HELPFUL TIPS TO AVOID FRAUD

- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Ensure Multi-Factor Authentication (MFA) is implemented on all sensitive log in environments.
- Use cybersecurity best practices, including:
  - Enabling anti-phishing protection on your web browser
  - Adding multi-factor authentication to account log ins
  - Using unique, strong passwords for different accounts
  - Not clicking on unsolicited links
- Contact the credit union directly by using the phone number or website listed on the back of your card, rather than following instructions from an email, phone call or text message your received.
- Never provide a one-time passcode to a caller or via email or SMS text message, and do not install Remote Access software unless instructed by a trusted system support provider.
- Check shipping details on accounts. Be aware of details in the 2nd or 3rd lines of the shipping addresses that might be used to reroute packages.
- Review bills, statements, and credit reports to identify anomalies that could indicate fraud, identity theft or if someone else has access to your account.
- Look for the "s" – When paying online, check the URL to ensure it begins with https://. The "s" at the end indicates a secure connection. Also check that the name of the web page does not contain spelling errors or strange characters.
- Update system and application software – Install the latest software on your computer, tablet or phone.
- Take advantage of identity and credit monitoring services.
- Watch for scam indicators in the method of payment being requested: scammers often ask for payment in the form of wire transfers or other money transfers, reloadable or prepaid gift cards, cryptocurrency or sending cash, since these formats are more difficult to trace.
- If you suspect a scam, stop, and call back the credit union or organization. Talk to someone using trusted phone numbers.

Use caution when posting on social media. Be aware that sharing sensitive personal information can provide criminals with clues to answer your security questions or craft believable, targeted scam messages.