

# Digital Banking Service Agreement (Consumer & Business)

(Version August 2019)

This Digital Banking Service Agreement ("Agreement") governs the Digital Banking services (online and mobile) that Zions Bancorporation, N.A. ("we", "us" or "our") provides to consumer and business customers ("you"). Zions Bancorporation, N.A. operates through divisions with trade names that include **Amegy Bank, California Bank & Trust, National Bank of Arizona, Nevada State Bank, Vectra Bank Colorado** and **Zions Bank** (each a "Division"). Important capitalized terms are defined in Section 3.

## 1. ACCEPTING THIS AGREEMENT

Before using the Digital Banking service, you must both (a) consent to receive disclosures, notices and other communications electronically, and (b) read and accept this Agreement. You agree that you are deemed to automatically renew your consent and acceptance each time you log in and use Digital Banking.

The current version of this Agreement can always be viewed online at your Division's Website (listed in Section 3 below). SECTION 3 OF THIS AGREEMENT INCLUDES DISPUTE RESOLUTION PROVISIONS, INCLUDING A WAIVER OF RIGHTS TO TRIAL BY JURY.

## 2. CONSENT TO ELECTRONIC DISCLOSURES, COMMUNICATIONS AND RECORDS; SYSTEM REQUIREMENTS

You should print or electronically save a copy of the following Consent and the remainder of this Agreement for your records.

Your consent in this Section 2 to electronic delivery of disclosures and other information, and to the use of electronic records, shall govern all of your Digital Banking services, including services that require you to also accept Related Documents (e.g., service agreements for Bill Pay, Popmoney, Zelle, External Transfers, Online Wires, etc.) Any similar consent in a Related Document that you have already accepted or accept hereafter shall be in addition to (and not limit) your consent in this Section 2.

**Consent.** We are required to disclose certain information to consumers in writing. With your prior consent, however, we can provide that information electronically rather than by paper. We also need your general consent to use electronic communications and records for certain consumer and business transactions.

By accepting this Agreement, you hereby consent and agree to: (a) our delivering disclosures, notices and any other information (including this Agreement) in only electronic form, even those required by law to be provided in writing, and (b) our using electronic records and communications with you in connection with Digital Banking. Your consent extends to each Eligible Account that you now or hereafter enroll in Digital Banking.

You agree that your use of Digital Banking to electronically authorize, instruct or interact with us (including but not limited to ordering a funds transfer, making a bill payment, borrowing from or paying a credit account, applying for or activating or accepting the terms of an additional service feature or related service, accepting Related Documents, accepting or receiving documents or notices, and self-administering your Digital Banking service or its settings or configurations) shall have the same force, effect and authority as if signed by you and delivered to us by paper.

**Canceling.** You may at any time withdraw your consent to electronic delivery instead of paper by calling or writing your Division's Customer Service, but we may then terminate your ongoing use of Digital Banking (and not process any previously-scheduled future payments). **Your Customer Service phone number and address are in Section 4.** Your consent for this Agreement is in addition to any other consents to electronic delivery you may have given in

separate agreements with us (whether or not Related Documents). Withdrawing your consent under this Agreement will not by itself cancel your consents for electronic delivery in those separate agreements.

**System Requirements.** To use Digital Banking and receive electronic disclosures and other communications: you must be enrolled and activated in at least one of our Digital Banking “Channels” (defined below); your computer and/or Mobile Device must use commonly accepted and recently updated software for reading and saving PDF and HTML documents; you must be connected to Digital Banking via your internet service provider or your mobile communications data service provider; your computer or Mobile Device must use a commonly accepted and recent updated version of an HTML compliant web browser that supports Transport Layer Security (“TLS”) encryption; you must have, maintain, provide and update us with your valid, active email address(es) for use in sending, receiving and retaining disclosures and other communications with Digital Banking; and you must be able to connect to websites via hyperlinks in email. For Mobile Banking, you must also have the most recent version of our Mobile Banking Software installed on your Mobile Device, have your Mobile Device and mobile phone number registered with Digital Banking, and have your Mobile Device enabled for SMS text messaging. 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). We may (but are not required to) deny service (1) if security features of your software, computer or Mobile Device have not been updated, or have been disabled or modified (e.g., a “jailbroken” mobile device), or (2) if you are using a disposable (e.g., “burner”) mobile device.

You hereby confirm to us that you have (1) the system required described above, and (2) verified your hardware and software, and your ability to access, view and print or electronically save (including taking screenshots) electronically delivered disclosures and communications. If you are not able to access, view and print or save such notices and disclosures, you must not enroll in or use Digital Banking.

**Electronic Delivery.** 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 SMS text message to any Mobile Device telephone number you may have provided to us for banking services (including but not limited to any Digital Banking service or function); (iii) by display on your screen or other “in-product” message or alert during your Digital Banking activity; (iv) by posting it to your Division’s Website, an Online Banking message center, or in our Mobile Banking Software; (v) by message printed on the periodic statement for your Eligible Accounts if you have agreed to receive that statement electronically; (vi) any other electronic means that you have authorized elsewhere (e.g., our eNotices service) or hereafter authorize; or (v) any other electronic means that is commercially reasonable and within the system requirements described above. Any of the foregoing methods of electronic delivery may be used for any Digital Banking service that requires logging into Digital Banking to use (e.g., Online Wires, External Transfers, Bill Pay, Popmoney or Zelle), even if that other function has its own terms and conditions that do not themselves list the foregoing methods of electronic delivery.

Electronic disclosures can include, without limitation, prior notice to you of preauthorized debits that vary in amount to your Eligible Accounts; notices of pending or processed payment instructions; notices of receipt of payments or deposits; notices of adjustments made to transactions; notices regarding service availability or suspension; and notices about operational or legal changes to Digital Banking, including notices of amendment to this Agreement.

**Change in Contact Information.** You are solely responsible for advising us of any change in your email, mobile device telephone number, or other electronic or postal addresses you use for Digital Banking or your Eligible Accounts. You can do so by calling or writing your Division’s Customer Service (see Section 4). We encourage you to simultaneously update your addresses within the separate general services section of your Division’s Website.

**Paper Copies.** We do not charge for electronic delivery. We ordinarily do not send paper copies of electronic communications. You may request a paper copy of an individual prior electronic notice or disclosure by calling or

writing your Division's Customer Service (see Section 4). Ordinary copy fees as disclosed for your Eligible Accounts shall apply.

