Some DO's and DON'Ts to Protect Yourself from Fraud

NEVER cash or deposit a check that you have no real valid reason for receiving. You should always know and trust the check payor when negotiating a check.

NEVER send money through Venmo, PayPal, Cash App, Zelle, or other various electronic methods to individuals that you do not know and trust.

NEVER buy gift cards, send cryptocurrency, or send a wire transfer as a form of payment or reimbursement to individuals and businesses that you do not know and trust.

NEVER provide your Social Security number, date of birth and other identifying information over the phone or by email.

NEVER allow remote access to your computer or smartphone to another individual or business.

NEVER allow another individual access to your online banking services and mobile banking apps.

NEVER allow another individual access to your debit card and PIN number.

NEVER open email attachments or links from individuals or companies that you do not know and trust. Examine the email address to determine if it looks suspicious. Business emails typically will not use domains such as yahoo.com, gmail.com, or hotmail.com. A business will generally use their company name in their email address.

ALWAYS be cautious of Caller ID when receiving telephone calls and texts. Caller ID is not always trustworthy. Criminals can spoof Caller ID to disguise their identity. If you're unsure, always hang up and call the person or business back at a number you know and trust.

ALWAYS check your monthly statements and/or online transaction history timely. Report any unauthorized activity immediately to your financial institution.

ALWAYS report a lost or stolen card to your financial institution immediately upon discovery.

ALWAYS understand the risks PRIOR to completing transactions. Funds generally cannot be recovered after they have been moved.

ALWAYS use caution when communicating with individuals that you meet online through dating sites and social media. Criminals use these platforms to create phony relationships and acquire trust with individuals for financial gain.

ALWAYS contact your financial institution for advice any time you are being coerced into conducting transactions that you feel uncomfortable about.

ALWAYS trust your instincts. If something doesn't seem right, it is worth taking extra precautions to keep your money safe.

ALWAYS contact your financial institution immediately to report identity theft and suspicious transactions in your account.

First Choice America will never contact you by telephone, text, or email to ask for personal sensitive information such as your social security number, account number, card number, or passwords. Please be aware of calls, texts, or emails that appear to be coming from First Choice America. If you receive any suspicious communications, please do not engage. Instead, contact us at 304-748-8600 to address concerns about your account.

For more information about frauds and scams, please contact First Choice America Community Federal Credit Union's Compliance Department by calling 304-748-8600, ext. 716.