be permitted to make principal-only payments. Which Loan Accounts will accept principal-only payments is subject to change from time to time without prior notice but will be reflected in the features available each time you log in to Digital Banking. Principal-only payments will not satisfy scheduled payment due requirements. Prior to making a payment to pay off a Loan Account, please contact your Loan Officer to obtain the payoff amount.

We cannot guarantee that estimated payoffs will satisfy the loan terms of the Loan Account.

32. LOAN ADVANCE

Digital Banking, if, and when, it is available, allows you to make an advance or otherwise draw from your eligible Loan Account, including a credit card held with the Bank, in order to make a deposit to one or more eligible Deposit Accounts ("Internal Advance"). You agree and acknowledge that the relevant loan or credit card agreement, note or other document is modified to the extent necessary to allow your Internal Advances. We may process transactions from Loan Accounts without regard to access limitations in any loan documentation or agreements.

33. EXTERNAL TRANSFER

You may be able to add an external deposit account to the Service in order to: (i) make a transfer of funds from one or more of your eligible Deposit Accounts to that external deposit account held outside of the Bank, which includes an account held at a division of the Bank, that is held by you or a third party (provided that you are authorized to transact on that account); or (ii) make a transfer of funds from your external deposit account held outside of the Bank to a Deposit Account ("External Transfers").

External Transfers requires that the Service validate each external deposit account that you wish to access in connection with the External Transfer service. Validation is done through account verification. Specifically, before the Service will allow you to transfer money to or from your external deposit account, you will be prompted to enter your banking credentials for your external deposit account. We will authenticate your banking credentials immediately, which will allow the Service to link your external deposit account quickly. The External Transfer Service is a business service offered to ZiFi business customers, and you should only use the External Transfer Service to send or receive external transfers for business purposes. You agree and understand that if you use the External Transfer Service to link an external deposit account, then any errors or questions you have in connection with that external deposit account must be addressed with your financial institution.

However, if you choose not to enter your banking credentials, or there is some error in validating your banking credentials, or your financial institution does not participate in the account verification method offered by the Service, or the account verification method is for some reason not available, then you will not be able to add your external deposit account for the External Transfer service through Digital Banking. But you may transfer funds into your eligible Deposit Account by using the online or mobile banking system of your financial institution that holds your external deposit account, which generally requires you to provide your ZiFi deposit routing and account number.

You agree and acknowledge that if you link an external account held at another financial institution in connection with the External Transfer service that: (i) you are the owner or authorized signer on that external account; (ii) the external account and depository financial institution is in the United States; (iii) the external account is linked with the correct usage type (e.g., business or personal) as designated within the Digital Banking external account validation process; (iv) you are authorized to make payment orders to and from that external account as permitted by the external account's requirements and applicable law; (v) by disclosing and authorizing us to use the financial information of the external account you are not violating any third party right; and (vi) you warrant and represent that the information about the external account is true and correct to the best of your knowledge.

Further, you agree and acknowledge that your agreement to this Agreement and/or your instructions within Digital Banking to credit or debit an external deposit account is the authorization necessary for us to complete each single-Entry transfer request now and in the future and by any means we select, including, but not limited to, the National Automated Clearinghouse. You agree and acknowledge that you are bound by the rules, laws and regulations that govern the applicable transfer means, such as the ACH rules as published by the National Automated Clearinghouse Association (Nacha) and that your ACH transactions comply with all applicable law, including, but not limited to, U.S. law, such as the rules, sanctions and executive orders that: (i) prohibit you from transacting with certain people, entities, countries, and officials; and (ii) prohibit you from transacting with a person when such person is located in certain countries. Also, you understand and agree that each ACH authorization will remain in effect until you notify us by cancelling the transfer within Digital Banking before the date the transfer begins processing. Finally, you agree and acknowledge that you will take a screenshot of the confirmation page of each transfer request, which also serves as your ACH authorization (if ACH is used as the means to execute your transfer request), and store it for your records.