### **3. INTRODUCTION; DISPUTE RESOLUTION; AND DEFINITIONS**

This Agreement governs our Digital Banking services for both consumer and business customers. Where specified, however, portions of this Agreement pertain only to consumers or only to business customers. We may choose to exclude any or all minors from enrolling in Digital Banking or using selected features.

Not all Digital Banking functions may be available in all Channels. (For example, remote deposit capture may be only in Mobile Banking; stopping checks may not be available in Mobile Banking; and consumer customers may not be able to send ACH files.) Features in Digital Banking or individual Channels made be added, deleted or changed without prior notice. To use Digital Banking with Eligible Accounts at more than one Division of Zions Bancorporation, N.A., you must separately enroll in each such Division's independent digital banking service. For purposes of cutoff times, posting and funds availability, and methods of execution, transfers between accounts at different Divisions of Zions Bancorporation, N.A. may be processed as transfers between separate banks (e.g., by ACH rather than as internal book transfers).

This Agreement is supplemented by the terms of your Deposit Account Agreement and other "Account Agreements" (defined below), but this Agreement governs over any conflicting terms therein with respect to Digital Banking. This Agreement is also supplemented by the terms of "Related Documents" (defined below) you have already accepted or may accept hereafter. If a provision in this Agreement directly conflicts with a specific provision in a Related Document, the Related Document shall govern. However, Section 2 hereof ("Consent to Electronic Disclosures, Communications and Records; System Requirements") shall govern over any conflicting provision in any Related Document. Otherwise, our rights (including the benefit of limitations of liability and indemnification) and your responsibilities under this Agreement, the Related Documents and the Account Agreements are intended to be cumulative.

**Dispute Resolution; Jury Waiver.** Except as may be prohibited by applicable law, you and we both hereby waive any rights to have a jury hear or decide any dispute between us, and hereby agree that the dispute resolution provisions found in your Deposit Account Agreement 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 Agreement, or any Digital Banking transaction.

**Definitions.** As used in this Agreement:

**Access Credentials** means one or more login ID, password, identification number, token, biometric identification (e.g., fingerprint or facial recognition) or other means of identification and authentication, or combination thereof, that we require for logging into 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** (*for Business Online Banking or Business Mobile Banking only*) means an individual who has been granted Access Credentials by us, or by your CSA to use Digital Banking as your authorized agent. If your Eligible Accounts are linked to the profile of another customer, then that customer's Authorized Users are deemed to be your Authorized Users as well.

**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.

**Channel:** each of Consumer Online Banking, Business Online Banking, Mobile Banking (associated with Consumer Online Banking), and Mobile Banking (associated with Business Online Banking) is a “Channel” for accessing Digital Banking. Not all Channels are available to all customers.

**Customer System Administrator, or CSA, (for Business Online Banking or Business Mobile Banking only)** means an Authorized User whose Access Credentials include the Digital Banking service’s self-administration functionality. You are required to have at least one CSA. **(Your CSA is your authorized agent in all matters regarding Digital Banking.** See the Subsection below entitled “Your Customer System Administrator.”) If your Eligible Accounts are linked to the profile of another customer, then that customer’s CSAs are deemed to be your CSAs as well.

**Consumer Online Banking** means the web-based Digital Banking service we make available to consumer customers via our Website.

**Deposit Account** means any checking, savings or other deposit account with us that you have enrolled as an Eligible Account.

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

**Digital Banking** means the digital banking services that we make available to customers who accept this Agreement and enroll in our Consumer Online Banking, Business Online Banking, and Mobile Banking Channels. Digital Banking also includes services that are available within one or more Channels after additional enrollment and acceptance of Related Documents (e.g., Bill Pay, Popmoney, Zelle, External Transfers and Online Wires).

**Eligible Account** means your Deposit Account or Loan Accounts with us that you have enrolled, in accordance with our procedures, to make such accounts accessible through Digital Banking. Some types of deposit and loan accounts cannot be enrolled. The types of accounts that can be enrolled is subject to change from time to time without prior notice.

**Internal Advance** means any transfer from a Loan Account to a Deposit Account with us, as provided under the section entitled “Transfers” below.

**Internal Transfer** means any transfer of funds from any of your Deposit Accounts to (a) any of your Deposit Accounts, or (b) an account that another person holds with us, as provided under the section entitled “Transfers” below.

**Loan Account** means any of your overdraft protection accounts (e.g., Reddi-Credit, Reddi-Reserve or Cash Reserve accounts), credit card accounts or other loans with us that is enrolled as an Eligible Account.

**Mobile Banking** means the Digital Banking services we make available to consumer customers and business 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 Banking Software and the features therein differ for consumer customers and business customers.

**Mobile Device** means a cellular telephone, tablet or similar wireless communication device (a) that is installed with Mobile Banking Software, or (2) 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 Consumer Online Banking and Business Online Banking, collectively.

**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 (e.g., Bill Pay), or (B) special conditions under which we are willing or unwilling to provide certain portions of Digital Banking, or (C) linking the Digital Banking service of two or more customers (e.g., permissible affiliates) 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.

**Website:** Your Division’s current or future Internet 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. Your Division’s current Website is listed below. Your Division Website depends on which Division of Zions Bancorporation, N.A. provides your Digital Banking service:

<u>Customers of:</u>	<u>Division Website:</u>
Amegy Bank	<a href="http://www.amegybank.com">www.amegybank.com</a>
California Bank & Trust	<a href="http://www.calbanktrust.com">www.calbanktrust.com</a>
National Bank of Arizona	<a href="http://www.nbarizona.com">www.nbarizona.com</a>
Nevada State Bank	<a href="http://www.nsbank.com">www.nsbank.com</a>
Vectra Bank Colorado	<a href="http://www.vectrabank.com">www.vectrabank.com</a>
Zions Bank	<a href="http://www.zionsbank.com">www.zionsbank.com</a>

#### 4. CUSTOMER SERVICE

The telephone number and address for your Customer Service depends on which Division of Zions Bancorporation, N.A. provides your Digital Banking:

