# SCAM ALERT:

## BANK IMPERSONATION & NUMBER SPOOFING

Banks and credit unions are reporting their phone numbers are being spoofed by scammers. They pose as your bank or credit union representative and try to get you to reveal sensitive personal information like your passwords or PINs, or transfer money directly to them.

## THIS IS A SCAM

- **Protect Yourself:**
  - **Be cautious of unsolicited contact:** If you get an unsolicited call or text from your bank regarding an urgent issue, treat it with caution. You can always hang up and verify the communication is legitimate by calling the number on the back of your card.
  - **Watch for urgent or threatening language:** Scammers fabricate a crisis scenario involving your account to create a sense of urgency. If you're feeling pressured, hang up and contact your bank on your own through official channels.
  - **Beware of requests to transfer money to a "new" account:** Scammers may claim there is fraud on your account and ask you to move your remaining funds into a "new" account via Zelle®, wire transfer, or a digital wallet. These accounts belong to the scammers.
  - **Do not participate in a 'sting operation':** Impostor scammers may claim a local branch employee is implicated in fraud and tell you to initiate a transfer or lie to other bank employees about your withdrawal. No reputable bank would ask you to do this.
  - **Deny requests for remote access:** If someone claiming to be from your bank asks for remote access to any of your devices or accounts to "fix" an issue, it's most likely a scammer.
  - **Avoid sharing sensitive information:** Never share your passwords, PINs, account numbers, or Social Security number with anyone.
  - **Monitor your accounts regularly:** Keep a close eye on your accounts by reading your monthly statements and periodically logging in to give everything a quick scan to notice any potential discrepancies.

Scammers rely on fear, urgency, and the promise of a quick solution to bypass your better judgment. If you have any concerns that you're not speaking with who you think you are, you should disengage and call the bank directly using a number you can trust, typically found on the back of your card or account statement.

**VISIT US ONLINE AT IOWAFRAUDFIGHTERS.GOV**