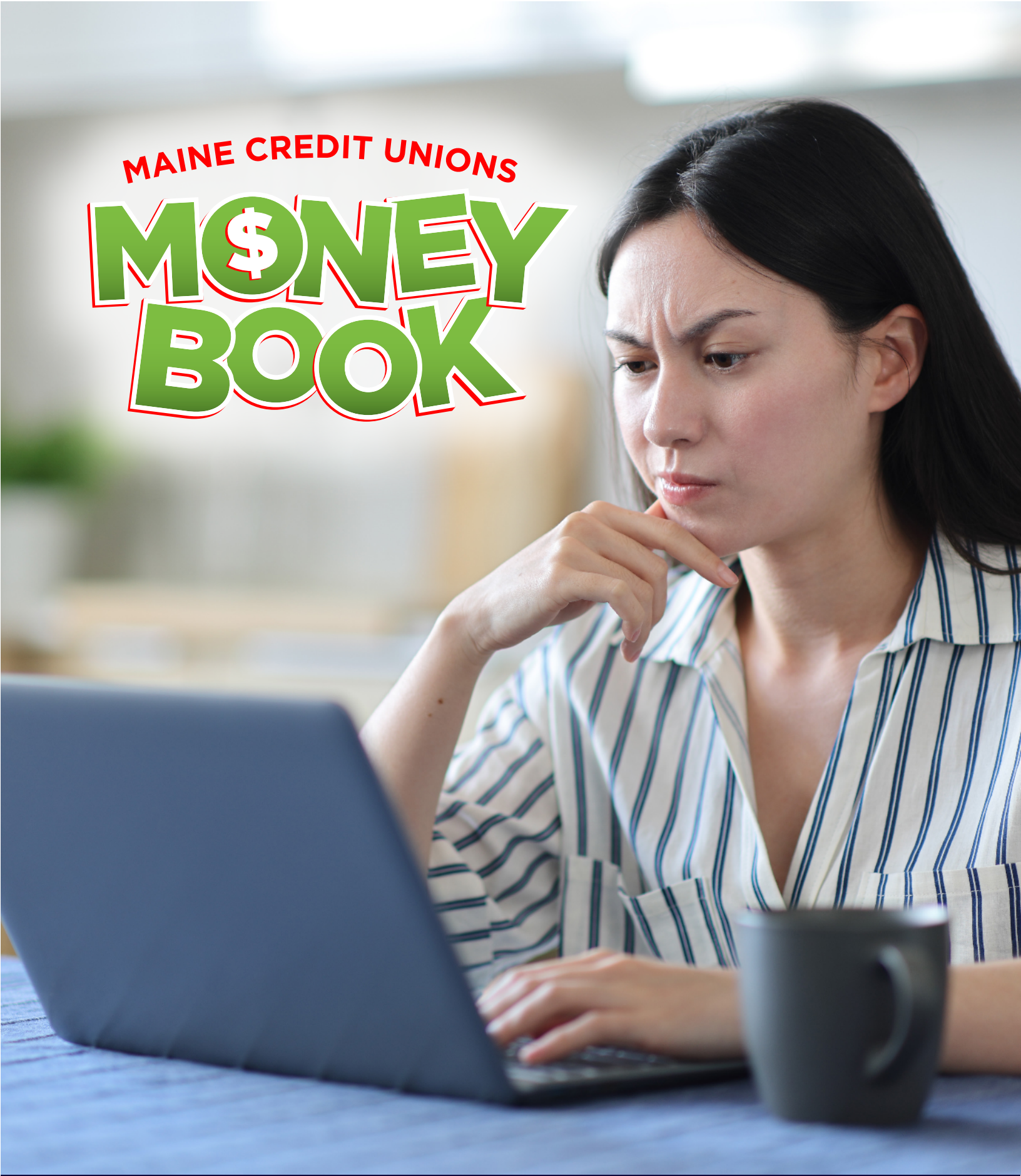
MAINE CREDIT UNIONS

MONEY BOOK



MAINE CREDIT UNIONS

PROTECTING YOUR ASSETS

What is Fraud? What are Scams?