<u>For Customers of:</u>	<u>Call:</u>	<u>Or write:</u>
Amegy Bank	(888) 500-2960	P.O. Box 30709 Salt Lake City, UT 84130
California Bank & Trust	(888) 217-1265	P.O. Box 30709 Salt Lake City, UT 84130
National Bank of Arizona	(800) 497-8168 option 4.	P.O. Box 30709 Salt Lake City, UT 84130
Nevada State Bank	(888) 835-0551	P.O. Box 30709 Salt Lake City, UT 84130
Vectra Bank Colorado	(800) 884-6725	P.O. Box 30709 Salt Lake City, UT 84130
Zions Bank	(800) 974-8800	P.O. Box 30709 Salt Lake City, UT 84130

#### 5. AVAILABLE ONLINE AND MOBILE BANKING SERVICES

With Digital Banking, you may enroll your Eligible Accounts and may then access their balances, transaction history and other information. You may also conduct the types of transfers described in the section below entitled

"Transfers." You may also be able to use related services (e.g., Bill Pay, Popmoney, Zelle, External Transfers and Online Wires) agreeing to Related Documents for those features. We may, from time to time, offer and introduce new electronic banking services. All current and future services will be governed by this Agreement and any service-specific Related Documents. Not all Digital Banking functions are available in every Channel.

## **6. PROTECTING YOUR ACCOUNTS: ERRORS & QUESTIONS; UNAUTHORIZED TRANSFERS; ACCESS CREDENTIALS; AND SECURITY PROCEDURES**

**6.1 Error Resolution Notice (Consumers Only)** – In case of errors or questions about your electronic transfers: call or write Customer Service at the telephone number or address listed 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. We must hear from you no later than 60 days after we sent or made available the FIRST statement on which the problem or error appeared. (1) Tell us your name and account number (if any); (2) Describe the error or the transfer you are unsure about and explain as clearly as you can why you believe it is an error or why you need more information; and (3) Tell us the dollar amount of the suspected error. If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days (5 business days for Visa® debit card point-of-sale transactions processed by Visa, or 20 business days if the transfer involved a new account) after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days (90 days if the transfer involved a new account, a point-of-sale transaction, or a foreign-initiated transfer) to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days (5 business days for Visa® debit card point-of-sale transactions processed by Visa, or 20 business days if the transfer involved a new account) for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account. Your account is considered a new account for the first 30 days after the first deposit is made, unless each of owner already had an established account with us before the affected account was opened.

We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation. Timeframes described herein may be different if your error or question does not claim unauthorized activity. You may ask for copies of the documents that we used in our investigation by calling Customer Service at the number listed above.

**6.2 Unauthorized Transfers and Limits on Your Liability (Consumers Only).** Tell us AT ONCE if you believe any of your Access Credentials have been lost or stolen, or if you believe that an electronic fund transfer has been made without your permission using information from your check. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account (plus your maximum overdraft line of credit). If you tell us within 2 business days after you learn of the loss or theft of your Access Credentials, you can lose no more than \$50 if someone used your Access Credentials without your permission. If you do NOT tell us within 2 business days after you learn of the loss or theft of your Access Credentials, and we can prove we could have stopped someone from using your Access Credentials without your permission if you had told us, you could lose as much as \$500. Also, if your statement shows transfers that you did not make, including those made by Access Credentials, debit card, code or other means, tell us at once. If you do not tell us within 60 days after the statement was sent or made available to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time.

**6.3 Protect Your Access Credentials.** Your Access Credentials are used to gain access to Digital Banking and must be kept confidential at all times. For your protection, we strongly recommend you change your Access Credentials regularly (at least every 60 days). It is recommended that you memorize your Access Credentials and do not write them down. You are responsible for keeping your Access Credentials, account numbers and other account data confidential. (For Business Customers, references to "your Access Credentials" include Access Credentials that are

issued to or by your Authorized Users. Access Credentials issued to your Authorized Users belong to you, and their use and confidentiality are your responsibility.)

If you have a consumer account that has been linked to a Business Online Banking profile, we may but have no duty to require you to enter Access Credentials for Business Online Banking plus separate Access Credentials (e.g., for Consumer Online Banking) before granting access to your consumer account in the Business Online Banking Channel.

**Note: some software may store Access Credentials to facilitate the 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, regardless of which Channel you enroll in first. For Mobile Banking, we may also permit you to use “alternate” Access Credentials that we make available. Alternate 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 alternate Access Credentials methods can be added, removed, substituted or changed by us from time to time without prior amendment of this Agreement. Alternate 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.**

**For Business Customers:** see also the subsections of this Agreement entitled “Your Customer System Administrator (CSA)” and “Your Authorized Users,” located in the section below entitled “Business Online Banking and Business Mobile Banking Additional Terms.”

#### **6.4 Security Procedure, Additional Security Tools and Your Responsibilities --**

**Agreed Security Procedure.** You agree that Digital Banking’s requirement for entry of valid Access Credentials, consisting of either (1) your company ID (for business Channels), user ID and password, or (2) your biometric identification (e.g., fingerprint or facial recognition) in a Mobile Banking Channel, is a commercially reasonable

“security procedure” for verifying the identity and authority of a person accessing or using Digital Banking, and verifying the authenticity and authorization of Communications made in your name to Digital Banking (the “**Agreed Security Procedure**”). By entering into Related Documents for specific functions (e.g., Online Wires), you and we may establish additional or alternate Agreed Security Procedures for those specific functions. Your assent to Digital Banking security procedures is for purposes that include, but are not limited to, Uniform Commercial Code Article 4A, Funds Transfers, Part 2. “**Communications**” include any electronic communication between 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 to Digital Banking’s messaging center, your customer profile updates, entering into and accepting Related Documents, and a business Channel CSA performing self-administration functions).

Communications shall be deemed made in your name if made using your Access Credentials. You agree and warrant that you have reviewed and determined that the foregoing Agreed Security Procedure is commercially reasonable for your needs, including but not limited to the size, type and frequency of Communications (including Orders) that you will normally send to us. You agree that we, acting in good faith, are entitled to receive, act upon, execute and rely upon any Communications (including Orders) that is verified by the Agreed Security Procedure, that such verified Communications (including Orders) shall be effective as your Communications (including Orders), and that you shall be bound by such verified Communications (including Orders) even if they were not in fact authorized by you. We shall have no obligation to further investigate the authenticity of any Communications that are verified through the Agreed Security Procedure. (**For Consumer Customers:** this paragraph is limited by (i) applicable consumer protection laws (including Regulation E), and (ii) the consumer protection terms and disclosures set forth in this Agreement, your Account Agreements, and your Related Documents.)

