Protect Yourself
FROM FRAUD AND IDENTITY THEFT

Centris
FEDERAL CREDIT UNION

As your trusted financial institution, our responsibility is to educate our members about fraud and how to prevent it. The following information provides our members with the details needed to stay vigilant against fraudsters and scammers.

Types of Scams

Fraud and scams that can negatively impact our personal identity or financials have become increasingly common. A general rule of thumb to follow is if an offer seems too good to be true, it probably is. One of the ways to help prevent fraud from happening is to understand the different types of scams that you could encounter. Here are a few common scenarios to be aware of:

- You've won or inherited something and need to pay taxes or fees before receiving the disbursement.
- You are told you have been overpaid and are asked to pay back or forward the excess funds.
- A caller threatens you.
- Someone from a dating or social media site allegedly needs money to come home/visit.
- A work from home job posting or loan company asks for your online banking login information or requests fees, class materials, etc. be paid up front.
- No legitimate business will ask you to pay them in gift cards. This is a scam.
- You are contacted about an investment opportunity and need to send funds immediately to lock the current rate.
- Someone disguises themselves as a company, financial institution or person that you regularly do business or correspond with by changing one letter, symbol or number in an email address, sender name, phone number or website URL.

Fraud Protection Tips

In the digital age, fraudsters and scammers have more ways to target individuals than ever before, such as email, text and social media. It's important to stay up to date on fraud prevention tips along with details so you can be proactive in protecting your finances and identity.

- Monitoring your bank accounts daily will allow you to catch any suspicious activity quickly. To help monitor your accounts, you can set up alerts though Centris online banking (Click on Services then click Alerts). Notify Centris immediately of any unauthorized transactions.
- Never give your password, account information or personal information to someone who calls you, even for identification purposes. If they initiate the call, they have to prove who they are, not the other way around.
- Use a password manager to generate unique passwords for all your different logins. Never reuse your banking credentials for other sites.
- Be wary of popups that appear on your electronic device from companies you do not do business with (i.e., Microsoft or Norton). These may appear out of the blue noting an overpayment or a compromise on your device.

CONTINUED ON BACK ›

FRAUD PROTECTION TIPS CONTINUED

- Don't download attachments or click on links in questionable emails, especially if it's claiming there is a problem with your account or asking you to reset your password. Go directly to the site in question by searching the URL in your web browser.
- Carefully examine the email address, URL and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Set-up two-factor (multi-factor) authentication on any account that allows it, and never disable it.
- Keep devices secure by installing updates and patches frequently and in a timely manner when prompted to do so.

Reporting Fraud

If you suspect you've been the victim of a scam, **call Centris Federal Credit Union at 402-334-7000 immediately**. If you've been a victim of identity theft, you can visit **www.identitytheft.gov/Steps** for tips on what you need to do right away and next steps to protect yourself and your accounts.

Scan the QR code below to visit the **Centris Federal Credit Union Cybersecurity Center**. This is a great resource with details on steps to take if you've been the victim of a scam. The site is updated quarterly with valuable educational articles including information on new fraud trends. For more information, check out our social media platforms. You can also find valuable insights on fraud prevention on the Centris Podcast, "A Penny or Two for Your Thoughts" wherever you get your podcasts.

Centris FEDERAL CREDIT UNION

Scan here to learn more.

How will Centris contact me?

Unfortunately, some fraudsters pretend to be from your trusted financial institution. So how can you tell if someone is legitimate or not? Knowing how your financial institution will contact you about suspected fraud is one way. Here's how the team at Centris will contact members:

Phone

- Our Member Protection Team will reach out to a member if they believe there is risk of fraud on an account.
- We will never call you and ask for sensitive personal information.

Text Alerts

- If you've enrolled in alerts through Centris mobile banking or the Centris Debit Card Companion App, you may receive text and/or email alerts.
  - For these alerts, we will never ask you to click a link or provide personal information including credentials.
- If you have a loan with Centris and missed a loan payment, you may get a reminder text regarding the payment from 402-315-2650. This text will include a link to make a payment. If you have any concerns or are unsure if the text is coming from Centris Federal Credit Union, you can find the 'Make A Payment' link on our homepage at www.centrisfcu.org.
- If you apply for a digital loan with Centris, you may receive text communications regarding your loan status from 402-697-6665.

Secure Access Codes (SAC)

- SAC may be sent via text, email or phone call to authenticate your identity when logging into Centris online banking.
  - You should never provide this code to anyone.

Debit Card

- VISA® Fraud Protection (Debit Card): If the VISA Team detects suspicious activity with your debit card, they will reach out via email, phone call and/or text.
  - Their communication will never include links and will not require your account information, such as PINs or card numbers.

Credit Card:

- If there is potentially fraudulent activity with your credit card, Elan will call the card holder.
  - They will never ask you for your card's CVV (three-digit code on the back of the card) or issue/expiration date.