An individual's 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 safeguarding oneself from having their hard-earned money taken away by scammers and fraudsters.

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 advantage(s) at another's expense.

What is the Difference Between Fraud and Scams?

A scam is financial theft with one's permission or knowledge. It's a trick that is designed to persuade people into believing false information or promises with the goal of gaining their money, personal information, or other valuables. Scammers often manipulate their victims by exploiting their trust. Examples of scams include people pretending to be debt collectors, offering fake investment opportunities, or promising fake lottery or prize winnings. For example, a scammer could mail, call, text, or email someone to tell them they've won a prize through a lottery or sweepstakes and then ask them to pay an upfront fee to receive the rest of the money. There is no prize. The scammer simply wanted quick payment from the victim.

Fraud is financial theft without one's permission or knowledge. Fraud refers to the deceptive and dishonest activities carried out with the intention of gaining financial or personal benefits—all while breaking the law. Examples of fraud include unauthorized use of someone's credit or debit card, stealing someone's identity and opening accounts in their name, and taking over an unsuspecting person's financial accounts. Fraud is more difficult to protect oneself from than scams, as it happens without people knowing about it.

Fraud and Scams - By the Numbers

Americans lose over

$10 billion

to fraud and scams annually.

That's only what is reported to the Federal Trade Commission each year! The actual 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 are:

Investment Scams

$6 billion

lost each year

Imposter Scams

$3 billion

lost each year

The top payment methods for loss are:

Bank Transfers

$2 billion

lost each year

Cryptocurrency

$1.5 billion

lost each year

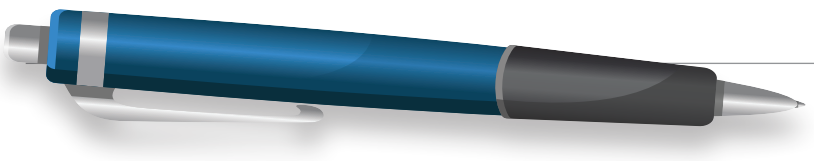
Americans who have experienced a scam in their lifetime lost an average of: **$2,647**

What Red Flags Do You Identify in Your Day-to-Day?

Most scam attempts exhibit red flags (warning signs) that people can identify to avoid falling victim. What red flags have you identified in the past to prevent you from being scammed?

On this page, list all the red flags of a scam you can think of.

After you create your list, the group will share answers aloud. If an example is shared that you didn't think of, add it to your list.

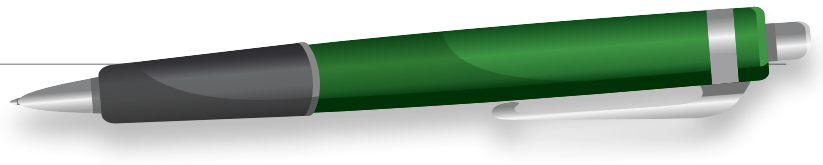


What Scams Are You Aware of?

Scammers are ever-evolving and deceptively clever in their attempts to obtain your money and personal information.

On this page, list all the types of scams you're aware of.

After you create your list, the group will share answers aloud. If an example is shared that you didn't think of, add it to your list.



What is Identity Theft?

Identity Theft: When someone uses another individual's personal or financial information without their permission, typically for economic gain.

When someone's identity is stolen, there is not only a threat to their finances, but there can also be other negative outcomes—including a loss of privacy and personal safety, strained relationships, reputational risks, administrative problems, and an emotional and psychological impact.

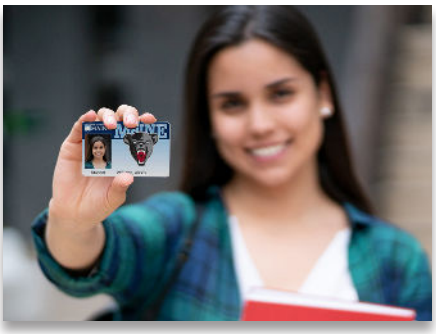
Why is Your Identity an Asset?

