WIRE TRANSFER FRAUD WARNING

Many times we do our communicating via email and never personally speak to the other party. In this day and age where "Hackers" can take over your email communications, we need to be very careful. This is especially important when doing business and there is going to be money or personal information transferred. Here are a few ways to help prevent your information from being "Hacked" by these Cyber criminals.

1. **Do not** use contact information (phone number, email, and website) that was included in the email as it might not be valid. Check your most recent billing statement to personally contact the person with whom you are doing business. Call them to confirm any personal information, email or money transfer transactions.

2. Even when something looks or sounds legitimate, **do not act on any change of wiring or Electronic Funds Transfer (EFT) instructions that you receive electronically (via email)**. Always call the original person you are dealing with to confirm the change.

3. Whenever possible, use alternatives to wire transfers or EFT's. For small transactions, make the payment in person by check or credit card.

These "Hackers" can create very legitimate looking documents and emails allegedly from Banks or Lending Institutions. Be aware and contact a relative, friend or neighbor for advice when you receive an unsolicited letter, email or phone call where you are asked to send money or personal information.

2/4/19