Security Statement

RiverWind Bank, ("Bank") strives to provide a safe environment for employees, customers, vendors and visitors. RiverWind Bank continues to maintain and update effective security programs to protect against a variety of operational and transactional risks, including crime, fraud and natural disaster. Many laws and regulations intensify regulatory attention on the Bank's risk management program and controls in place to guard against threats. As threats to security change and technology improves, it becomes necessary and essential for our systems to be upgraded to maintain a secure operating environment. Our physical facility, branches and office locations are an integral part of our security protocol to ensure maximum safety for employees and customers. Fraud issues occasionally contain a criminal component and it is our procedure to investigate and prepare documentation for potential prosecution and/or asset recovery. RiverWind Bank is strongly committed to protect customer assets and the assets of the Bank. We take pride in our security culture and management support to provide the utmost assistance to our customers and employees in this endeavor. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated consumer.

- ✓ Watch out for copycat websites that deliberately use a name or web address very similar to, but not the same as the real one. The intent is to lure you into clicking through to their website and giving out your personal information such as a bank account number, credit card number or Online Banking login information.

- ✓ Always use you pre-established links to access websites and avoid clicking on links in unsolicited emails. If you ever receive a suspicious email representing itself as RiverWind Bank, please forward the message in its entirety to support@riverwindbank.com

- ✓ Ensure that your own personal computer has updated anti-virus and firewall protections. Apply security patches for all your programs and operating systems regularly.

- ✓ Passwords should be unique to you and changed regularly. Do not use birthdays or other numbers or words that may be easy for others to guess. Never write down your password or give it to another person.

- ✓ Monitor your account activity frequently using our free Online and Mobile Banking Services.

- ✓ Sign up for free Online Banking eStatements to avoid having your paper statement sitting in an unsecure mailbox where it could be compromised.

- ✓ Set up free Security and Balance Alerts through Online Banking or Shazam Bolts mobile app to be notified via phone, email and/or SMS text message when there is login activity or changes in your expected balance.

Please keep in mind that we will never ask for or email you requesting your Online Banking password. We may on occasion call to verify other information regarding your online activity should we see something of concern in you login patterns. If you plan to travel and use your Online Banking or debit card, it is very helpful to call us in advance to avoid your account being temporarily disabled for security purposes. We encourage you to review our Privacy links and our Security Center tips link which can be found on our riverwindbank.com website. **If at any time you have questions regarding security or possible fraud, please contact your customer service representatives at 1-870-347-2511 or support@riverwindbank.com.**