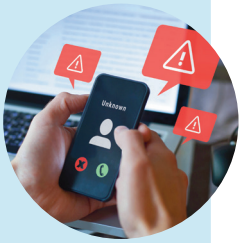
IDENTITY THEFT

MERCK SHARP & DOHME
FEDERAL CREDIT UNION
(215) 996-3700 | msdfcu.org
Federally Insured by the NCUA
Equal Opportunity Lender | Equal Housing Lender

FALL 2025

PAYMENT METHODS THAT SCAMMERS LOVE



No matter how a scam starts – a message from a "friend" asking for help, a phone call claiming to be the IRS, or a stranger contacting you about your online marketplace listing – one of the biggest things to look out for is how they want to handle payment. If anyone asks for one of the payment methods listed below, that's your sign to stop the interaction and verify its legitimacy through other means.

- **Wire transfer** – Wire transfers are like sending cash directly to another person. Once you send it, it's almost impossible to get that money back.
- **Gift cards** – No legitimate agency or person will ask to be paid in gift cards or pre-loaded cards. Gift cards do not have the same protections as your credit or debit card. Once you hand over the gift card's information, the money is gone.
- **Cryptocurrency** – The blockchain behind crypto means that any money you send cannot usually be reversed by the company. Getting your money back requires the other person to send it manually, which a scammer is obviously not going to do.
- **Too-large check** – They might insist on paying you via check, then send too much money and ask you to send some back. But in this case, the check is bad, and by the time your financial institution figures it out, you've already sent the money. Never accept an "overpayment" – destroy the check and ask the buyer to send you a new one, then wait until it properly deposits before sending them what they paid for.

WATCH OUT: VISHING THAT USES AI VOICES

Have you heard about this new phone scam? Fraudsters are using recorded snippets of your voice – or even AI-generated imitations – to deceive your friends and family into believing you're requesting money.

Here are two ways to protect yourself and your loved ones:

1. If you get a call from an unknown number, be careful what you say over the phone. Even something as simple as saying "Hi, this is [your name here]" could be recorded and used for scam tactics later. Instead, do not answer calls from unknown numbers; let them go to voicemail. If you answer and hear silence, hang up. Do NOT say your name or the word "yes."
2. If you get a call from an unknown number and the caller is claiming to be someone you know in a desperate situation, be wary, especially if they're urgently asking for money. Ask them a question only the person you know would be able to answer, or hang up and call the person using the phone number you have saved for them.

Scams are getting more and more sophisticated and it's very easy to fall victim to one. Be vigilant and spread the word!

HOW TO REPORT FRAUD AND SCAMS

If you've been a target of a scam or other type of fraud, reporting it has never been easier. The Federal Trade Commission (FTC) has a simple online form that, once you fill it out and submit it, makes your report available to thousands of law enforcement officers around the country.

Even if you spotted the scam and protected your money and private information, reporting your experience can help the FTC stay on top of current scams and understand how widespread they are.

Report your experience at: **ReportFraud.ftc.gov**

Learn what you can do if you were scammed at: **Consumer.ftc.gov**

STAY SAFE AT THE ATM

Follow these quick tips to help protect your private information!

- Choose an ATM that is in a well-lit area with high traffic.
- Jiggle the card reader – counterfeit card readers are designed to be removeable and will move.
- Cover your hand when you type your PIN.

Federal law allows you to get a FREE COPY of your credit report at your request, from each credit reporting company – Equifax, Experian, and TransUnion.

AnnualCreditReport.com | 1-877-322-8228

RED FLAGS FOR JOB POSTINGS

Looking for a new job to advance your career? Job hunting can be frustrating even on the best of days, but don't let that lower your guard against fake job opportunities. Scammers are always seeking opportunities to steal money and information, so be sure to keep an eye out for these red flags as you navigate the job market.

Be cautious of recruiters and job listings if they:

- Promise a lot of money with little to no experience necessary.
- Ask you to send money or buy start-up materials to get the job.
- Don't disclose information on when or how you'll get paid.
- Only have one form of contact, such as a single email.
- Ask for private information, such as bank account, Social Security or credit card numbers, especially before or during your "interview."
- Don't provide the employer's name or much information about the business.
- Contact you from what seems like a personal email, not a corporate one.
- Move the process along unusually fast, maybe even offering you the job before you interview.

If you're worried that a business could be a scam, here's what you can do to verify its validity:

- Find a second form of contact for the business and verify that the person you're talking to is a legitimate employee.
- Look at reviews of the business online.
- Check with the Better Business Bureau or Attorney General's Office to see if there have been negative reports about the business.
- Look for testimonials from past employees.

If it sounds too good to be true... it probably is! Stay vigilant, and be sure to report any job scams you find to the FTC.

NOT ALL DEBT COLLECTORS ARE REAL

It is difficult to get through life without ever accruing any debt, and scammers know this. Some pose as fake debt collectors who claim to be calling about a debt you've forgotten about and are incredibly behind on repaying. They may threaten you with steep fines or even jail time if you don't pay this "debt" right away.

Don't let these fear tactics pressure you into making rash decisions with your money. If a debt collector calls, don't trust them if they:

- Want you to pay off a debt you don't recognize
- Are secretive about who they work for and refuse to give you a mailing address or phone number
- Make the situation sound urgent, including threatening to report you to law enforcement
- Swear at you or harass you

Knowing your rights can go a long way in keeping you safe from fake debt collectors. Legally, legitimate debt collectors must provide you:

- The name and mailing address of their agency
- The name of the creditor to whom you owe money
- How much money you owe, including any interest or fees
- Steps you can take if you don't think it's your debt
- Your debt collection rights

You might also want to search their company's name on the internet to confirm they are legitimate.

Once you get this "validation" information, you have 30 days to dispute the debt if you believe it's on your account in error.

Being told you have debt you forgot about can be alarming, but stay calm. You will always have time to validate the call and confirm if the debt is real or not.