34. AVAILABILITY OF FUNDS AND CUT-OFF HOURS

Internal Transfers will be processed on that current day, and available balances in your Deposit Account(s) will be adjusted immediately and available for subsequent withdrawals or other debits as applicable to your Deposit Account(s). External Transfers have a cut-off time of 1:00 p.m. Eastern Time on a Business Day for same day External Transfers and 4:00 p.m. Eastern Time on a Business Day for next day External Transfers. An External Transfer submitted after the applicable cut-off hours or on a non-Business Day will be deemed submitted on the next Business Day. The funds representing the settlement of an incoming External Transfer will be available by the fourth Business Day from the Settlement Date, as defined in the ACH data accompanying the transaction. This means that we will hold the funds for three Business Days, starting on the Settlement Date, and release the hold no later than the opening of business on the fourth Business Day.

35. INSUFFICIENT AVAILABLE FUNDS

If an Internal Transfer, Internal Payment or External Transfer would result in an overdraft of your Eligible Account, we may in our sole discretion honor the transaction and create the overdraft or cancel the transaction. In addition, you may be charged any applicable overdraft fees (as disclosed for your Eligible Account).

36. CANCELLING AN INTERNAL TRANSFER, INTERNAL PAYMENT, INTERNAL ADVANCE OR EXTERNAL TRANSFER

You may schedule one-time Internal Transfers, Internal Payments, Internal Advances or External Transfers. You may cancel any of the foregoing one-time transfers if you do so at least one Business Day prior to the scheduled transaction processing date. Scheduled Internal Transfers, Internal Payments, Internal Advances and External Transfers can only be canceled by placing a request through Digital Banking. You may NOT cancel any immediate Internal Transfer, Internal Payment, Internal Advance or External Transfer. (An "immediate" transfer is one that you schedule to begin processing immediately at the time of your instruction, rather than on a future date.)

37. MOBILE CHECK DEPOSIT SERVICE

The mobile remote deposit capture feature of Mobile Banking (the "Mobile RDC Service"), when it becomes available, allows you to make deposits to your ZiFi Business Checking, ZiFi Business Savings, and other deposit accounts (that are eligible) with us using your camera-enabled Mobile Device. That device must be capable of capturing check images and information, and electronically delivering the images and associated information through the Mobile Banking Software to us or our designated processor. The Mobile Device must capture an image of the front and back of each check to be deposited, including the magnetic ink character recognition line on each check, and such other information as required by this Agreement or applicable law. Such other information includes, but is not limited to, certain technical information such as your IP Address, Mobile Device identifier, and may also include your longitude and latitude at the time the image is transferred to us.

Eligible Items. You agree only to capture images of "**checks**" as that term is defined in Federal Reserve Regulation CC ("**Reg. CC**"). When the image is converted to an Image Replacement Document for subsequent presentment and collection, it shall be deemed an "**item**" within the meaning of Articles 3 and 4 of the Uniform Commercial Code.

You agree to not capture images of any of the following types of checks or other items which shall be considered ineligible items:

- Checks payable to anyone other than the owner of the account in to which it is being deposited;
- Checks containing any unauthorized alteration;
- Checks payable jointly, unless deposited into an account with the names of all payees;
- Checks previously converted to a substitute check, as defined in Reg. CC;
- Checks drawn on a foreign bank and/or that are not payable in United States currency;
- Checks that are payable on sight or payable through drafts, as defined in Reg. CC, or are remotely created checks, as defined in Reg. CC;
- Checks that are undated, post-dated, or are dated 6 months or more prior to the date of deposit;
- Checks with any endorsement on the back other than that specified in this Agreement;
- Checks that have previously been deposited by any remote capture or physical delivery;

- Checks that have previously been returned unpaid for any reason;
- Travelers Checks;
- Savings Bonds;
- Checks payable to "Cash;"
- Checks transmitted from outside the United States;
- Registered government warrants;
- Money Orders;
- Government checks of any type, state or federal; or
- Checks that are prohibited by our current procedures relating to the mobile remote deposit capture feature, or which are otherwise not acceptable under the Deposit Account Agreement, or as we may otherwise determine in our sole discretion.