After accepting this Agreement, each subsequent use of Digital Banking by you shall constitute a reacceptance and a reaffirmation of your ongoing agreement and warranty that the Agreed Security Procedure remains commercially reasonable for your needs. If our mutual reliance on the Agreed Security Procedure is not (or ceases to be) commercially reasonable for your security needs, then do not enroll (or immediately terminate your enrollment) in Digital Banking.

**Additional Security Tools.** You further agree to enroll in (or, for businesses, to configure through your CSA’s self-administration) such additional security tools as we may make available from time to time for Digital Banking, or specific features of Digital Banking. For example, Digital Banking in business Channels can be configured to require that certain Orders must be initiated and approved using the separate Access Credentials of two Authorized Users (“**Dual Control**”). We also offer certain transaction alerts.

Additional security tools are not part of the “Agreed Security Procedure” that we must satisfy to verify the authenticity of your Communications to us. However, if you choose to not use an additional security tool (such as Dual Control) that we make available to you, then you release and hold us harmless from any loss that you or we may suffer to the extent that such loss could have been detected, prevented, reduced or recovered by your use of that additional security tool. (Note: the foregoing release and hold harmless provision shall not arise from your decision to not use Positive Pay, ACH Positive Pay or IBM® Trusteer Rapport™ software. However, we strongly recommend that you use Positive Pay, ACH Positive Pay and Trusteer Rapport as part of your internal controls. We may contend in court that your failure to do so was negligent and a proximate cause of an experienced loss.

**Other Responsibilities.** If a Communication is not verified pursuant to the Agreed Security Procedure, but we can establish that the Communication originated from you, your Authorized User or your other agent, or was originated to or for your benefit, you shall nevertheless be bound by that Communication. We shall have no liability to you if, despite verification by the Agreed Security Procedure, we delay or do not process a Communication that we in good faith believe or suspect might not be authentic or authorized. We have the right, but no obligation, to present you with challenge questions to help further authenticate your (or your users’) identity, and to deny service if you are unable to answer those questions to our satisfaction at that time. Digital Banking and its security procedures are not designed, and we have no duty, to detect errors in the transmission or



content of your Communications to Digital Banking. You are solely responsible for the accuracy of your Communications.

**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 include using Digital Banking to review your Eligible Accounts on a daily basis. We may deem your failure to frequently review and immediately notify as a proximate cause of an experienced loss. You also agree to frequently check Digital Banking's messaging center for notices from Bank. (For Customers using Business Online Banking or Business Mobile Banking: see additional responsibilities in the Subsection below entitled "Monitoring Your Digital Banking Accounts.")

## **7. ACCESSING YOUR ELIGIBLE ACCOUNTS**

**7.1 Functions.** When you access Digital Banking, you will see a menu of currently available functions (e.g., view balances; view or search for transactions; locate branches; execute specific types of internal or external funds transfers; mobile remote deposit capture; 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. Not all Digital Banking functions are available in every Channel.

We reserve the right to refuse to make any transaction that you may request through Digital Banking.

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

**7.2 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 for unavailability of Digital Banking, or your inability to access the service or to execute its functions.

**7.3 Electronic Mail.** Sending email is one way to communicate with us. You may use email to ask general questions and to provide feedback to us. However, you cannot use email to initiate transactions on your Eligible Account(s). For your security, please do not include any sensitive information (e.g. account numbers) in emails to us. In Online Banking, you may include sensitive information using the Message feature.

**7.4 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.

### **7.5 Fees.**

**Consumer Channels.** Currently, we charge no fees for accessing your Eligible Account(s) through the consumer Channels of Digital Banking. Please note, however, that fees may apply to certain transactions performed while using Digital Banking. Those fees are either (a) stated in your separate fee schedule disclosures for the affected

Eligible Account (e.g., the fee to stop payment on a check, or the cash advance fee to transfer funds from a credit card account to a deposit account); or (b) displayed within the Digital Banking service itself when you request the transaction but before the fee is actually incurred (e.g., the fee for expedited delivery of a Bill Pay, Popmoney or Zelle transfer, or the fee for a mobile remote deposit capture). Note, if we consent to enrolling or linking your consumer Eligible Account in a business Channel, it may incur the fees applicable to the business Channels of Digital Banking.

**Consumer and Business Channels.** 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. We reserve the right to add or change fees for Digital Banking after sending prior notice. See the Subsection below entitled “Changes to Fees or Other Terms.”

**Business Channels.** You agree to pay the fees separately disclosed for enrollment in, or transactions in, the business Channels of 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.

**7.6 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 other any 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 choice, downloading, installation and use 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.

We do not currently require, but do recommend, that you use IBM® Trusteer Rapport® on your computer. (Check your Division’s website which may provide a link to IBM for a free download of Trusteer Rapport. That link is subject to cancelation without notice.) 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.

**7.7 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.

**7.8 Mobile Banking License Rights Generally.** For your use of Mobile Banking Software, we and our licensors (or other third-parties who have directly or indirectly granted rights in those software systems and programs) require your agreement to certain license rights arrangements and/or end-user agreements (“Licenses”). By enrolling in portions of Mobile Banking relating to those software systems and programs, and by downloading and installing Mobile Banking Software, you accept the terms and conditions of those Licenses. You agree that we are intended to be a third-party beneficiary, but not an obligor, of your rights and duties with those licensors and third-parties. A License with our primary licensor appears in the “Appendix: End User Agreement” at the end of this Agreement. We, our licensors and above third-parties reserve all rights not granted to you in this Agreement and under the terms of such Licenses.

You agree to delete all such software from your Mobile Device(s) promptly if the Licenses or this Agreement terminate for any reason. We reserve the right to change, add to, or terminate services with our third-party Mobile Banking Software providers, to substitute different Mobile Banking Software providers, and to enter into or arrange for the provision of Mobile Banking Software by other licensors and third-parties.

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.

## **8. TRANSFERS**

**8.1 Types of Transfers Allowed.** You can transfer funds from your Eligible Accounts (a) to your other Eligible Accounts or to another person’s eligible account with us (“**Transfers to a Friend**”) (collectively “**Internal Transfers**”), or (b) to your Loan Accounts (“**Internal Payments**”). You may also be able to transfer funds from eligible loans or credit cards to your deposit accounts (“**Internal Advances**”). Not all types of transfers may be available in all Channels of Digital Banking. Details of your transfers will be available through Digital Banking and listed on your regular account statements.

