Is That Really My Bank?

GENERATIONAL KNOWLEDGE LLC

A verification card for calls, texts, emails, and account alerts.

What Scammers Can Fake

Caller ID, a familiar logo, a believable message, and even some personal details. **These do not prove a caller is from your bank**.

What Your Bank Will Never Ask You

Your bank will never ask you for PINS, One-time passcodes (OTS), card CVV codes, your full Social Security number (SSN), your online security question, or to transfer money. Beware of any call, text, email, or account alert that asks you to do so.

Use this Verification Routine

1. Do not click the message link or call the number supplied in the suspicious message.
2. End the call or close the message.
3. Open your bank's official app yourself, or call the number printed on your card.
4. Ask whether there is a genuine alert or suspicious activity on your account.
5. If needed, change credentials and follow the bank's fraud procedures.

Never Give an Unexpected Caller

- Your online banking password or PIN.
- One-time authentication or password-reset codes.
- Remote access to your phone or computer. Never install unfamiliar software on a computer sent to you via a caller, text message, or email.

A Sentence You Can Use

"I'll contact my bank directly using the number on my card. Thank you."

My Bank Contact Plan

Where I keep my bank's verified contact number:

If you suspect unauthorized transactions, contact your financial institution promptly.