Fraud Alerts, Scams & Tips: What Members Need to Know

Protecting You From Fraud & Scams

Phantom Debt Scam: It's Not Your Imagination

A phantom debt collection scam is when someone calls, emails, or sends a letter saying you owe money, but the debt they're talking about is fake. It might be something you already paid, something you never owed, or something completely made up.

In cases where there is an outstanding loan, the scammer may claim that the victim owes far more in fees and interest than they actually do. In other cases, the victim of the scam may be behind on a loan, but the caller has no authority to actually collect on the debt. These con artists are even threatening and convincing enough to make you wonder whether someone has taken out a loan in your name. No matter your actual situation, don't let them convince you to hand over precious cash to settle the "debt."

Here are some red flags to watch for:

- You don't recognize the debt. You're sure you never borrowed money from that company.
- They won't give you details. They claim you owe money but won't explain why.

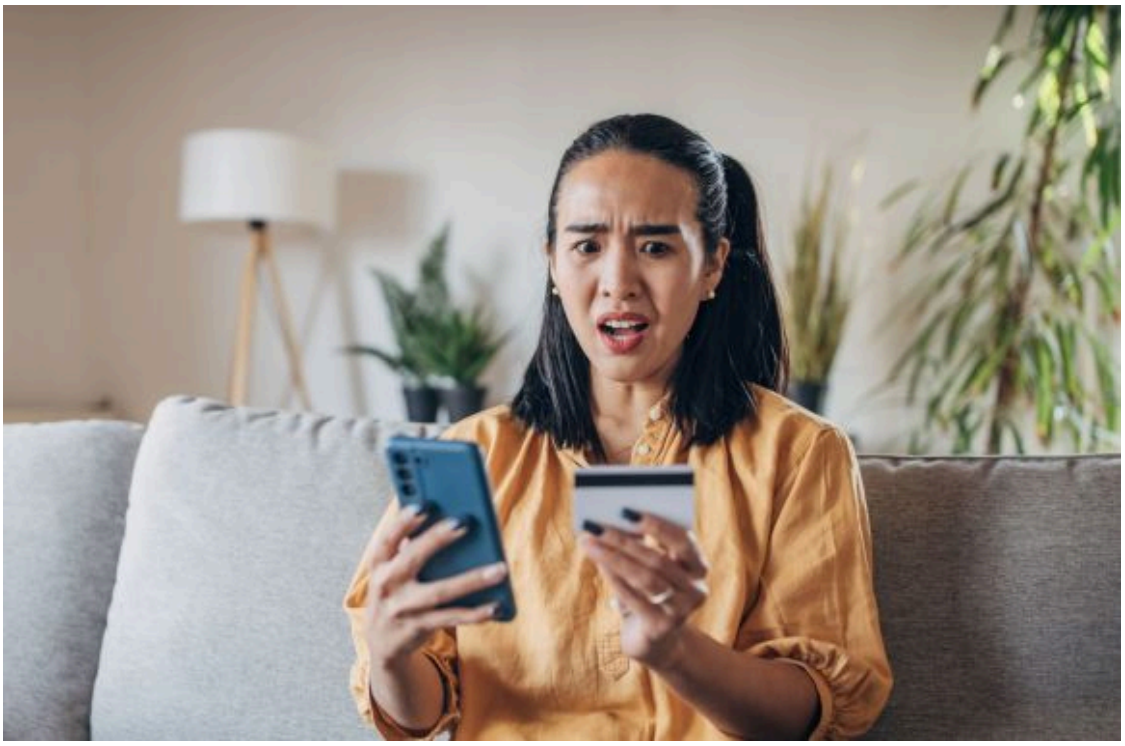
- They refuse to send a letter. Real collectors must send something in writing within 5 days.
- They ask you to pay right away, using an unusual payment method. They may want you to pay by wire transfer, prepaid card, or gift card—methods that are hard to trace.
- They threaten you. They say you'll go to jail or lose your benefits if you don't pay.

To avoid a phantom scam:

- Ask the caller to contact you by mail and provide written proof of the debt. The Fair Debt Collection Practices Act requires debt collectors to stop calling their targets if they are asked to do so.
- If you receive a call from someone claiming to be from a government agency or official-sounding institution who says you owe money on a debt, hang up and call the organization in question directly.
- Look up numbers or email addresses for lenders on your own or rely on your loan paperwork to find a legitimate contact number.

If you receive a call from a phantom debt collection scammer, you may have had your personal information exposed, raising the risk of identity theft. The Federal Trade Commission (FTC) offers a step-by-step process for recovering from identity theft. Even if you didn't lose money, report the scam to the FTC or the Consumer Finance Protection Bureau so others can be warned.

The Holidays May Be Over, But Scammers Haven't Gone Home



The holiday shopping season may be behind us, but shopping scammers are keeping busy year-round. One way to remain vigilant with your everyday shopping is to understand the different benefits and risks associated with popular payment methods – from credit and debit cards to more novel services like buy now, pay later and payment apps.

Credit Cards

While credit cards enjoy the strongest legal protections against fraud out of all the payment methods, with features like clear dispute processes and the ability to remotely and instantly lock a lost or stolen card, you must remember to:

- Regularly check your transaction activity since most card issuers require prompt reporting of fraud.
- Pay off the debt each cycle to avoid accumulating interest.

