

FRAUD DOS AND DO NOTS



- Educate yourself and stay up to date with recent scams.
- Remain vigilant, and act fast if you believe you have fallen victim to a scam or fraud.
- Answer phone calls with caution, and forward unknown numbers to your voicemail.
- Verify the purpose of a call and the identity of the caller.
- Create strong login information, and only share passwords with trusted individuals.
- Use safe devices to log into accounts, and always log back out.
- Protect your mail.
- Shred sensitive documents.
- Monitor your credit report often.
- Implement fraud detection tools with your bank or other offering reputable companies.
- Choose your caregivers carefully, and have a trusted individual oversee your finances, if necessary.



- Do not answer unknown phone numbers. Government agencies or financial institutions will never call demanding for urgent financial transactions or personal information.
- Do not provide personal identifying information to questionable sources.
- Do not click or open suspicious texts, e-mails or links.
- Do not accept offers, gift cards, jewelry or valuable items from strangers that sound or look too good to be true.
- Do not leave any bags, wallets, or items with personal identifiers in shopping carts.
- Do not mail, wire transfer, or pay money to unknown, questionable sources.
- Do not communicate with strangers on social media outlets who seem questionably friendly, or ask for financial assistance.
- Do not use outdated ATM machines, or insert cards in outlets that seem loose or installed incorrectly.