We may in our sole discretion, and without liability to you, refuse any check for any or no reason, or elect to take the check on a collection basis only. We reserve the right to charge back to your account, at any time, any item that we subsequently determine was an ineligible item. We are not liable for any loss, costs, or fees you may incur as a result of our chargeback of an ineligible item.

Endorsements and Procedures. You agree to restrictively endorse any item transmitted through the Mobile RDC Service as follows: sign the back of your check with your name and the words "**FOR MOBILE DEPOSIT TO ZiFi**" or as otherwise instructed by us. You agree to follow all other procedures and instructions for use of the Mobile RDC Service as we may establish from time to time.

Image Quality. The image of a check or item transmitted to us using the Mobile RDC Service must be legible and must comply with the requirements established from time to time by us, applicable law, or clearing house or association rule. We shall not be liable to you for failure to process or improperly processing any item for which you have not provided an accurate and legible image, and we reserve the right to reject any deposit.

Receipt, Security and Errors in Transmission. Use of the Mobile RDC Service involves the electronic transmission of information across the networks of your wireless service provider and others that we do not operate or control. You accept the risk, and we bear no responsibility or liability, for the quality, privacy, security or act or actual delivery of wireless data transmissions, or the disclosure of information through such errors. An image of an item shall be deemed received when you receive a confirmation from us that we have received the image.

Receipt of such confirmation does not mean that the transmission was error free, complete or will be considered a deposit and credited to your account.

Keeping and Destroying Checks After Imaging. Upon your receipt of a confirmation from us that we received an image you transmitted, you agree to retain the check for no more than 30 calendar days from the date of the image transmission. After 30 days, you must destroy the check, mark it "VOID", or otherwise render it incapable of further transmission, deposit, or presentment. During the time you retain the check, you must: (1) promptly provide it to us upon request; (2) keep it secure against loss, theft, misplacement or accidental redeposit or transfer; and (3) not intentionally or accidentally redeposit or transfer the item. You agree to indemnify us, hold us harmless, and defend us against any damages, claims or losses suffered or alleged by any person arising from the check (or a substitute check therefore) being deposited, negotiated, purchased or transferred after your remote deposit. Intentional, knowing or reckless use of the check after remote deposit may constitute fraud and/or criminal offense.

Availability of Funds. In general, if an image of an item you transmit through the Mobile RDC Service is received and accepted before 4:00 p.m. Eastern Time on a Business Day that we are open, we consider that day to be the day of your deposit, subject to the other terms and conditions herein. Otherwise, we ordinarily consider that the deposit was made on the next Business Day we are open.

Funds deposited using the Mobile RDC Service will generally be made available by the third Business Day from the day of deposit. However, we generally make the first $275 of the aggregate of your checks deposited through the Mobile RDC Service on each Business Day available by the next Business Day. We may delay the availability of your funds for a longer period of time at our discretion if we deem it appropriate in accordance with our policies and procedures.

Deposit Limits. The Mobile RDC Service may apply dollar limits to each deposit account (provided that the deposit account is an Eligible Account, and the Eligible Account has been enabled to use the Mobile RDC Service) and generally the dollar limits, if any, should appear when you use the Mobile RDC Service. If you are unable to deposit one or more checks through the Mobile RDC Service, please call Client Support as set forth in Section 3 above to obtain further information. We reserve the right to change the dollar amounts and/or number of checks allowed within the Mobile RDC Service at any time and without notice. For example, higher limits may be made available in our sole discretion for certain qualified accounts, but those higher limits: (a) may not appear in the Mobile Software; and (b) may be revoked at any time by us for any or no reason without notice (in which case the standard deposit limits disclosed apply).