Debit Cards

Generally, paying with a debit card is riskier than paying with a credit card because debit cards have fewer legal protections against fraud. If your card is stolen or you notice unfamiliar charges, contact your bank immediately. Most banks will require notice within just a few days to limit your liability.

Buy Now, Pay Later

Buy now, pay later (BNPL) offerings may be attractive to shoppers looking to spread costs over a few weeks, but there are risks involved:

- Late fees and other hidden charges.
- Keeping up with staggered payments; it can become difficult to track competing payment dates.
- Overextension. Just because a seller provides the option to use BNPL doesn't mean it's the best method for your financial situation.

Payment Apps

While these platforms can be convenient, they're best used with friends and family. Most legitimate sellers will not ask for payment over Cash App, Venmo, or Zelle. Paying with these peer-to-peer apps carries a couple of important risks.

- Few—if any—refund protections. While Zelle has announced limited protections for victims of imposter fraud, the full extent of these safeguards is still unknown and unreliable.
- Scammers have taken advantage of the near-instant transfer of funds offered by these apps, in addition to some users' limited knowledge of the technology.

Don't Fall for the Bait!

Phishing emails and spoofing continue to be some of the most prevalent forms of fraud.

Phishing attacks can be spotted by their suspicious email addresses, generic greetings, urgent or threatening language, and requests to click on unfamiliar links. The best way to prevent phishing attacks is to use phishing-resistant multifactor authentication (PR-MFA), exercise caution with message links and attachments, and stay informed about the latest phishing tactics.

In a **spoofing** scheme, the fraudster disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source. For example, you might receive an email that looks like it's from your boss, a company you've done business with, or even from someone in your family—but it actually isn't.

If you get a call or message claiming to be a family member or a friend desperate for money, DON'T trust the voice on the line — even if it really sounds like your family member or friend. **Voice spoofers** are effective at mimicking voices, especially with the latest advances in AI.

- **Resist the pressure** to react and send money immediately. Hang up — or tell the person you'll call them right back. If you don't feel comfortable hanging up, try asking a question or using a safe word that only the real person could answer.
- **Use a phone number you know is right** to call or message the family member or friend who (supposedly) contacted you to find out if they're really in trouble.
- **Call someone else in your family or circle of friends**, even if the caller said to keep it a secret, or it sounds like your loved one. Do that especially if you can't reach the friend or family member who's supposed to be in trouble. A trusted person can help you figure out whether the story is true.

Top 3 Fraud Predictions for 2026

Fraud continues to plague families, organizations, and businesses. No one is completely safe. A common theme as we move into 2026 is the growing use of artificial intelligence (AI) as a tool for deception. While this isn't a positive message, it's one we must acknowledge to protect our assets and information.

With that in mind, here are the top three fraud trends to watch out for in the new year:

Business Email Compromise (BEC) and Email Account Compromise

With the aid of artificial intelligence, fraudsters will craft highly targeted communications that appear authentic and convincing. Expect deepfake audio to impersonate your trusted partners, combined with email or text messages to persuade you to alter payment details or initiate new transactions.

To mitigate Business Email Compromise and email account compromise:

- Utilize strong vendor relationships and a robust vendor management program – including emergency contacts and data protection protocols.
- Adopt the STOP–CALL–CONFIRM approach. If you receive a request to change payment details or initiate a new payment: STOP your process, CALL the requestor using a number you know (not the one provided in the message), and CONFIRM the request is legitimate.

Surge in Identity Theft

The ease of creating legitimate-looking websites, business documents, and credit histories is fueling more sophisticated fraud schemes. Businesses that extend credit should prepare for a rise in synthetic identities – combinations of real and fabricated personal data used to commit application fraud. Even nonprofits may be targeted by fraudsters posing as charities seeking funding.

How to fight identity theft:

- Know your customer.
- Conduct thorough due diligence before extending credit or entering purchase agreements.
- Closely guard your personal information and monitor your credit reports and bank statements for unusual activity.
- Freeze your credit to help deter the unauthorized use of your identity.

Multi-Step and Long-Term Scams

Fraudsters are patient. Many scams unfold over months as criminals build trust and credibility:

- Investment scams promising exorbitant returns.

- AI-driven deception– victims may believe they're communicating with an old friend or business associate when, in reality, it's a criminal using AI-generated audio or video.
- Impersonating a "trusted partner" like a bank, attorney, or investment advisor aids a fraudster in their deception and scam. **Remember, People's will never ask you for your User ID and Password combination!**
- Communications designed to direct a victim to a website with the appearance and characteristics of the legitimate site are a favorite tactic of fraudsters.

Contact us:

Email: memberservice@peoplescu.com

Phone: 800.498.8930

** By clicking the above social networking links, you will be re-directed to a Web site not directly controlled by People's Credit Union. We do not endorse or guarantee the products, information or recommendations provided by the linked Web site, and we are not liable for any products, services, or content advertised on those linked Web sites.

Follow Us:

A proof of the "Fraud February 2026" template has been sent to you for review by Jessica Holden, at People's Credit Union.