BEWARE THESE COMMON TYPES OF PHONE SCAMS!

Here are some tips on how to respond:

Threatening calls from the IRS

The IRS never calls; they only communicate in writing.

Law Enforcement Agency Calls

Do not respond to a call you cannot verify as to its authenticity; never give out bank information on threatening calls from law enforcement. Real law enforcement and federal agencies won't call and threaten you. Don't give personal information such as SSN, date of birth or address information.

Bank Fraud

This occurs when someone is pretending to represent your financial institution. They will indicate that a fraud may have occurred on your account, and will request password and account number. Immediately hang up and call your institution directly on a verified phone number.

Website Password Request

Never respond to a request over the phone asking for access to a website.

Lottery

Have you ever received a call or email saying that you have won a certain amount of money in a lottery, but you need to wire money to pay the taxes? Do not provide the caller with any personal information, especially your credit union/bank account information. **Never** wire money in situations such as this.

Family Members in Peril

This type of scam typically targets the elderly. If you ever receive a phone call from a family member that is in crisis and requires immediate payment, **hang up** if the call is from an unknown number and contact your family member on a trusted phone number.

COVID Vaccine

In an attempt to convince you to provide personal or medical information, scammers will offer early access to the vaccine or to have the vaccine shipped to you for a direct payment. **Never** share personal identifiable information over the phone.

Insurance, Health Care and Debt

Typically, this is an attempt to get personal information such as Social Security Number, Date of Birth and address. Frequently an extended warranty on your automobile is offered. Do not answer a call from an unknown number.

Technical Support

If you receive a call or email from a well respected company such as Apple or Microsoft stating they have detected a problem on your personal computer **do not respond** to the call or click on a link, as this could subject your computer to a virus.

Fake Charity Appeals

Do not make donations to unsolicited callers.

What to do if you believe you are a victim of some of these scams:

- ⚠ Immediately contact your financial institution(s) and notify them of the breach and to issue new debit/credit cards.
- ⚠ Contact the 3 primary credit reporting agencies to place a freeze on your account - this can be done online and will prevent fraudulent loan activity under your name.
- ⚠ Contact the IRS so that someone cannot fraudulently file a tax return under your name; a special PIN number will be provided by the IRS.
- ⚠ Contact the 3 primary credit reporting agencies to place a freeze on your account - this can be done online and will prevent fraudulent loan activity under your name.
- ⚠ If you are receiving Social Security Payments, immediately contact the local Social Security office to prevent payments from being diverted as a result of the ID theft.
- ⚠ Retain the phone number or email information and contact your local police department to make a report.

Register for the National Do Not Call List: donotcall.gov