Fraud Prevention Tips

Do's

• Monitor your bank and credit card statements regularly.

• Set up alerts & notifications on bank accounts & credit cards.

• Use strong, unique passwords for all your online accounts.

• Enable multi-factor authentication (MFA) whenever possible.

• Verify the legitimacy of emails, phone calls, or messages before responding.

• Shred documents that contain personal or financial information.

• Update your devices and software to the latest security versions.

• Use secure Wi-Fi networks, especially when handling financial transactions.

• Limit who you provide your account information to. Pay bills through bank's bill pay verses the bill's website.

• Use a separate account & debit card or a virtual credit card for online purchases and subscriptions.

• Be aware of the company/merchant you are doing business with. Do your research.

• "Lock up" your debit cards and credit cards when not in use.

• Obtain your credit report once year by getting a free credit report through AnnualCreditReport.com

• Place a credit freeze on all three credit bureaus

• Protect your passwords and PIN numbers. Sheild (Cover up) the pin pads when entering your pin numbers at ATMs, stores, restaurants, gas stations, etc.

• Add your contacts names and phone numbers to your cell phone, so you know who is calling you.

Don'ts

• Do not share personal information such as Social Security numbers, account numbers or passwords.

• Do not click links or open attachments from unknown senders.

• Do not use public Wi-Fi for online banking or shopping. Hospitals, airports, and hotels are prime targets

• Do not trust unsolicited phone calls requesting financial information.

• Do not store sensitive information in easily accessible places.

• Do not ignore alerts or messages from your bank regarding suspicious activity.

• Do not provide or allow remote access to your computer or cell phone.

• Do not answer phone calls of phone numbers you do not know or a call that comes through saying "spam risk." If the call is important, they will leave a message.

Important Notes & Questions to Ask Oneself

• If it is too good to be true, it is.

• Does this make sense?

• Was I expecting this email, phone call, letter, check, etc.?

• What sources can I contact to find out if this situation is legitimate?

• Think before you click. Think before you respond.

• Are the "scammers" asking for money to be withdrawn, wired, sent in form of gift cards, and/or in precious metals like gold? If so, IT'S A SCAM!!!! DO NOT SEND MONEY OR PROVIDE ANY ACCOUNT INFORMATION.