Mobile Agreement

Welcome to Mobile Banking with Points West Community Bank

Thank you for using the Mobile Money Services ("Services") and any related Software ("Software") provided by Points West Community Bank ("Financial Institution") combined with your handheld's text messaging capabilities. By participating in the Services or using the Software, you are agreeing to the following terms and conditions, in addition to any terms and conditions to which you have previously agreed with respect to the underlying electronic banking and bill pay services of which the Service is a part. Financial Institution in its discretion may modify these Terms and Conditions at any time. Standard messaging charges apply.

Terms and Conditions:

a. **Program:** Financial Institution offers their customers mobile access to their account information (e.g., for checking balances and last transactions) over the Short Message Service (SMS), as well as the option to set up alerts for their accounts (e.g., low balance alerts). Enrollment requires identification of the user's banking relationship with Financial Institution as well as providing a mobile phone number. The mobile phone number's verification is done by the user receiving an SMS message with a verification code which they will have to enter on the website. Additionally, customers may select the type of alerts and other preferences which will determine, together with their account data, the frequency of alerts delivered to the customer. This program will be ongoing. Standard messaging charges apply. Customers will be allowed to opt out of this program at any time.

b. **Questions:** You can contact us at *www.pwcbank.com* or (833)226-7474, or send a text message with the word "HELP" to this number: 96924. We can answer any questions you have about the program.

c. **To Stop the program:** To stop the messages from coming to your phone, you can opt out of the program via SMS. Just send a text that says "STOP" to this number:(256)907-8669. You'll receive a one-time opt-out confirmation text message. After that, you will not receive any future messages.

d. The Services and/or Software may not be available at any time for any reason outside of the reasonable control of Financial Institution or any service provider Privacy and User Information.

You acknowledge that in connection with your use of the Services, Financial Institution and its affiliates and service providers, including Fiserv, Inc. and its affiliates, may receive and may share with one another names, domain names, addresses, passwords, telephone and device numbers, the content of messages, data files and other data and information provided by you or from other sources in connection with the Services or Software (collectively "User Information"). The Financial Institution and its affiliates and service providers will maintain reasonable safeguards to protect the information from unauthorized disclosure or use, but reserve the right to use and disclose this information as reasonably necessary to deliver the Services and as otherwise permitted by law, including compliance with court orders or lawful instructions from a government agency, to protect the personal safety of subscribers or the public, to defend claims, and as otherwise authorized by you. The Financial Institution and its affiliates and service providers also reserve the right to monitor use of the Services and Software for purposes of verifying compliance with the law, these terms and conditions and any applicable license, but disclaim any obligation to monitor, filter, or edit any content.

Restrictions on Use. You agree not to use the Services and Software in or for any illegal, fraudulent, unauthorized or improper manner or purpose and will only be used in compliance with all applicable laws, rules and regulations, including all applicable state, federal, and international Internet, data, telecommunications, telemarketing, "spam," and import/export laws and regulations, including the U.S. Export Administration Regulations. Without limiting the foregoing, you agree that you will not use the Services and Software to transmit or disseminate:

(i) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom you do not otherwise have a legal right to send such material;

(ii) material that infringes or violates any third party's intellectual property rights, rights of publicity, privacy, or confidentiality, or the rights or legal obligations of any wireless service provider or any of its clients or subscribers;

(iii) material or data, that is illegal, or material or data, as determined by Financial Institution (in its sole discretion), that is harassing, coercive, defamatory, libelous, abusive, threatening, obscene, or otherwise objectionable, materials that are harmful to minors or excessive in quantity, or materials the transmission of which could diminish or harm the reputation of Financial Institution or any third-party service provider involved in the provision of the Services; or

(iv) material or data that is alcoholic beverage-related (e.g., beer, wine, or liquor), tobacco-related (e.g., cigarettes, cigars, pipes, chewing tobacco), guns or weapons-related (e.g., firearms, bullets), illegal drugs-

related (e.g., marijuana, cocaine), pornographic-related (e.g., adult themes, sexual content), crime-related (e.g., organized crime, notorious characters), violence-related (e.g., violent games), death-related (e.g., funeral homes, mortuaries), hate-related (e.g. racist organizations), gambling-related (e.g., casinos, lotteries), specifically mentions any wireless carrier or copies or parodies the products or Services of any wireless carrier;

(v) viruses, Trojan horses, worms, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or personal information;

(vi) any material or information that is false, misleading, or inaccurate;

(vii) any material that would expose Financial Institution, any third-party service provider involved in providing the Services, or any other third party to liability; or

(viii) any signal or impulse that could cause electrical, magnetic, optical, or other technical harm to the equipment or facilities of Fiserv or any third party.

