FRAUD WATCH

STAY INFORMED. STAY PROTECTED.

MINNESOTA VALLEY
FEDERAL CREDIT UNION

FRAUD & SCAMS

By the Numbers

Americans lose

$10+ Billion

to fraud & scams each year.



That is only what's reported to the Federal Trade Commission. The actual annual number is likely ***much*** *higher.*

Just over **30%** of Americans are scammed each year, with **73%** having experienced an online scam ***at least once*** in their life.

THE MOST COSTLY SCAMS EACH YEAR:



Investment Scams

$6 billion lost



Imposter Scams

$3 billion lost

THE TOP PAYMENT METHODS FOR LOSS EACH YEAR:



Bank Transfers

$2 billion lost



Cryptocurrency

$1.5 billion lost

FRAUD & SCAMS

Differences

Your personal and financial information is a valuable commodity and protecting it is key to maintaining financial security. Being able to recognize the signs and understand the differences between fraud and scams is essential to keep your finances secure.

SCAM: A deliberate scheme designed to deceive people in order to steal money, personal information, or other assets.

FRAUD: When a person intentionally creates or uses a false impression in order to secure money, assets, services, or other financial advantages at another's expense.

Americans who have experienced a scam in their lifetime lost an average of **$2,647**

FAQs

What are the most common types of fraud?
Account takeovers, identity theft, credit card fraud, phishing emails, and even fake investments.

What kinds of scams should I watch for?
Peer-to-peer payment requests, fake sellers, tech support scams, impersonators, and romance scams. Only send money to people you know and double-check before you click anything.

How can I spot fraud before it happens?
Trust your instincts. If something feels rushed, strange, or too good to be true...STOP! Don't click on suspicious links.

What's the best way to protect my financial information?
Use strong passwords for every account and change them often. Keep account numbers and login details private. Use a password manager app like KeePass or LastPass.

Learn more at: https://reportfraud.ftc.gov/faq/

FRAUD & SCAMS

Protect Yourself

HANG UP. LOOK UP. CALL BACK. Scammers often pretend to be the credit union, a specific MVFCU department, or a vendor that works on our behalf. They may also pose as a retailer, a delivery company, or even law enforcement. They may sound convincing, know a few details about you, or create a sense of urgency.

HANG UP. If a call feels unexpected or pressured, end it. A legitimate organization will understand your concerns.
LOOK UP. Do your own search and find a trusted phone number yourself, such as the number on the back of your card, on your statement, or on our official website.
CALL BACK. Use that trusted phone number to confirm you're speaking with who the caller claims to be.

NEVER SHARE CODES. Do not share access codes, PINs, passwords, or security codes with anyone who contacts you.

As a reminder, MVFCU will never contact you by email, text, or phone to request personal information such as usernames, passwords, account numbers, or access codes. If a call or message appears to come from MVFCU — even if your Caller ID shows our name, it may be a spoofing scam. To stay safe, **never** click on links or share personal information.

Staying in control of your accounts and verifying who you're talking to are two of the simplest ways to protect yourself. If something ever doesn't feel quite right, turn your card off, hang up, and call us directly using the number on the back of your card or on our official website. We're always here to help.

HOW TO REPORT FRAUD

- Notify Us: Call (507) 387-3055 or report card fraud 24/7 at 1-800-234-5354.
- Document as much as you can.
- File a Report with the Federal Trade Commission at: **https://reportfraud.ftc.gov/assistant**
- Safeguard Your Credit

TIPS TO STAY SAFE

What To Do

Fraud happens FAST but a few small changes can make a big difference. These tips can help you catch fraud early and protect what you've worked so hard to build. Some of the easiest ways to help protect yourself:

1. **Use Strong Passwords:** Choose something only you would know. Mix letters, numbers, and symbols — and avoid using names or birthday. Example of a strong password: **Blu3R!v3rL@nD985**
2. **Watch for Scams:** If a text or email seems odd, don't click it. Scammers want you to panic — pause instead. When in doubt, call us: (507) 387-3055.
3. **Update Regularly:** Keep your phone and apps up to date. Updates fix known security problems that fraudsters look for.
4. **Use Private Networks:** Public Wi-Fi is not always safe. Wait until you're home or use your phone's data when banking.
5. **Check Activity:** Look at your account activity often. A quick peek now can save you stress and money later.
6. **Use Card Controls:** Turn your card off instantly if something doesn't look right. Your fast action can help stop fraud instantly.

What NOT To Do

1. **DON'T** use common passwords. If it is a word that can be found in the dictionary, do not use it.
2. **DON'T** use birth dates or names in passwords.
3. **DON'T** re-use passwords.
4. **DON'T** share passwords.
5. **DON'T** write passwords on a piece of paper near your desk.
6. **DON'T** have your files on your computer with passwords in plain text.
7. **DON'T** save your passwords in your browser.
8. **DON'T** use the same passwords for personal and professional use.

YOUR IDENTITY

Biggest Asset

Your identity is your biggest asset because your name, Social Security number and other personal financial information can help you get a job, be approved for a loan, rent an apartment, and open an account at a financial institution—among other things.

If a fraudster were to steal your identity, they could do all of those things, and more, using your name. The following is a list of documents with very sensitive identity information:

- Social Security card
- Birth certificate
- Driver's license
- Passport
- State ID
- Student ID
- Individual Taxpayer Identification Number (ITIN)

IDENTITY THEFT: When someone uses another individual's personal or financial information without their permissions, typically for economic gain.



Fraud is on the rise and we care about helping you protect your finances. Our staff has been trained to watch for red flags and unusual account activity. As a member, you have access to fraud alerts and account monitoring in your online banking app. If something doesn't feel right, please call us immediately. We are here to help keep your finances secure.

WARNING SIGNS

Clues of Identity Theft

How do fraudsters gain access to personal info?

They steal identities by collecting personal information through digital, physical, and sometimes social methods.

CLUES TO WATCH FOR:

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.
- If your wallet, Social Security number, or other personal information is lost or stolen, there are steps you can take to help protect yourself from identity theft.



You can file a report at:
https://www.identitytheft.gov/

STAY AWARE

Trust your instincts and check in often.
If you think you've been targeted,
contact us right away.

mnvalleyfcu.coop

(507) 387-3055

MINNESOTA VALLEY
FEDERAL CREDIT UNION

Greater Mankato's Community Credit Union Since 1934