We have the right to establish, without prior notice, limitations on the amount or number of Internal Transfers. We may also without prior notice increase, decrease or remove such limitations at any time, and we are not obligated to enforce our limitations for any particular Internal Transfer. You may make Transfers to a Friend (consumers only) if you know the other person’s account number. Without our express consent, Transfers to a Friend may not exceed \$1,000 in the aggregate on any single day (or \$2,500 for customers of the California Bank & Trust Division). Be certain that you enter in the correct destination account information as Transfers to a Friend will not be recoverable after processing if you make any input errors.

You may also make Internal Payments to Loan Accounts. These 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 Internal 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 Division’s Customer Service to obtain the payoff amount. We cannot guarantee that estimated payoffs will satisfy the loan terms of the Loan Account.

Note: transfers from your Eligible Accounts to another person's account at a different bank is called an "external transfer to a friend" which is an ancillary service that requires enrollment and acceptance of additional terms and conditions. External transfers to a friend are not available in all Channels of Digital Banking.

**8.2 Availability of Funds and CutOff Times.** Internal Transfers and Internal Payments ordered before the daily cutoff time will be processed on that day, and available balances in your Deposit Account(s) will be adjusted immediately and available for subsequent (a) ATM transactions, (b) PIN-based Debit Card transactions, (c) withdrawals at the branch teller, and (d) payment of checks or other debits as applicable to your Deposit Account(s). Please refer to your Account Agreement(s) for information on how regular payments will be credited to a designated Loan Account. The cutoff time is 9:00 p.m. Pacific Time, 10:00 p.m. Mountain Time and 11:00 p.m. Central Time on any Business Day. For Amegy Bank customers only, the cutoff time is 10:00 p.m. Central Time. (Note: during national daylight savings time (typically the second Sunday in March to the first Sunday in November) the Internal Transfer and Internal Payments cutoff time is 9:00 p.m. Arizona local time).

Internal Transfers, Internal Payments and Internal Advances ordered after the daily cutoff time, or not on a Business Day, are ordinarily posted to your Eligible Accounts on the next Business Day. However, available balances in your Deposit Account(s) are adjusted immediately and available for subsequent (a) ATM transactions and (b) PIN-based Debit Card transactions.

Any Internal Transfer to a Deposit Account may require up to one full Business Day before the funds are available for subsequent non-PIN based Debit Card transactions. Internal Payments made to an enrolled credit card may take up to two Business Days to post, but the credit will be effective as of the date the transfer was initiated. If the available balance in a transferring account is insufficient at the time of a scheduled transfer, these transactions may overdraw your account and result in fee (as disclosed for your Eligible Account).

**8.3 Canceling an Internal Transfer, Internal Payment or Internal Advance.** You may schedule one-time and recurring Internal Transfers, Internal Payments, or Internal Advances. You may cancel any one-time or recurring Internal Transfer, Internal Payment or Internal Advance if you do so at least one day prior to the scheduled transaction processing date. Scheduled one-time and recurring Internal Transfers, Internal Payments or Internal Advances can only be canceled by placing a request through your Digital Banking, or by calling your Division's Customer Service. You may NOT cancel any immediate Internal Transfer, immediate Internal Payment, or Internal Advance. (An "immediate" transaction is one that you schedule to begin processing immediately at the time of your instruction, rather than on a future date.)

**8.4 Insufficient Funds.** If your Eligible Account has insufficient funds to complete all of the day's transactions (including ATM withdrawals, preauthorized transactions, Internal Transfers, Internal Payments, and Bill Pay payments, etc.) that will process for a given Business Day, then certain electronic funds transfers involving currency disbursement, like ATM withdrawals, will have priority. If an Internal Transfer or Internal Payment 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 will be charged any applicable overdraft fees (as disclosed for your Eligible Account).

## 9. MYALERTS

The MyAlerts function allows you to request select email messages notifying you of certain events and information of interest to you (e.g., balance information, failed transfers and reminders). We will deliver the MyAlerts messages that you have requested to your secured mailbox within the Digital Banking service (and, if you have requested it, to an external email address you designate). The MyAlerts messages are not delivered in real-time but may be delayed until all transactions for the day have been posted to your account. We make no promise that any MyAlerts messages will be delivered at the times requested. We obtain the information contained in the MyAlerts service from sources we consider reliable but we do not warrant its accuracy.

MyAlerts messages should not be used to monitor account balances as a method of avoiding overdrafts or non-sufficient funds fees. We may from time to time include in MyAlerts messages information about new products

and services, even if you do not qualify for them. You may elect to have MyAlerts delivered via email, but that email is not encrypted and you agree to hold us harmless against unauthorized access. You should not use your account numbers as account nicknames. If you choose to receive account-specific messages, your actual balance and transaction information may appear in your MyAlerts email messages.

## **10. WEBCONNECT**

Using the Web Connect feature, you may download account information from your Eligible Accounts using personal banking software that we from time to time elect to support (e.g., Quicken® and QuickBooks®). You are responsible for obtaining and maintaining that personal banking software. You must use the versions that are currently supported by us and the personal banking software vendor (e.g., which shall include the most recent version and may but it not required to include one or more prior versions). We are not required to notify you when the provider(s) of supported personal banking software release updates. We shall not be liable for incorrect information or misapplication of information resulting from the downloading process or the use of such personal banking software. We may charge fees as described in the fee schedule governing your affected Eligible Accounts. Please note that other fees may be assessed by your internet service provider or personal banking software provider.

## **11. STOP PAYMENT OF CHECKS (ONLINE BANKING ONLY)**

You may stop payment on a single check through Digital Banking. If you would like to stop payment on a series of checks, you may do so by contacting your Division's Customer Service or a branch. You must make any stop-payment order in the manner required by law and we must receive it in time to give us a reasonable opportunity to act on it before our stop-payment cutoff time. To be effective, your stop-payment order must precisely identify the number, date and amount of the item, and the payee (or such lesser combination as we may specify at the time). You may stop payment on any item drawn on your account whether you signed the item or not, if you have an equal or greater right to withdraw from this account than the person who signed the item. Our stop-payment cutoff time is one hour after the opening of the next Business Day after the Business Day on which we receive the item. Additional limitations on our obligation to stop payment are provided by law (e.g., we paid the item in cash or we certified the item). Stop payment fees for your applicable account will apply.