You agree that you will not attempt to:

(i) access any Software or Services for which your use has not been authorized; or

(ii) use or attempt to use a third party's account; or

(iii) interfere in any manner the provision of the Services or Software, the security of the Services or Software, or other customers of the Services or Software, or otherwise abuse the Services or Software.

Fingerprint Login for Mobile Banking: Fingerprint Login is an optional fingerprint sign-in method that may be available for certain Android® mobile devices that have a built-in fingerprint scanner. To use Fingerprint Login, you will need to first save your fingerprint on your mobile device (for more help with fingerprint scanning, contact the manufacturer that supports your mobile device). Fingerprints are stored on your device only and Points West Community Bank never sees or stores your fingerprint information. You acknowledge that by enabling Fingerprint Login, you will allow anyone who has a fingerprint stored on your device access to your personal and payment account information within the app. Points West Community Bank reserves the right to suspend or disable this feature at any time. Fingerprint Login can only be associated with one Mobile Banking username at a time on a device. If your device does not recognize your fingerprint, you can sign in using your standard login credentials (e.g. password). To use Fingerprint Login for Mobile Banking on multiple devices, you will need to set it up for each device. You can enable or disable Fingerprint Login anytime within the app. Android is a trademark of Google Inc.

Mobile Deposit Agreement

This Agreement contains the terms and conditions for using Points West Mobile Deposit that Points West Bank ("we" or "us") may provide to you ("you" or "your"). The Internet Banking and Bill Payment Access User Agreement and the Rules & Regulations Applicable to all Points West Accounts and Cards ("Rules and Regulations"), also apply to transactions made using Mobile Deposit.

By using Mobile Deposit, you acknowledge and accept this Agreement.

Features and Services: Points West Mobile Deposit allows you to deposit money into certain accounts with your mobile device camera using the Points West Mobile Application or "Mobile App". To use Mobile Deposit, you must have agreed to the Internet Banking User Agreement.

Charge: There may be a charge to use this service. The Mobile App will inform you of the current charge to use the service prior to the completion of the transaction.

Types of Checks: You can only deposit checks using Mobile Deposit; however, there are some checks that you cannot deposit. These include:

a. Checks payable to any person or entity other than you.

b. Checks containing any alteration of which you know or believe to be fraudulent or not authorized by the owner of the account on which the check is drawn.

c. Any checks that are not in original form with a signature, such as substitute checks or remotely created checks.

d. Checks written off an account at a financial institution located outside the United States.

e. Checks not payable in United States currency.

f. Checks dated more than 6 months prior to the date of deposit.

g. Temporary checks or counter checks (any check without a check number).

Note that any check that you attempt to deposit using Mobile Deposit is subject to verification by Points West. We may reject an item for deposit for any reason and will not be liable to you. In such a case, you will need to deposit the item using other means, such as visiting a Points West branch. Endorsements: You must endorse the back of each check submitted through Mobile Deposit. You must endorse with 1) the words “For Deposit Only by Mobile Deposit” or “Mobile Deposit Only” or “For Remote Deposit Only” AND 2) the date of deposit. If the check being deposited has a box in the endorsement area that may be checked to indicate it is for mobile or remote deposit, you may check the box instead of writing in the endorsement area. In the case that you check the box indicating the item is for mobile deposit, the date of deposit is still required to be included. Please note that if a check is not properly endorsed Points West Community Bank reserves the right to reject the check for deposit.

Receipt: We are not responsible for items that we do not receive. Processing and/or transmission errors can occur after we acknowledge receipt that may impact transaction completion.

Cut off Times for Deposits: Deposits made via Mobile Deposit must be made before 2 PM Mountain Standard Time in order to be considered deposited same day. Deposits made after 2 PM Mountain Standard Time will be considered deposited the next business day. A business day is Monday through Friday, excluding Federal Holidays.

