# BEWARE OF THE CALL FORWARDING SCAM

## HOW THE SCAM WORKS

### 1 THE INITIAL CONTACT

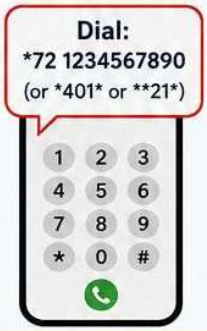
You receive an urgent phone call, text, or message from someone spoofing your credit union's name on your caller ID.


### 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 YOUR 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 of your debit or credit card, of use your credit union's official website or mobile app to contact them. They can connect you to the legitimate fraud department.

### NEVER SHARE CODES

Legitimate credit unions 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 YOUR 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 or credit card and request to be connected to the fraud department.

### 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.