Presentment. The manner in which the items are cleared, presented for payment, and collected shall be in our sole discretion and subject to your Account Agreements.

Termination. We may suspend or terminate your use of the Mobile RDC Service at any time without cause, but your prior representations, warranties and obligations shall remain in full force and effect. Without limiting the foregoing, your use of the Mobile RDC Service may be terminated if you breach any term of this Agreement, if you use the Mobile RDC Service for any unauthorized or illegal purposes, or you use the Mobile RDC Service in a manner inconsistent with the terms of any other agreement you may have with us.

Mobile Banking Software Restrictions. You agree and acknowledge that: (i) the Mobile Banking Software will only be used in accordance with this Agreement; (ii) the Mobile Banking Software cannot be reassigned or otherwise be transferred for access and/or use to a third party; and (iii) you will not assist or permit others to disassemble, decompile, reverse engineer the Mobile Banking Software or other otherwise attempt to derive the source code (or the underlining ideas, algorithms, structure or organization) of the Mobile Banking Software.

38. AUTOMATED CLEARING HOUSE ("ACH") SERVICE

Scope. Subject to credit and other approvals by us, credit limits established by us, and your acceptance of required Related Documents, you can use the business Channels of Digital Banking to submit files to originate the following types of domestic ACH transfers ("**Entries**"):

ACH transactions for credit to payee purposes.

NACHA Rules. You agree and acknowledge that you authorize us to be the Originating Depository Financial Institution ("ODFI") in order to transmit ACH transactions in your name as the originator ("Originator") and to comply with the Operating Rules and Guidelines of the National Automated Clearing House Association ("**Nacha**") as amended from time to time (collectively the "Rules"). Also you agree and acknowledge that your ACH transactions will comply with all applicable law, including, but not limited to, U.S. law, such as the rules, sanctions and executive orders that: (i) prohibit you from transacting with certain people, entities, countries, and officials; and (ii) prohibit you from transacting with a person when such person is located in certain countries. You and we are bound by the Rules for all Entries, whether or not an Entry is sent through an automated clearing house. You can obtain a copy of the current Rules at https://www.nacha.org or by telephoning Nacha at (703) 561-1100. As used in this Agreement, "Entries" includes both the meaning provided in the Rules, and also entry data you submit from which we may prepare Entries.

You must submit your Entries to us in the manner we designate, including any terms or instructions that may be presented to you on-screen when submitting Entries. Unless we have otherwise agreed in writing after credit underwriting, you must submit ACH credit Entries to us two Business Days before the payment date. Also, you agree and acknowledge that you are prohibited from initiating any IAT transactions through Digital Banking as we only allow domestic ACH Entries in U.S. dollars. Further, you agree and acknowledge that we reserve the right to impose further restrictions on the types of ACH Entries we will allow you to initiate with or without notice and at any time in our sole discretion.

Funding. **All ACH credit files must be pre-funded unless otherwise agreed in a separate writing signed by us.** "Pre-funded" means that we will debit your offset (i.e., payment) eligible Deposit Account for an amount equal to the total of your ACH file. That offset will be made on the day your file is sent to the ACH network for processing (i.e., typically two Business Days prior to the transaction effective date). However, for same day or next day ACH credit transactions, the offset will be made at the moment you schedule each ACH credit transaction. Each ACH file you send to us will consist of one or more batches of ACH Entries. Sufficient available funds must be in your offset eligible Deposit Account at the time the batches are processed. If you do not have sufficient available funds at the time of offset for all batches, then we will process only those batches for which you have sufficient available funds, in the order those batches appear within your file. Batches for which you do not have sufficient available funds will be rejected and therefore not processed by us.