## **12. MOBILE REMOTE DEPOSIT CAPTURE**

**12.1 The Deposit Service.** The mobile remote deposit capture feature of Mobile Banking (the "Deposit Service") allows you to make deposits to your eligible checking, savings or money market accounts 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.

**12.2 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:**

- a. Checks payable to anyone other than the owner of the account into which it is being deposited;
- b. Checks drawn or issued by you; or drawn by others against an account on which you are a joint owner or authorized signer;
- c. Checks containing any unauthorized alteration;
- d. Checks payable jointly, unless deposited into an account with the names of all payees;

- e. Checks previously converted to a substitute check, as defined in Reg. CC;
- f. Checks drawn on a foreign bank and/or that are not payable in United States currency;
- g. 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;
- h. Checks that are undated, post-dated, or are dated more than 6 months prior to the date of deposit;
- i. Checks with any endorsement on the back other than that specified in this Agreement;
- j. Checks that have previously been deposited by any remote capture or physical delivery;
- k. Checks or items that are drawn or otherwise issued by the U.S. Treasury Department;
- l. Checks that have previously been returned unpaid for any reason;
- m. Travelers Checks;
- n. Checks payable to "Cash";
- o. Checks transmitted from outside the United States;
- p. Registered government warrants;
- q. Money Orders; or
- r. Checks that are prohibited by our current procedures relating to the mobile remote deposit capture feature, or which are otherwise not acceptable under your Deposit Account Agreement, or as we may otherwise determine in our sole discretion;
- s. Government checks of any type, state or federal.

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

**12.3 Endorsements and Procedures.** You agree to restrictively endorse any item transmitted through the Deposit Service as follows: sign the back of your check with your name and the words "**FOR MOBILE DEPOSIT TO [NAME OF YOUR BANK DIVISION]**" or as otherwise instructed by us. (See p.1 for a list of "Division" names). You agree to follow all other procedures and instructions for use of the Deposit Service as we may establish from time to time.

**12.4 Image Quality.** The image of a check or item transmitted to us using the Deposit 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.

**12.5 Receipt, Security and Errors in Transmission.** Use of the Deposit 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.

**12.6 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.

**12.7 Availability of Funds.** In general, if an image of an item you transmit through the Deposit Service is received and accepted before 7:00 p.m. Mountain Time (8:00 p.m. Central Time, 6:00 p.m. Pacific 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. (Note: during national daylight savings time (typically the second Sunday in March to the first Sunday in November) the Deposit Service ends at 6:00 p.m. Arizona local time). Otherwise, we ordinarily consider that the deposit was made on the next Business Day we are open. Funds deposited using the Deposit Service will generally be made available the next Business Day after the day of deposit. We may delay the availability of your funds at our discretion if we deem it appropriate in accordance with our policies and procedures.

**12.8 Deposit Limits.** We may establish limits on the dollar amount and/or number of items or deposits from time to time. If you attempt to initiate a deposit in excess of these limits, we can reject your deposit. If we permit you to make a deposit in excess of these limits, such deposit will still be subject to this Agreement, and we will not be obligated to allow such a deposit at other times. We will inform you of our current generally applicable standard deposit limits in a notice appearing within your Mobile Software at the beginning of each deposit session. Higher limits may be made available in our sole discretion for certain qualified accounts, but those higher limits (a) will 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 in the Mobile Software shall apply).

**12.9 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.

**12.10 Termination.** We may suspend or terminate your use of the Deposit 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 Deposit Service may be terminated if you breach any term of this Agreement, if you use the Deposit Service for any unauthorized or illegal purposes, or you use the Deposit Service in a manner inconsistent with the terms of any other agreement you may have with us.

**12.11 Fees for Remote Deposit Capture.** A fee may be charged for using the Deposit Service. We may change that fee amount from time to time, but the current amount will be disclosed before you choose to submit your deposit transaction. You authorize us to deduct any such fees from any account in your name with us.

**12.12 User Warranties and Indemnification.** You warrant to us that:

- a. You will only transmit eligible items;
- b. Images will meet our image quality standards;
- c. You will not transmit duplicate items;
- d. You will destroy remotely deposited items, and not re-deposit or re-present any original item;
- e. All information you provide to us is accurate, true and correct;
- f. You will comply with this Agreement and all applicable rules, laws and regulations;
- g. With respect to each check image that you transmit, you are deemed to have made any representation or warranty that would have applied had you deposited a paper check by other means;

You must indemnify and hold us harmless from any loss or damage arising from or in connection with breach of these warranties.

## 13. GENERAL

**13.1 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 HERELY 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.**

**For Consumer Customers:** If we do not complete an electronic fund transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages as prescribed by the federal Electronic Fund Transfer Act and its implementing Regulation E. However, there are some exceptions to our liability. We will not be liable, for instance: (1) if, through no fault of ours, you do not have enough money in your account to make the transfer, or if the transfer would create an overdraft which would not be covered by or would exceed the credit limit on any overdraft protection account you have with us (or would exceed funds available in any deposit account that has been linked for overdraft protection); (2) if the funds you are attempting to transfer are subject to legal process or other encumbrance restricting such transfer; (3) if the electronic funds transfer system was not working properly, and you knew about the breakdown when you started the transfer; (4) if circumstances beyond our control prevent the transfer despite reasonable precautions that we have taken; or (5) if any other exception stated in this Agreement or other governing Related Documents or by law applies.

**13.2 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 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 at least twenty-one (21) days in advance of the change's effective date, 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 twenty-one (21) thereafter. By continuing to use the service after a change (or after the effective date of any prior notice), you are accepting the changes. 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.

**13.3 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. In any event, sending twenty-one (21) days' prior notice shall be reasonable prior notice.

**If all of your enrolled Eligible Accounts become closed, or if you do not access any of your Eligible Accounts via Digital Banking for any consecutive one hundred twenty-day (120) period, your access to Digital Banking (including related services that you access through Digital Banking such as Bill Pay or eDocuments) may be terminated or suspended without prior notice.**

You may terminate your Online Banking or Mobile Banking services at any time by calling or writing your Division's Customer Service. 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.



**13.4 Payment Account.** You may be asked to designate a payment account for selected related services (such as Bill Pay, Popmoney, Zelle or Online Wires) that you access through Digital Banking. 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 Eligible Account.

