Account Protection Tips

Checking Account:

- Report lost or stolen cards/checks immediately.
- Review account statements carefully. Notify the Credit Union of suspicious charges.
- Monitor your account online any time with online banking and mobile banking.
- Carry your checkbook only when necessary

Debit and Credit Cards

- Always keep your credit or debit card in a safe and secure place. Contact card issuers immediately if your card is lost or stolen, or if you suspect unauthorized use.
- Do not give out your card number over the phone unless you initiated the call.
- Sign your card as soon as you receive it and NEVER keep your PIN on the card. Never give your card or PIN to anyone else.
- Carefully monitor ATM and gas pumps for skimmers. A skimmer is a device that fits over an existing card reading and that harvests data off a card's magnetic stripe.
- Check your account activity regularly or setup eLerts in online banking that will notify you of any activity. Download our mobile app in Apple or Google play for convenient account access.
- Consider using a Financial Center VISA® credit card for online purchases. Although we cover you against any fraud on both your Financial Center credit and debit cards**, your debit card links directly to your checking account. Debit card fraud can create greater vulnerability and tie up your funds temporarily. Using a credit card provides the same level of coverage without the concern of impacting your everyday banking.
- Enroll in Financial Centers IDProtect® Service, available with our new Champion Checking* account.

Online

- Do not use your Social Security number as a username or password.
- Protect your online passwords. Don't write them down or share them with anyone.
- Make sure any internet purchase is secured with encryption to protect your account information. Look for secure transaction symbols such as a lock symbol in the lower right-hand corner of your web browser, or "https://..." in the address bar of the website.

Email

- Never open attachments, click on links, or respond to emails from suspicious or unknown senders. **Financial Center will never send you an email requesting personal/account information**. Report suspicious emails immediately.

Mobile

- Use the security functions that come with your devices, such as the keypad or phone lock function when it is not in use.
- Avoid storing your banking password or other sensitive information on your smartphone or in an app where it could be discovered if your phone is lost or stolen.
- Only download banking apps from your phone carrier's app store. Search 'Financial Center' to download our mobile app from your app store.