If we do not require your file to be prefunded, we may still refuse your ACH credit file if you have insufficient available funds in your eligible Deposit Account on the date we initiate the transaction (e.g., two Business Days prior to the Settlement Date) or before we start processing (e.g., for same day ACH instructions). We may also require you to maintain sufficient available funds in your eligible Deposit Account prior to processing of your files. We may also place a hold on funds pending processing of your files. If we have reason to believe you may not have adequate available funds to cover your ACH file, we may delay execution until we receive adequate assurance from you that the funds will be available.

Unfunded batches may be deleted by the Bank in its sole discretion.

If we, in our sole discretion, choose to execute any file that hasn't been prefunded and for which you lack adequate sufficient available funds in your eligible Deposit Account, you agree to immediately pay any resulting overdraft and overdraft fees, and you authorize us to collect those amounts on the date of the transaction, or any time thereafter and without prior notice, by debiting any deposit account you have with us or by advancing funds under any credit account you have with us. You acknowledge that online balances information may not include all recent transactions in your eligible Deposit Accounts, and that balances may reflect funds that are not available for immediate withdrawal. Nothing in this Agreement or any course of dealing shall constitute a commitment or obligation to lend money to you.

Cutoff Hours and Timing of ACH Files. You agree and acknowledge that we generally require at least two Business Days before the Settlement Date to execute your ACH credit files or instructions to pay one or more persons through the ACH Service. However, we may allow you, in our sole discretion, to submit ACH instructions in connection with the ACH Service at least one Business Day before the Settlement Date or on the same Business Day. The cutoff hour for providing non-same day ACH credit files or instructions to pay one or more persons through the ACH Service is 4:00 p.m. Eastern Time on a Business Day. However, the cutoff hour for providing same day ACH credit files or instructions to pay one or more persons through the ACH Service is 1:00 p.m. Eastern Time. You agree and acknowledge that if you give us ACH instructions through the ACH Service after the applicable cutoff hours or on a non-Business Day, then your ACH instructions will be deemed to be given to us on the next Business Day.

Account verification. You agree and acknowledge that before you initiate a live Entry for a new Receiver, you will first engage in an acceptable method of account verification as set forth under the Nacha rules, this may include, but is not limited to, initiating prenotes or micro deposits. However, you agree that we may at any time require that you use a particular method and unless we do so, you are responsible for using such an acceptable method as prescribed under the Nacha rules. Further, you agree that you will not send any Entry when an account verification method has failed or has been inconclusive, such as when an Entry has been rejected or returned, unless you have first corrected the reason for the failure or inconclusiveness.

Authorization and Record Retention. You will initiate Entries only with the prior written authorization of the owners of the accounts that are affected by such Entries. You agree to maintain a copy of each authorization for a period of two years following its termination, and to provide us with a copy upon request. For any warranty that we are deemed by law, the Rules or other payment system rules to make to others regarding your Entries, you make the same warranty to us.

Your Instructions. We are not responsible for detecting or rejecting duplicate Entries or files. If you give us an Entry or file that is incorrect in any way, we may charge your eligible Deposit Account for the payment whether or not we could have detected the error. Your Entries and files must accurately describe your transaction beneficiaries/receivers, intermediary financial institutions, the beneficiaries'/receivers' financial institutions, beneficiaries'/receivers' accounts, and intended payment/effective dates. If you describe any beneficiary/receiver or institution inconsistently by name and number, we and other institutions are entitled to process your instruction solely on the basis of the number even if the number identifies a person, entity or institution different from the one you named. If we allow you to select a financial institution's numeric identification (e.g., routing and transit number) by entering or selecting the institution's name, then you are solely responsible for entering the correct name of that institution.

Cancellation, Amendment and Reversal of ACH Files or Entries. Digital Banking may provide an online tool to cancel an ACH file that has not yet begun processing. You can also cancel files that have not begun processing by calling Client Support at (800) 341-73031. A file which has begun processing cannot be cancelled or amended.

To cancel one in a series of recurring files, we may require that you cancel the series and reschedule the remainder of the series. We may permit you to amend a scheduled file, or may require that you cancel it and reenter the desired file.

