VILLAGE OF CLOUDCROFT NEW MEXICO

TO: **VILLAGE OF CLOUDCROFT RESIDENTS & VISITORS** **OCTOBER 5, 2022**

FROM: **KEVIN SUMMERS, CHIEF OF POLICE**

SUBJECT: **PHONE & INTERNET SCAMS**

During these trying times, scammers may try to take advantage of you. They might get in touch by phone, email, postal mail, text, or social media. Protect your money and your identity.

DO NOT SHARE PERSONAL INFORMATION LIKE YOUR BANK ACCOUNT NUMBER, CREDIT OR DEBIT CARD NUMBER, SOCIAL SECURITY NUMBER, OR DATE OF BIRTH.

The most common banking scams include:

- Overpayment scams - Someone sends you a check, instructs you to deposit it in your bank account, and wire part of the money back to them. But the check was fake, so you'll have to pay your bank the amount of the check, plus you'll lose any money you wired.
- Unsolicited check fraud - A scammer sends you a check for no reason. If you cash it, you may be authorizing the purchase of items or signing up for a loan you didn't ask for.
- Automatic withdrawals - A scam company sets up automatic withdrawals from your bank account to qualify for a free trial or to collect a prize.
- Phishing - You receive an email message that asks you to verify or change your bank account or debit/credit card number.

Remember these tips to avoid a banking scam:

Do:

- Hang up on suspicious callers and ignore suspicious text messages and/or emails.
- Be suspicious if you are told to wire a portion of funds from a check you received back to a company.
- Be wary of lotteries, free trials, and callers claiming you've won money that ask for your bank account information.
- Verify the authenticity of a cashier's check with the bank that it is drawn on before depositing it.
- When verifying a check or the issuer, use contact information on a bank's website.
- Be cautious of caller ID. Scammers can change the phone number that shows up on your caller ID screen. This is called "spoofing."

Don't:

- Don't say anything if a caller starts the call asking, "Can you hear me?" This is a common tactic for scammers to record you saying "yes." Scammers record your "yes" response and use it as proof that you agreed to a credit card and/or bank account charge.
- Don't trust the appearance of checks or money orders. Scammers can make them look legitimate and official.
- Don't deposit checks or money orders from strangers or companies you don't have a relationship with.
- Don't wire money to people or companies you don't know.
- Don't give your bank account number to someone who calls you, even for verification purposes.
- Don't click on links in an email to verify your bank account.
- Don't accept a check that includes an overpayment.