Availability of Funds Deposited: Checks are subject to verification by Points West and may be rejected for any reason without liability to you. If the check is verified by Points West, the balance of the check will be made available to you the first business day after the day of deposit in most cases. There are some reasons that you may have delayed availability such as a history of repeated overdrafts, or checks totaling more than $5,000 deposited on the same day (a complete list of these reasons is available in the Rules and Regulations). In such cases, you will receive full availability by the seventh business day after the day of deposit. If your account has been open 30 days or less, however, you may not receive full availability until the ninth business day after the day of deposit. If the check is not approved, the amount that was made available to you will be removed from your account and you will be notified that we could not accept your deposit. Notifications of delayed availability or disapproval of the deposit may not be available to you via the Mobile App and instead may come via the mail or other acceptable means. There is additional information relating to availability in the Rules and Regulations. You can get a copy on our website or by calling (833)226-7474.

Destruction of Original Check: Once you receive full credit for the check, you must destroy the check. Shredding it is one way to destroy it. Destroying the check prevents it from being presented for deposit another time. You will be liable for checks that are presented more than once.

Image Quality: The image of an item transmitted to Points West must be legible. You must capture the front and back of each check deposited.

Changes/Removal of Service: We may, in our sole discretion, modify, add or remove portions of the service or end the service at any time without notice. We may turn off the service to you if we suspect fraud, if you misuse Mobile Deposit, have excessive overdrafts or returned items or for other reasons in our sole discretion.

Limitations: When using Mobile Deposit, you may experience difficulties that are outside the control of Points West or there may be times when Mobile Deposit is not available. We are not responsible for any difficulties or any damages that you may incur as a result of these difficulties or unavailability.

Compatible Hardware and Software: In order to use Mobile Deposit, you must use, at your expense, compatible hardware and software. We are not responsible for any third-party software you may need to use Mobile Deposit. We may change requirements at any time without prior notice. You may need to upgrade the Mobile App to use Mobile Deposit. A software update is the best way to keep your phone secure. Software updates regularly provide security patches; for that reason, we highly recommend and may require you to keep your phone current. Updates are released at different times depending on your provider.

Deposit Limits: There is a $5,000 aggregate daily limit for items deposited via Mobile Deposit by individuals and a $15,000 aggregate daily limit for items deposited via Mobile Deposit by businesses. These limits may change from time to time without prior notice to you.

Errors: You must notify us of any errors (or suspected errors) related to the items deposited through the Services as soon as possible after they occur, and in no event later than 30 days after the related Points West account statement is sent. You can contact us by calling (833)226-7474 or by visiting a Points West branch. Unless you notify us within 30 days, the account statement containing the deposits made through the Services is deemed correct, and you cannot bring a claim against us for any alleged errors.

Alerts. Your enrollment in Points West Community Bank Online Banking and/or Mobile Banking (the "Service") includes enrollment to receive transaction alerts and notifications ("Alerts"). Alerts are electronic notices from us that contain transactional information about your Points West Community Bank account(s). Account Alerts and Additional Alerts must be managed and/or added online through the Service. We may add new alerts from time to time, or cancel old alerts. We usually notify you when we cancel alerts, but are not obligated to do so. Points West Community Bank reserves the right to terminate its alerts service at any time without prior notice to you.

Methods of Delivery. We may provide alerts through one or more channels ("endpoints"): (a) a mobile device, by text message, (b) a mobile device, by push notification; (c) an email account, by an e-mail message; or (d) your Points West Community Bank Online Banking message inbox. You agree to receive alerts through these endpoints, and it is your responsibility to determine that each of the service providers for the endpoints described in (a) through (c) above supports the email, push notification, and text message alerts provided through the alerts service. Please be advised that text or data charges or rates may be imposed by your endpoint service provider. Alert frequency varies by account and preferences. You agree to provide us a valid mobile phone number or email address so that we may send you alerts. If your email address or your mobile device's number changes, you are responsible for informing us of that change. Your alerts will be updated to reflect the changes that you communicate to us with regard to your primary and secondary email addresses or mobile device number.

Alerts via Text Message. To stop alerts via text message, text "STOP" to (256)907-8669 at any time. Alerts sent to your primary email address will be unaffected by this action. To restore alerts on your mobile phone, just visit the alerts tab in Points West Community Bank Online Banking. For help with SMS text alerts, text "HELP" to (256)907-8669. In case of questions please contact customer service at (833)226-7474. Our participating carriers include (but are not limited to) AT&T, SprintPCS, T-Mobile®, U.S. Cellular®, Verizon Wireless, MetroPCS.

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

Alert Information. As alerts delivered via SMS, email and push notifications are not encrypted, we will never include your passcode or full account number. You acknowledge and agree that alerts may not be encrypted and may include your name and some information about your accounts, and anyone with access to your alerts will be able to view the contents of these messages.