**13.5 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, affiliates, 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, affiliates, and subsidiaries, 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 (except as may be otherwise provided by applicable consumer protection laws, including Regulation E); (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 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 Subsection shall survive the termination of this Agreement.

**13.6 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")).

**13.7 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., Online Wires) for the benefit of anyone other than yourself. We may assign this Agreement without notice to you.

**13.8 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 your Consent to Electronic Disclosures, Communications and Records; (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 you 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.** For customers using Business Online Banking or Business Mobile

Banking: notice to a CSA (e.g., your CSA's email address or by electronic message accessible via your CSA's Access Credentials) shall be effective notice to you; **your duty to update your contact information includes changes to any CSA's email address or phone number**).

**13.9 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 to Digital Banking's electronic messaging center; (2) telephoned to Customer Service; or (3) delivered by commercial service or U.S. Mail delivered to Customer Service. You authorize us to act on your oral notices, but we may require you to promptly confirm any oral notice via Digital Banking's messaging center or delivery to the Customer Service 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 Customer Service.**

**13.10 Governing Law.** This Agreement will be governed by and interpreted in accordance with Federal law and regulations, and by the laws of the state specified in your Deposit Account Agreement as governing your Eligible Accounts (which is determined by which Division of Zions Bancorporation, N.A. holds your deposit accounts).

**13.11 Entire Agreement.** This Agreement includes an end user agreement between you and our primary software licensor. See "Appendix: End User Agreement" below. This Agreement, as supplemented by your Account Agreements and your Related Documents, constitute 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 during enrollment for Consumer Online Banking, Business Online Banking or Mobile Banking services. When you enroll in a new Channel, 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 (e.g., Bill Pay, Popmoney, Zelle, External Transfers and Online Wires).

#### **14. BUSINESS ONLINE BANKING AND BUSINESS MOBILE BANKING ADDITIONAL TERMS**

This Section and its Subsections pertain only to customers (whether businesses or consumers) who use our Business Online Banking Channel or the Business Mobile Banking Channel.

**14.1 Your Customer System Administrator (CSA).** You hereby fully authorize your Customer System Administrator (CSA) to act as your designated agent in all matters regarding the Digital Banking itself and transactions using Digital Banking. You may designate more than one CSA. 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 any CSA.

Each of your CSA's authority includes, without limitation, the power to:

- (A) amend the terms of your Digital Banking service application, or any instructions or specifications therein or pursuant thereto;
- (B) **accept, enter into or amend the terms of any Related Documents in connection with Digital Banking, including Addenda for additional functionality such as alternate method of accessing Digital Banking, specialized funds transfer services (e.g., Online Wires, Bill Pay, Popmoney, Zelle, External Transfers, etc.), or linking your Digital Banking service with other customers' digital banking services;**
- (C) enter into or issue and deliver Related Documents and other instructions that, without limitation:
  - (i) designate optional service functions you wish activated;
  - (ii) set limits Digital Banking may allow you to impose (e.g., dollar limits) for certain functions;

- (iii) designate Eligible Accounts accessible via your Digital Banking; and
  - (iv) designate one or more Authorized Users, and issue them Access Credentials for using Digital Banking, subject to limits configurable by the CSA;
- (D) 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 CSA's authority also includes the power to designate, on your behalf, one or more additional CSAs for your Digital Banking service, and issue additional Access Credentials for performing CSA 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 be CSA.

Your CSA's authority and Access Credentials shall remain in place until (a) you deliver formal written notice of revocation to us, (b) you notify us by calling the Customer Service phone number for your Division, or (c) that CSA's Access Credentials are revoked online by another CSA using Digital Banking service's self-administration functionality; but in each case we shall have a commercially reasonable time and opportunity to act upon that written notice or online revocation. In addition, we may revoke or refuse to accept your CSA's authority and Access Credentials in connection with Digital Banking at any time without prior notice.

**14.2 Your Authorized Users.** Through his or her Access Credentials, an Authorized User can access Digital Banking's functions, subject however to restrictions imposed by Digital Banking itself or by your CSA (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 (in paper or electronic delivery) any disclosures that we may be required by law to provide to you (including consumers) in writing.

You represent that each individual who is issued Access Credentials by your CSA, or by us at the request of you or your CSA, 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 (A) you deliver formal written notice of revocation to us, (B) you notify us by calling the Customer Service phone number stated in this Agreement, or (C) those Access Credentials are revoked online by a CSA using Digital Banking's self-administration functionality; but in each case we shall have a commercially reasonable time and opportunity to act upon that written notice or online revocation. In addition, we may revoke or refuse to accept any User's Access Credentials at any time without prior notice. Authorized Users may be allowed to change their Access Credentials.

**14.3 Additional Function -- 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 ACH transfers ("**Entries**"):

1. Employee Direct Deposit transactions for payroll purposes;
2. Electronic Tax Payments. *[Tax Payments Service terminated, effective August 1, 2019.]*

**NACHA Rules.** You agree 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**") and applicable law. 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 consumer credit Entries to us two business days before the payment date and all other ACH Entries one business day prior to the payment date.

**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 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 days prior to the transaction effective date). Each ACH file you send to us will consist of one or more batches of ACH Entries. Sufficient funds must be available in your offset Eligible Account at the time the batches are processed. If sufficient funds are not then available, we will process only those batches for which sufficient funds are available, in the order those batches appear within your file. Batches for which sufficient funds are not available will suspend, and will be attempted again in the next available settlement window. If a batch cannot be processed the night before the effective date of that batch, that batch will not be processed.

If we do not require your file to be prefunded, we may still refuse your ACH credit file if you have insufficient funds in your Eligible Account on the date we initiate the transaction (e.g., two business days prior to the settlement date for an ACH credit entry) or on the payment/settlement date. We may also require you to maintain sufficient available funds in your Eligible 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 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 funds in your Eligible 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 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.

**Prenotifications.** You agree to send pre-notification Entries as defined in the Rules, and you agree not to send any Entry when a prior pre-notification for that Entry has been rejected or returned, unless you have first corrected the reason for the rejection or return.

**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 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 settlement 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 the 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 Customer Service. 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 effect 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 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 effected. 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 regarding any Entry or file that is rejected or returned for any reason. We are not obligated to credit your Eligible 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 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.

