Internet Banking Security Policy

At River Bank, we take safeguarding our customer's data seriously. We are proud of our history of offering the same commitment to each and every one of our customers. Our promise has given our customers the confidence and assurance to rely on, and our bank a firm foundation to build on. River Bank remains strong as one of Western Wisconsin's most respected and trusted banking institutions. Below is a list of tips and helpful advice to help protect yourself.

Identity theft and phishing are crimes. Fraud may be disguised in many forms and fraudsters are coming up with new ploys every day. This page lists some tips and recommendations to help you identify and in some cases deal with fraud.

- *Identity theft* occurs when your personal information is obtained without your knowledge or consent and is used to commit fraud or theft. It is not possible to completely eliminate the risk of fraud or theft but here are some ways to mitigate the risk.
    - Do not provide personal information to anyone over the phone, through the mail, or over the internet unless you have initiated the contact or are sure who you are talking to.
    - Do not carry your social security card with you.
    - Avoid using passwords that are easily identifiable (birth dates, phone numbers, Social Security Numbers etc.).
    - Shred any receipts or documents that contain personal information.
    - Do not print your Social Security Number or phone number on your checks.
    - Alert the U.S. Postal service if you will be away from home and promptly remove mail from your mailbox.
    - Do not distribute personal information on social networking sites.

- *Phishing* is defined as attempting to obtain financial or other confidential information from internet users, typically by sending an email that appears to be from a legitimate organization, usually a financial institution, or any other source, but contains a link to a fake web site that replicates the real one. Some alerts may be:
    - Emails that urge you to act quickly because your account may be suspended or closed, or update personal information.
    - Emails that don't address you by name but use a generic greeting.
    - Emails that ask for specific confidential information (account numbers, passwords, access IDs etc.).

If you receive an email from River Bank, or any other source, asking for personal information, treat it as suspicious. Never reply to an email with sensitive information. If you believe your personal financial information has been compromised, contact your local River Bank branch. The following are some additional computer tips:

- Do not write down PIN numbers. When you use your PIN, shield the entry from view by others.
- Treat your card, PIN Number, and passwords as though they are cash.

- If you travel outside of Minnesota, Wisconsin or Iowa, notify the bank and your credit card company.
- Protect your personal computers by having up-to-date Anti-Virus and Anti-Spyware installed.
- Use a personal Firewall. Firewalls serve as an additional protective barrier between your computer and the internet.
- Install security updates and patches regularly. Set your PC up to receive updates automatically whenever possible.
- Be proactive about protecting yourself. Check your credit report at least annually. You can order online at www.annualcreditreport.com or call 1-877-322-8228 for a free copy (One per year)
- Make your passwords long and strong. Combine capital and lower case letters with numbers and symbols to create a stronger password.
- Do not use the same password for all of your accounts.
- Do not agree to save passwords on your computer operating system.
- Do not click on pop-ups that advertise Anti-virus or Anti-spyware programs. Contact the retailer directly.
- Do not download software from unknown sources.
- Back up critical files.

Perhaps the fastest growing Information Technology area is Mobile Applications or "Apps". Make sure that you actually need an app before downloading. When you download you may be opening yourself to potential vulnerabilities. The following are additional tips:

- Research the app yourself before downloading.
- Research the app store you download from.
- Password-protect your mobile device with a strong password. Do not store passwords on the device, do not enable apps to remember your password, and set up your device to auto-lock after a few minutes.
- Learn to remotely wipe your device. If your device has a remote wipe option, you should enable it.
- Do not use Wi-Fi when performing financial transactions. Use only 3G or 4G networks for any secure transactions.
- Keep your apps updated as soon as updates are available.
- Disable Bluetooth settings when not in use. If left on, someone could potentially pair to your device and obtain information.

If you think your identity has been stolen, report it to your local River Bank branch. You may also want to report stolen finances, identities or other cyber-crime to the Internet Crime Complaint Center at www.ic3.gov, the FTC at http://www.ftc.gov/bcp/edu/microsites/idtheft/ and/or your local law enforcement or State Attorney General's office.

Thank You for choosing River Bank.