RENY
RETIRED EDUCATORS OF NY

OUTSMART SCAMMERS

Protecting your finances is one of our highest priorities. That includes arming you with knowledge to defend against banking fraud.

Most Banks will never ask you to verify personal information via text, direct message or e-mail. If you get a call from someone saying they're from Community Bank and you are uncomfortable or unsure, please:

- Ask for the individual's name and ask to call them back
- Call back the individual through your local branch or their Customer Service center

Banks will never contact you for personal information like:

- Passwords
- Account numbers
- Social Security numbers

If something doesn't feel right to you, it probably isn't. Stop and talk to someone you trust. Before you do anything else, tell someone — a friend, a family member, a neighbor, your local banker — talking about it could help you realize it's a scam.

Know the signs that it's a SCAM. Never send money, provide personal or financial information to anyone whose identity you can't independently verify or in response to an unexpected request. When confirming the identity of someone, call a TRUSTED and verified phone number (the one provided to you could be part of the scam.)

We're on guard against cyberattacks and our security team undergoes regular training to stay ahead of the latest methods to safeguard your accounts.

FOUR SIGNS THAT IT'S A SCAM

1. **Scammers say there's a PROBLEM or a PRIZE.**
   They might say: you or a family member is in trouble with the law or you owe money; someone in your family had an emergency; or, there's a virus on your computer.

   Some scammers say there's a problem with one of your accounts and that you need to verify some information.

   Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

2. **Scammers PRETEND to be from an organization you know.**
   Scammers often pretend to be contacting you on behalf of the government (IRS), a financial institution or investment firm. Some pretend to be from a business you know, like a utility company or even a charity asking for donations.

   Some use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

3. **Scammers PRESSURE you to act immediately.**
   Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story.

   They might threaten to arrest or sue you. They might even say your computer is about to be corrupted. Or that your accounts will be locked.

4. **Scammers tell you to PAY in a specific way.**
   They often insist that you pay by transferring money (wire or instant money transfers like Zelle®), or by putting money on a gift card and then giving them the number on the back. Some will send you a check to deposit or even ask for your online banking credentials so they can mobile deposit the check for you. They then tell you to send them money and the check later turns out to be fake.