MOBILITY
CREDIT UNION

Because of recent credit and debit card breaches at many retailers, MOBILITY Credit Union wants to inform you of our procedures when asking members for confidential information regarding their accounts.

MOBILITY CU will NEVER ask for your PIN number.

MOBILITY CU will NEVER ask for account information to be verified via email or text.

To verify member identity, you will be asked three security questions when calling MOBILITY CU Member Services. At least one of these questions will pertain to information that cannot be obtained from a member statement, such as:

- How did you join MOBILITY CU?
- What is your mother's maiden name?
- What is your date of birth?

Other questions asked by MOBILITY CU to verify your identity are:

- What is your zip code?
- What are the last four digits of your social security number?
- What type of loan do you have with MOBILITY CU?
- What branch do you usually visit?
- When was your last deposit?/What was the amount of your last deposit?

If preferred, MOBILITY CU is able to set up a member password for your account(s) that has to be answered correctly before MOBILITY CU can provide account information.

If your debit card or credit card account is suspected of fraud, you will be called by a MOBILITY CU representative. MOBILITY CU will NOT ask you for identifying account information. Instead, you will ONLY be asked to confirm or deny your most recent transactions.

***Phishing* is fraud that occurs via email where con artists pose as legitimate financial institutions or businesses. When con artists use either automated phone calls or a real person to call to ask for account information, it is known as *vishing*, short for voice phishing.**

To protect yourself from phishing and vishing schemes and account fraud, here are some easy tips you can follow:

- When contacted via phone, NEVER provide account information or identifying information, such as social security numbers. Hang up and contact the organization directly to verify the caller's claims.
- Ask for a call-back number if you are suspicious of the caller.
- Most financial institutions will not ask for personal and account information via email. Do not reply to the email and contact your financial institution to verify the email's claims.
- Fraudulent emails often include spelling and grammatical errors, do not address recipient by name, claim that you are a victim of fraud, or urgently warn you that your account will be compromised if you do not confirm your account information.
- Educate yourself on how to protect your finances and identity. MyCreditUnion.gov, a consumer site run by the National Credit Union Association (NCUA), provides useful information on current fraud and scams.

For more information, contact Member Services at 800-388-7889 / 214-574-3110 or info@mobilitycu.com.

Updated 4/30/2014