If we attempt to reverse an Entry or file at your request, we shall have no liability for any interest or losses that result if the attempt is not successful. You agree to reimburse, indemnify, defend, hold us harmless for all expenses, losses, claims, actions, proceedings and damages we may incur in effecting or attempting to affect your requested reversal. You are solely responsible for providing notice to beneficiaries/receivers that a reversal is being attempted and the reason for the reversal no later than the Settlement Date of the reversal.

Rejections. We may reject any Entry or file if: (a) it does not conform to the limitations, security procedures or other requirements set forth in this Agreement; (b) there are insufficient unencumbered funds in your eligible Deposit Account; (c) it is not authenticated to our satisfaction or we have reason to believe it may not be authorized (notwithstanding compliance with any security procedure); (d) it contains incorrect, incomplete, or ambiguous information; (e) it exceeds any established dollar limits; (f) we believe the beneficiary may be on the list of Specially Designated Nationals and Blocked Persons issued by the U.S. Treasury's Office of Foreign Assets Control (which may require us to not complete the transfer and to "block" the funds until that Office issues a written release); (g) it appears to us to potentially be in contravention of applicable law, regulation, executive order or payment system rules; (h) it would cause us to exceed any limitation on our intraday net funds position established pursuant to Federal Reserve guidelines; (i) it would result in violation of any other law or regulation, or any applicable governmental or Nacha risk control program; or (j) it presents any other risk to us that we in our discretion deem unreasonable. We may notify you of our rejection orally, electronically, or in writing, no later than two Business Days after the date the Entry or file was to be affected. We are not required to pay you interest on a transfer for the period between the rejection and your receipt of the notice of our rejection.

Notice of Returns. We may notify you electronically, in writing, by telephone, or otherwise, such as recrediting your ZiFi Business Checking or other eligible Deposit Account, regarding any Entry or file that is rejected or returned for any reason. We are not obligated to credit your eligible Deposit Account with any interest unless the return is caused by our failure to properly execute the Entry or file. We may attempt to reprocess the Entry or file if the return is due to our error and we have sufficient data to do so. You agree to reimburse us promptly for the amount of any ACH debit or other debit to another account that is reversed, adjusted or returned. You may not resubmit any ACH debit or other debit if the payment was stopped by the account owner.

Provisional Credit. Under the Rules, if you originate an ACH credit entry transferring funds to a receiver, any credit given by the receiving financial institution to the receiver's account is provisional until the receiving financial institution receives final settlement. If final settlement does not occur, then the receiving financial institution is entitled to a refund of that provisional credit, and you will not have paid the amount of that credit transfer to your receiver. In addition to the Rules, you agree that any amount we credit to your eligible Deposit Account for any funds transfer to you is provisional until we receive final settlement through a Federal Reserve Bank (or payment is otherwise made as provided in Article 4A-403(a) of the Uniform Commercial Code), and we are entitled to a refund from you of that provisional credit if final settlement does not timely occur.

Audit. You hereby grant us the right (but we shall have no duty) to audit from time to time your practices, procedures and controls in originating Entries, prenotifications and ACH files, and your compliance with the Rules and the terms of this Agreement (collectively "Order Controls"). You agree to cooperate with our audit, and you are responsible for providing us access to the personnel, records and facilities of any third-party contractor or vendor you may employ in using our funds transfer services, as reasonably necessary to complete our audit of your Order Controls. You also agree to provide us with copies of reports you may create or receive of audits conducted by you or third-parties concerning your Order Controls. You agree to reimburse and indemnify us for any penalties, fines and/or charges that we may incur as a result of your failure to comply with this Agreement, the Rules or applicable law.

39. SECURE MESSAGES

The Secure Messages feature provides a method for you to communicate with the Bank in connection with questions regarding Digital Banking services. The Secure Messages feature should provide you with information to either answer your question or provide you with next steps in order to help answer your question. You agree and acknowledge that the Secure Messages feature cannot be used to give the Bank one or more instructions to move funds. However, you may use the Secure Messages feature to request one or more forms to start a claim for unauthorized use or file a dispute.

