Beware of the Call Forwarding Scam

How the SCAM works

1 The Initial Contact

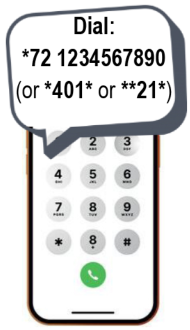
You receive an urgent phone call, text, or message from someone spoofing your credit union's name on your caller ID.

2 Creating Urgency

The scammer claims there is "suspicious activity" or a "fraudulent charge" on your account and that immediate action is required to secure your funds.

3 The Trap

They instruct you to dial a specific activation code followed by a 10-digit number that they provide. The code is typically *72 (or sometimes *401* or **21*).



4 The Hijack

Dialing this sequence unconditionally forwards all your incoming calls to the scammer's phone. When you attempt to log in or when your credit union calls to verify a transaction, the scammer receives the verification code instead of you.

How to PROTECT Yourself

Never Dial Unknown Star Codes

Do not follow instructions from a stranger to dial codes starting with an asterisk (*) or pound sign (#).

Hang up and call NCE Credit Union Directly

If you receive a call from your "Credit Union" about a security issue, hang up immediately. Call the official number on the back your debit card.

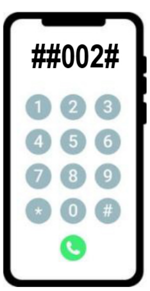
Never Share Codes

Legitimate credit union and financial institutions will never ask you to provide a security code, one-time passcode (OTP), PIN, or authentication code over the phone.

What to do if you've BEEN SCAMMED

1 Cancel the Forwarding Immediately

On most mobile networks dial ##002# and press the call button to deactivate any active call forwarding.

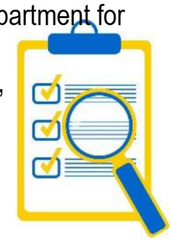


2 Contact NCE Credit Union Immediately

Notify the fraud department right away so they can secure your accounts, review recent transactions, and monitor for unauthorized activity. Call the number on the back of your debit card or call the credit union directly at (361) 882-4780, speak to Member Services

3 Review Security Resources

Consult your credit union's fraud prevention resources, security center, or member services department for additional guidance on securing your accounts, updating passwords, and protecting your identity.



REMEMBER:

Caller ID can be spoofed. Even if the call appears to come from your credit union, always verify by hanging up and calling the official number yourself.

What is Check Fraud?

Check fraud happens when someone steals, alters, or misuses a check to access money or banking information.

Common examples include stolen checks, altered checks, fake checks, forged signatures, and scam-related fake payments.

Who is Most at Risk?

* Renters paying by check
* Small business owners
* Families managing shared finances
* Older adults
* Young adults targeted by job scams

Simple Ways to Protect Yourself

* Mail checks from inside the post office
* Avoid leaving outgoing checks in the mailbox overnight
* Use gel ink and avoid leaving blank spaces on checks (blank space can make it easier for scammers to alter information)
* Monitor your bank account
* Set up account alerts
* Be cautious of unexpected checks, checks received electronically or through messaging apps
* Never send money back on "pending" deposits alone

If Something Looks Wrong

Contact your financial institution immediately!

Check Fraud Can also be Digital

Check fraud isn't limited to paper checks anymore. Today, scammers may also use electronic checks or digital methods, including:

* Sending fake checks electronically via email or messaging apps
* Asking you to deposit checks through a mobile banking app
* Combing fake checks with requests to send money back quickly

Even if a check appears in your account, it does not always mean the money is real or finalized.

NUECES COUNTY EMPLOYEES

NCE

Credit Union

FBI FRAUD ALERT

IF YOU CAN ANSWER "YES" TO ANY OF THE FOLLOWING QUESTIONS, YOU COULD BE INVOLVED IN A FRAUD OR ABOUT TO BE SCAMMED!

DON'T GET RIPPED OFF!

- Is the **CHECK** from an item you sold on the Internet, such as a car, boat, jewelry, etc?
- Is the amount of the **CHECK** more than the item's selling price?
- Did you receive the **CHECK** via an overnight delivery service?
- Is the **CHECK** connected to communicating with someone by email?
- Is the **CHECK** drawn on a business or individual account that is different from the person buying your item or product?
- Have you been informed that you were the winner of a **LOTTERY**, such as Canadian, Australian, El Gordo, or El Mundo, that you did not enter?
- Have you been instructed to either **"WIRE", "SEND" OR "SHIP" MONEY**, as soon as possible, to a large U.S. city or to another country, such as Canada, England, or Nigeria?
- Have you been asked to **PAY** money to receive a deposit from another country such as Canada, England, or Nigeria?
- Are you receiving **PAY** or a **COMMISSION** for facilitating money transfers through your account?
- Did you respond to an email requesting you to **CONFIRM, UPDATE, OR PROVIDE** your account information?

TELL BRANCH PERSONNEL IMMEDIATELY!