



# NOBLE CREDIT UNION

## Tell the Scammers to Skedaddle

They're out there, of that there is no doubt. We're talking about fraudsters, people who looking to catch you off-guard in the hopes you'll give them some personal and/or account information. You have the power to stop them. It starts with knowing what to look for:

- A call or text from a phone number you don't recognize – a tactic called spoofing
- An email from someone you don't know that contains a link or attachments – a tactic called phishing
- A communication with someone that you have not initiated yourself

Not all communications are potentially fraudulent. Noble Credit Union Credit Union has *numerous* fraud protection measures to protect your accounts and personal information. One such fraud protection is a communication to you when an unusual transaction is done using your debit and/or credit card. If something unusual appears, we will contact you. Recently Noble Credit Union Credit Union members were contacted via a spoofing tactic claiming to be a Noble Credit Union representative who "noticed unusual transactions." What made this outreach different from a real one is that the people on the other end asked for personal and account information...this is something Noble Credit Union will NEVER do. Here's what you can expect from Noble Credit Union:

1. No links of any kind will be included in the text message regarding a possible fraudulent transaction. You will simply be instructed to respond "yes" or "no" to the notification text message.
2. Text messages regarding account transactions will always come from a 5-digit number and NOT a 10-digit number.
3. When on a phone call with a Noble Credit Union representative, they will ask only for your zip code UNLESS you confirm that a transaction is fraudulent. If the transaction is fraudulent, you will be transferred to another agent, who will confirm your identity before going through your transactions with you.
4. Noble Credit Union will NEVER ask you for your PIN, the 3-digit security code on the back of your card, or the multi-factor verification code. If you are asked for this information, hang up and immediately call Noble Credit Union.

If you receive a text or email you are unsure about from an unknown sender, do not click on any links or open any attachments. If you receive a phone call you believe could be from a fraudulent caller or that the person you are speaking with is not from Noble Credit Union, hang up and call us directly at 252-5000. This is true of anyone contacting you from any organization. When in doubt, do not give out any personal or account information, don't hang on, hang up, and call the company directly using the phone number provided on a billing statement, documentation, and/or their website.

Three steps you can do immediately if you believe your Noble debit or credit card is being used without your permission:

1. Call Noble Credit Union right away at 252-5000.
2. Log into your Noble Credit Union online banking account (either from a computer or your mobile device) and navigate to the Card Control feature. The debit and/or credit cards you have with Noble Credit Union will be displayed. Toggling the card to "off" will immediately prevent any transactions associated with that card number from taking place, stopping the bad guys right in their tracks. If you need to use the card, you can simply toggle the card back to "on."
3. Continue to monitor your account and notify the Credit Union if you see any transactions you don't recognize.

Keep you and your family safe from fraudsters and stay informed by visiting Noble Credit Union's security page at <https://www.noblecu.com/home/security>. There you'll find lots of great tips to protect yourself.