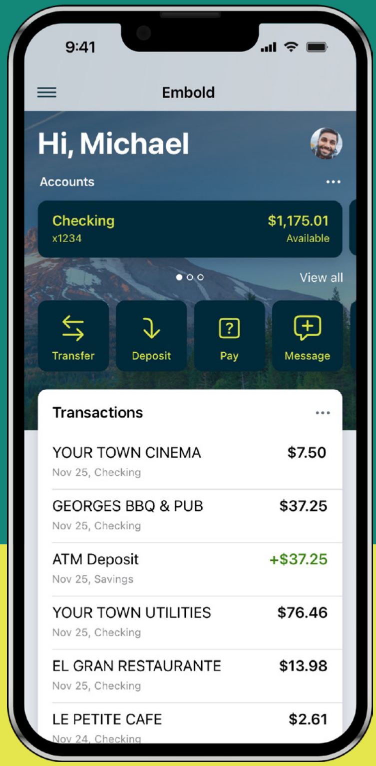
Federally Insured by NCUA

Protect Yourself During Our Digital Banking Conversion

As we transition to our new digital banking platform, we want to remind members to remain alert for fraud attempts. Unfortunately, fraudsters often take advantage of major events, such as system upgrades and digital banking conversions, to impersonate financial institutions and trick members into sharing sensitive information.



Common Red Flags to Watch For

Unexpected calls, texts, or emails claiming to be from the credit union

- Fraudsters may contact you claiming there is a problem with your account or that immediate action is required.
- Be cautious of messages that create a sense of urgency or fear.

Requests for your online banking credentials

- We will never contact you and ask for your password, one-time security codes, PIN, or multi-factor authentication (MFA) codes.
- Never share these credentials with anyone.

Requests for personal information

- Be suspicious of anyone asking for your Social Security number, debit card information, account numbers, or security question answers through email, text, or an unsolicited phone call.

Links directing you to “verify” or “reactivate” your account

- Fraudsters may send messages containing links to fake websites designed to steal your login information.
- Access online banking by typing our website address directly into your browser or using our official mobile app.

Requests to move money to a “safe” account

- The credit union will never ask you to transfer funds, send a wire, purchase gift cards, or move money to protect your account.

Unexpected requests for authentication codes

- If you receive a one-time passcode or authentication request that you did not initiate, do not provide the code to anyone.

Remember

- The credit union will **never** call, text, or email you asking for your password, PIN, security codes, or full online banking credentials.
- If you are unsure whether a communication is legitimate, **contact us directly** using the phone number listed on our website or your debit/credit card.
- Do not use phone numbers, links, or contact information provided in an unsolicited email, text, or message.

Your Best Defense

Stop. Think. Verify.

During the conversion, fraudsters may try to use the excitement and confusion surrounding the change to gain access to your accounts. When in doubt, contact the credit union directly before taking any action.

This simple step can help protect your account and personal information from fraud.

EMBOLD CREDIT UNION