PART C – DEFINITIONS

Part C sets forth the definitions of terms utilized elsewhere in this Agreement and for purposes of this Agreement.

Access Credentials means one or more username, password, identification number, one-time passcode, security question and answer, biometric identification (e.g., fingerprint or facial recognition) or other means of identification and authentication, or combination thereof, that we require for signing in to or otherwise accessing Digital Banking or a particular function of the service.

Account Agreements means all agreements and disclosures specifically governing your Eligible Accounts (including without limitation the Deposit Account Agreement, credit card agreements, loan agreements, rate and fee schedules, applications and disclosure statements, and credit agreements).

Authorized User means an individual who has been granted Access Credentials by your Primary Administrator to use Digital Banking as your authorized agent and includes any Primary Administrator.

Business Customers mean persons, who generally are businesses, that have a financial relationship with us and have established their Deposit Accounts for non-consumer purposes. Such persons include, but are not limited to, sole proprietorships, partnerships, limited liability companies and corporations.

Business Day means every Monday through Friday, excluding Federal Reserve holidays or other days that banks are legally closed.

Business Online Banking means the web-based Digital Banking services we make available to Business Customers via our Website.

California Commercial Code shall have the meaning as set forth in CA UCC 1101 et. seq., as it may be amended from time to time.

Channel means, depending on the context, either both and/or either Business Online Banking and Mobile Banking. Business Online Banking and Mobile Banking is a "Channel" for accessing Digital Banking. Not all Channels may be available to all customers.

Communications mean any electronic communication between you and us using the Digital Banking service itself, including, but not limited to, submitting or acknowledging Orders for payments, amendments and cancellations of Orders, electronic messages through Digital Banking's Secure Messages feature, your customer profile updates, entering into and accepting Related Documents, and a business Channel Primary Administrator performing self-administration functions.

Client Support means the dedicated team at the Bank that provides customers with assistance in connection with Digital Banking.

eDocument Communications mean any statement, notice, disclosure, agreement, fee schedule, transaction or event record, invoice, response to a claim or other communication regarding your deposit accounts that we choose to provide by eStatement or eNotice instead of paper. "eDocument Communication" also includes eTax Documents that we make available.

eDocuments Service means the eStatements, eNotices and/or eTax Documents service(s) for your deposit accounts.

eStatements means an electronic version of the paper account statement, including notices, disclosures and other information that would be printed on or with the paper statement.

eNotices means any eDocument Communication that is not an eStatement or eTax Documents.

eTax Documents means any IRS tax reporting form that we make available for electronic delivery. We may from time to time, in our sole discretion, add or delete which IRS forms are included as eTax Documents.

Deposit Account means any ZiFi Business Checking, ZiFi Business Savings or other deposit account with us that we have enrolled as eligible for one or more Digital Banking services.

Deposit Account Agreement means our standard agreement governing your Deposit Accounts (together with its associated rate sheets, if applicable, fee schedules and disclosures), as amended from time to time.

Digital Banking means the digital banking services that we make available to Business Customers who accept this Agreement and are enrolled in our Business Online Banking and/or Mobile Banking Channels. Digital Banking also includes services that are available within one or more Channels after additional enrollment and/or acceptance.

Dual Control means the requirement that Orders must be initiated and approved using the separate Access Credentials of two Authorized Users.

Eligible Account means your Deposit Account or Loan Account with us that are enrolled, in accordance with our procedures, to make such accounts accessible through Digital Banking. Some types of deposit and loan accounts cannot be enrolled, or, if enrolled, enrolled with limited access and use of one or more Digital Banking services. The types of accounts that can be enrolled are subject to change from time to time without prior notice.

Internal Advance means any transfer, if, and when allowed, from a Loan Account to a Deposit Account with us, as provided under the Section entitled, "Loan Advance" above.