**14.4 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.** If you do not notify us prior to close of the Business Day after the first Business Day in which the questioned transaction first appeared in Digital Banking, the transaction is not eligible for automated returns. In that event, 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. (**For Consumer Customers:** this paragraph is limited by (i) applicable consumer protection laws (including Regulation E), and (ii) the consumer protection terms and disclosures set forth in this Agreement, your Account Agreements, and your Related Documents.)

**14.5 Your Internal Security (non-consumer customers only).** 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:

- Verifying all instructions from your payees (e.g., ensure new or changed payment addresses were not communicated by an imposter);
- Limiting and controlling who has access to your computer systems and Mobile Devices;
- Protecting and frequently changing your Access Credentials;
- Adopting dual authorization and/or transaction-based authentication procedures for financial transfers;
- 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, e-mail programs, and the like (such as IBM® Trusteer Rapport™ software);
- Prohibiting the disabling or modification the security features of any software or hardware (e.g., "jailbreaking" of mobile devices); and prohibiting the use of "burner" mobile devices.
- Using effective, up-to-date firewalls;
- 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, e-mail 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;
- Reconciling all accounts on a daily basis, and immediately reporting any discrepancies;

- 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);
- Allowing Digital Banking to be accessed only from secure locations; and
- 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 listing 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.

#### **APPENDIX: END USER AGREEMENT FOR MOBILE BANKING SOFTWARE**

Zions Bancorporation, N.A.'s primary licensor for the Mobile Banking Software is mFoundry, Inc. (and/or one or more affiliates thereof, hereafter collectively "**mFoundry**"). mFoundry authorizes and requires Zions Bancorporation, N.A. to enter into the following end user agreement (the "**End User Agreement**") with you for the use of mFoundry's "Software" (defined below). By enrolling in Zions Bancorporation, N.A.'s Mobile Banking service, and during such time as Zions Bancorporation, N.A. maintains its rights to license the mFoundry Software, you hereby agree as follows:

A.1. Ownership. You acknowledge and agree that a third party provider or licensor to your financial services provider ("**Licensor**") is the owner of all right, title and interest in and to the downloaded software to be used for access to mobile banking services from Zions Bancorporation, N.A. as your financial services provider and the computer programs contained therein in machine readable object code form as well as any accompanying user documentation along with all subsequent copies, updates or versions thereof which are made available to you (if any), regardless of the media or form in which they may exist (collectively the "**Software**").

A.2. License. Subject to the terms and conditions of this End User Agreement, you are hereby granted a limited, nonexclusive License to use the Software. All rights not expressly granted to you by this End User Agreement are hereby reserved by the owner of the Software. Nothing in this License will entitle you to receive hard-copy documentation, technical support, telephone assistance, or updates to the Software. This End User Agreement may be terminated at any time, for any reason or no reason. Upon termination, you agree to immediately destroy all copies of the Software in your possession or control.

A.3. Restrictions. You shall not: (i) modify, revise or create any derivative works of the Software; (ii) decompile, reverse engineer or otherwise attempt to derive the source code for the Software; (iii) redistribute, sell, rent, lease, sublicense, or otherwise transfer rights to the Software; or (iv) remove or alter any proprietary notices, legends, symbols or labels in the Software, including, but not limited to, any trademark, logo or copyright.

A.4. Disclaimer of Warranty. THE SOFTWARE IS PROVIDED ON AN 'AS IS' AND 'AS AVAILABLE' BASIS WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED BY ANY PERSON (INCLUDING LICENSOR, Zions Bancorporation, N.A., OTHER PROVIDERS OF FINANCIAL SERVICES, ANY OF THEIR CONTRACTORS OR PROVIDERS, AND THEIR RESPECTIVE AFFILIATES), INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. NO WARRANTY IS PROVIDED THAT THE SOFTWARE WILL BE FREE FROM DEFECTS OR VIRUSES OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED. YOUR USE OF THE SOFTWARE AND ANY OTHER MATERIAL OR SERVICES DOWNLOADED OR MADE AVAILABLE TO YOU THROUGH THE SOFTWARE IS AT YOUR OWN DISCRETION AND RISK, AND YOU ARE SOLELY RESPONSIBLE FOR ANY DAMAGE RESULTING FROM THEIR USE.

A.5. Limitation of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR, Zions Bancorporation, N.A., OTHER PROVIDERS OF ANY FINANCIAL SERVICES AVAILABLE THROUGH OR RELATED TO THE SOFTWARE, ANY OF THEIR CONTRACTORS OR PROVIDERS OR ANY OF EACH OF THEIR AFFILIATES BE LIABLE FOR ANY DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY THEREOF, AND REGARDLESS OF THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT OR OTHERWISE) UPON WHICH ANY CLAIM IS BASED. IN ANY CASE, LIABILITY OF LICENSOR OR ANY OF THE OTHER PERSONS OR ENTITIES DESCRIBED IN THE PRECEDING SENTENCE ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE SHALL NOT EXCEED IN THE AGGREGATE THE LESSER OF \$10.00 OR THE SUM OF THE FEES PAID BY YOU FOR THIS LICENSE.

A.6. U.S. Government Restricted Rights. The Software is commercial computer software subject to RESTRICTED RIGHTS. In accordance with 48 CFR 12.212 (Computer software) or DFARS 227.7202 (Commercial computer software and commercial computer software documentation), as applicable, the use, duplication, and disclosure of the Software by the United States of America, its agencies or instrumentalities is subject to the restrictions set forth in this End User Agreement.

A.7. Miscellaneous. This End User Agreement constitutes the entire agreement between the parties concerning the subject matter hereof. This End User Agreement will be governed by and construed in accordance with the laws of the state of Florida, excluding that body of laws pertaining to conflict of laws. If any provision of this End User Agreement is determined by a court of law to be illegal or unenforceable, such provision will be enforced to the maximum extent possible and the other provisions will remain effective and enforceable. All disputes to which Licensor is a party relating to this End User Agreement are subject to the exclusive jurisdiction of the courts of Florida and the parties expressly consent to jurisdiction and venue thereof and therein. The parties confirm that this End User Agreement and all related documentation is and will be in the English language. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly waived and excluded.

A.8. Content and Services. Neither Licensor nor the provider of the wireless network is the provider of any financial services available through or related to the Software, and neither Licensor nor the provider of the wireless network or any contractor of the provider of the financial services available through or related to the Software, is responsible for any of the materials, information, products or services made available to you via the Software.