Safeguarding Your Information Best Practices

At **Range Bank** the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, dishonest 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 your pre-established links to access websites and avoid clicking on links in unsolicited e-mails. If you ever receive a suspicious e-mail representing itself as **Range Bank**, please forward the message in it's entirety to **operations@rangebank.com**.
- Ensure that your own personal computer has updated anti-virus and firewall protections. Apply security patches for all of your programs and operating systems regularly.
- Passwords should be unique to you. 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. Passwords for Range Bank's online banking must be alphanumeric, contain one special character and must be 8-25 characters long. Your last four passwords cannot be reused. While having to come up with a new password may cause some inconvenience, it is important to remember the monetary and information loss that may occur if login credentials are ever lost or stolen.
- Monitor your account activity frequently using our free online banking services.
- Sign up for free online banking eDocs to avoid having your paper statement and documents sitting in an unsecure mailbox where they could be compromised.
- Set up free security and balance alerts through online banking to be notified via email or at login.

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 your 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.

In case of errors or questions about your electronic transfers, call or write us at the telephone number or address listed, 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 the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared.

For personal accounts, limitations on your liability for unauthorized electronic funds transfers and other electronic errors that are covered by Regulation E are explained in the EFT Disclosure given to you at account opening. However, if you use online services for any business activity, you assume all risk of loss for unauthorized transfers and payments, and you must establish your own internal security procedures for employees you authorize to prevent all unauthorized use by other employees or persons.

If at any time you have questions regarding security or possible fraud, please contact our customer service representatives at **906-226-0587** or via e-mail at **operations@rangebank.com.**

Range Bank
100 N Front Street
Marquette, MI 49855

rangebank.com

Member FDIC