Internal Transfer means any transfer of funds to and from any of your Deposit Accounts, as indicated or provided for under the section entitled "Internal Transfers" above.

Loan Account means any loan that is eligible for one or more Digital Banking services.

External Transfer means any transfer from your deposit account held at another financial institution in order to make a deposit into any one of your Deposit Accounts with us or a transfer from any one of your Deposit Accounts in order to make a deposit to your deposit account held at another financial institution, as provided under the Section entitled, "External Transfers" above.

MFA means multi-factor authentication where, as part of the Security Procedures, Digital Banking may require a user to use multiple authentication methods. MFA combines two or more independent Access Credentials. For example, if a particular transaction or feature is deemed by us, in our sole discretion, to be a certain risk or sensitive, then we may ask for additional Access Credentials from the user (e.g., step-up authentication), such as a one-time passcode ("OTP") before we will allow the transaction or feature to be submitted through Digital Banking. For security reasons, you must provide us with a valid mobile number in connection with a device that is SMS enabled, along with a valid phone number available to receive a phone call for a voice-speaking one-time passcode (OTP). You agree and acknowledge that MFA requires an accurate mobile phone number, and we only support using SMS or phone for MFA destinations.

Mobile Banking means the Digital Banking services we make available to customers via their Mobile Devices and Mobile Banking Software.

Mobile Banking Software means software permitted by us that you have downloaded for conducting Mobile Banking transactions.

Mobile Device means a cellular telephone, tablet, or similar wireless communication device with the appropriate hardware and operating system that: (a) is installed with Mobile Banking Software; or (b) that can conduct mobile banking transactions by using other protocols we may choose to permit (e.g., Wireless Application Protocol (WAP) or text (SMS) messaging).

Online Banking means using Digital Banking services through a web browser instead of through a mobile banking app.

Orders mean one or more instructions given to the Bank in your name to pay an amount of money, which is funded by debiting your eligible Deposit Account or otherwise receiving payment from you, to a beneficiary.

Payment Account means the deposit account that you may be asked to designate as the payment account for selected related services that you access through Digital Banking.

Primary Administrator means an individual whose Access Credentials include the Digital Banking service's self-administration functionality. You are required to have at least one Primary Administrator at all times. **(Your Primary Administrator is your authorized agent in all matters regarding Digital Banking.)**

Regulation CC or **Reg CC** shall have the meaning as set forth in 12 C.F.R. 229, as it may be amended from time to time.

Related Documents means any application, fee schedule, disclosures, set-up forms, specifications or addenda concerning the Digital Banking service. Related Documents can include, but are not limited to, terms for: (A) optional or related functions that are accessed within or via Digital Banking; (B) special conditions under which we are willing or unwilling to provide certain portions of Digital Banking; (C) linking the Digital Banking service of two or more customers in approved cases; or (D) otherwise amending this Agreement. A Related Document is not required to state it is a Related Document.

Note: references in a Related Document to our "internet banking," "online banking," "business online banking," or "mobile banking" (or the like) service or agreement, shall be deemed references to Digital Banking, its Channels, and this Agreement, all as the context requires.

Security Procedures mean the Access Credentials and any additional or modified authentication tool or method we make available now or in the future (such as, but not limited to, MFA, Dual Control, security codes, personal identification numbers, procedures, algorithms, or key strokes, call backs or any other out of band authentication tool or method), to authenticate any Communications, including Orders, received by us in your name and/or prevent unauthorized access and/or use of a service provided by Digital Banking.

Service or Services shall mean one or more of the services described in this Agreement.

Uniform Commercial Code shall have the meaning as provided by the Uniform Law Commission and as adopted by the applicable state as the law of the state governing commercial transactions.

Website: Our Website, and all related web pages, for offering Online Banking services, enrolling Eligible Accounts and/or performing, authorizing, or canceling any specific Online Banking service transaction is ZiFi Bank at ZiFi.com.