MIDMINNESOTA FEDERAL CREDIT UNION
mmfcu.org

Fraud Warning Signs Checklist

Below you will find a list of **WARNING SIGNS** that a situation might be fraud, how to **PREVENT** fraud and some additional **RESOURCES** to help you navigate fraudulent situations.

Four Signs that it is a Scam:

Scammers PRETEND to be from an organization that you know - They will often pretend to be from an organization you are familiar with, including government agencies, utility companies, charities, and even your financial institution.

- Fraudsters have software that changes the number on your Caller ID and makes it look like it is from a trusted source, but it is not. MMFCU will never ask you for your account, social security, or credit/debit card numbers when we call you.

Scammers may say there is a PROBLEM or PRIZE - They say that you are in legal trouble, you owe money, your family member has had an emergency, or there is a virus on your computer.

Scammers PRESSURE you to act immediately - They want you to act before you have time to think. They will instruct you to not hang up so you cannot check out their story. If you do hang up, they will warn you to not tell anyone else about what is happening.

- They might threaten to arrest you, sue you, take away your drivers license or business license, or say that your computer will be corrupted.

Scammers tell you to PAY in a specific way - They will often insist that you can only pay by depositing to a bitcoin/cryptocurrency machine, doing a money wire, transferring funds in an online banking or mobile app, by purchasing gift cards, paying with gold, or paying in cash.

- Sometimes they will send you a check, cashier's check, or cash and then they find a reason that you need to send some or all the money back to them. (Checks that they send to you that you deposit are fraudulent, and will be returned and debited from your account, leaving you out the funds that you have sent to them).
- Scammers will coach you to explain the reason for your withdrawal/purchase with a made-up story or will instruct you to keep the transaction private from everyone.

How to Avoid a Scam:

Block unwanted calls and text messages

- Do not answer the phone if you don't recognize the phone number. If you do pick it up, hang up as quickly as possible.
- Do not click on any links within text messages, if you don't know who it is from or you were not expecting it.
- Text messages that come from an email address are typically fraud.

Do not give your personal or financial information in response to a request you did not expect

- Honest organizations will not ask you for your personal information if they initiated contact.
- If you think it is legitimate, hang up and look at a statement or invoice to verify their contact information before calling them back. Do not call the number from the Caller ID or the number they gave you. (This is true for websites they give you too).
- If you receive a phone call, and you are unsure, have a prepared statement ready. An example of a prepared statement would be *"I don't believe I owe any money. I will double check and give the main office a call back"* or *"This is not something I am interested in, but thank you for your time."*

Resist the pressure to act immediately

- Honest businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.

Know how scammers tell you to pay

- Never pay someone who insists on payment by cryptocurrency, wire transfers, a payment app, gift cards or gold. And never deposit a check and send it back to someone.

Stop and talk to someone you trust

- Before you do anything else, tell someone - a friend, family member, or neighbor - what happened. Talking about it could help you realize it is a scam.
- Staff at MMFCU may ask you questions about your transactions - the landscape of fraud is always changing, and they ask these questions to recognize red flags and prevent financial loss. If they do not ask, please initiate the conversation yourself if you are unsure. Employees are trained to identify most fraud and are happy to review your situation.

REV 04/2025

Additional Prevention Tips

Review Account Transactions - Try to do this as often as possible to identify any fraudulent or unauthorized transactions. Report anything that you did not authorize, even if it is for a small amount. Some unauthorized transactions must be reported within a certain amount of time, so it is best to report as soon as possible.

- **Sign up for Alerts & Notifications** - Personalize your alerts and sign up to be notified about any log ins to your Online Banking/Mobile App account by logging into your account, then go to Account Security and then:
  - Alert Settings, then Accounts - for general transaction alerts.
  - Credit and Debit Card Alerts & Controls then Alerts and Controls - for card transaction alerts.

Watch Your Credit - There are two options available:

- **SavvyMoney** is a service through MMFCU's Online Banking and Mobile App that allows you to monitor your credit score for free.
- **AnnualCreditReport.com** allows you to pull your credit report annually and watch for accounts opened in your name.

Place a Credit Fraud Alert - Fraud alerts require creditors to verify your identity before approving credit in your name. You can place a free one-year fraud alert by contacting one of the major credit bureaus listed in the Resource section at the end of this document.

Freeze Your Credit - A credit freeze will restrict creditors from accessing your credit report to open new credit accounts in your name. Contact one of the four major credit bureaus listed in the Resource section at the end of this document.

Keep Your Contact Information Up-To-Date - By keeping your information up-to-date, we will be able to reach you quickly in the event that we identify suspicious activity.

Create Strong Passwords - It is best to use a different password for every site, if possible. And, of course, never give out your password.

Setup Multifactor Authentication - If Multifactor Authentication is available, set it up. It requires the user to provide additional verification information.

Be Careful About What You Throw Away - Do not toss pre-approved credit card offers or documents with your personal information on them in the trash without shredding them. Mark MMFCU's annual Shred Days on your calendar.

DoNotCall.gov - Put your name on the Do Not Call registry. This will block unwanted telemarketing calls. Caution, this does not always block calls from fraudsters, but it will reduce the number of calls you receive.

Protect Your Wallet - Use a wallet or card sleeve that has RFID protection. RFID uses radio waves at a short distance to communicate with card readers. An RFID wallet disrupts the radio waves to protect against fraudsters using technology to gain information.

Protect Your Debit/Credit Card Number -

- Do not share your card number with anyone and be cautious of your surroundings when you have your card out of your wallet.
- Use the tap feature or a digital wallet when possible. Instead of using your card number, tap creates an encrypted message to communicate with your card company, meaning that your card number is not exposed.
- When using a machine to swipe your card, make sure there is not a device in place known as a skimmer that captures your card number and expiration date.
- If you have a tap card, using an RFID wallet or sleeve can help protect your card from a close encounter with a fraudster attempting to gain information.

Resources

Mid Minnesota Federal Credit Union

- Call us at (218) 829-0371
- Stop by your local office. Find them at mmfcu.org/locations
- Chat with us at mmfcu.org or within Online Banking
- Visit mmfcu.org/community for information on financial education, community events and our blogs
- Follow MMFCU on Facebook, Instagram and LinkedIn

Credit Bureaus:

- Equifax: 1-888-378-4329 or go to www.Equifax.com
- Experian: 1-888-397-3742 or go to www. Experian.com
- TransUnion: 1-800-916-8800 or go to www. transunion.com
- Innovis: 1-800-540-2505 or go to www.innovis.com

Federal Trade Commission:

- The FTC is the primary government agency that enforces, advocates, researches and educates fraud. "*Four Signs that it is a Scam*" and "*How to Avoid a Scam*" is courtesy of the FTC through their fraud education resources.
- Visit Consumer.FTC.gov/Consumer-Alerts for updates on the latest fraud.