Your identity is an 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 many other things.

Alternatively, if a fraudster were to steal your identity, they could do all of those things and more in your name.

Documents with very sensitive identity information include:

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

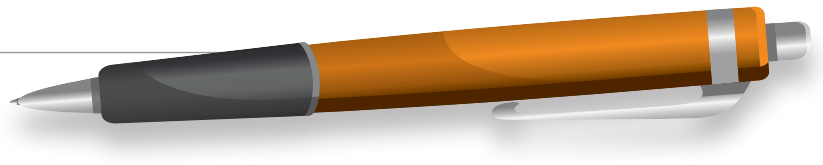


What Could a Fraudster Use or Reference to Impersonate Someone?

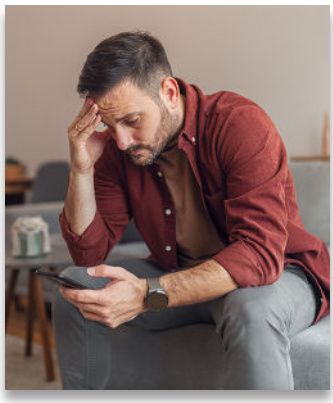
Understanding what information can be misused is the first step in protecting it. When people know which documents carry risk, they are better-equipped to safeguarding themselves and others.

On this page, list all the documents you can think of that a fraudster could use to gather personal information and potentially impersonate someone.

After you create your list, the group will share answers aloud. If an example is shared that you didn't think of, add it to your list.



How Could You be Harmed by Identity Theft?



Becoming a victim of identity theft can lead to financial loss, a damaged credit score, legal troubles, emotional distress, a loss of reputation, and more.

Below, please find what a fraudster using a stolen identity could do:

- Open up accounts in your name at financial institutions, including credit accounts like credit cards, personal loans, or other lines of credit.
- Access your financial accounts and steal your money.
- File a false tax return in your name, stealing your refund and reporting inaccurate information you will need to clear up.
- Use your identity to obtain prescriptions or medical treatments. This may result in medical providers billing you for services you did not receive.
- Rent property or obtain utilities using your name.
- Conduct social engineering scams where they pose as you to deceive your friends, family, or coworkers.
- Blackmail or extort you by leveraging sensitive or private information.

How Do Fraudsters Gain Access to Your Personal Information?

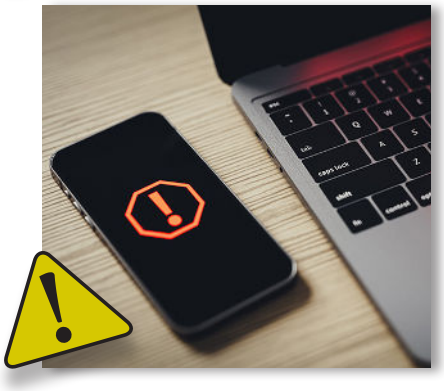
Fraudsters steal identities by collecting personal information through **data breaches, stolen mail, malware**, or **online exposure**, and then use that information to impersonate someone. One of the most common methods is **phishing**, where criminals send emails, texts, or phone calls that appear to come from legitimate organizations (like financial institutions, employers, or government agencies) to trick people into clicking malicious links or providing passwords, account numbers, or one-time passcodes. **Malware** can also be installed through infected attachments or websites, allowing fraudsters to log keystrokes, capture credentials, or access stored data on a device.

Another popular tactic is **social engineering**, which involves manipulating people rather than technology. Fraudsters exploit trust, urgency, fear, or authority—posing as coworkers, IT support, family members, or officials—to persuade victims to bypass security controls or share sensitive information. They often combine these techniques with publicly available data from social media or public records to sound convincing, then exploit weak passwords, reused credentials, or unsecured networks to take control of accounts and commit identity fraud.

What Are the Warning Signs of Identity Theft?

Financial & Credit Warning Signs

- Unexpected credit card charges or account withdrawals
- New accounts or loans you don't recognize on your credit report
- Being denied credit unexpectedly
- Bills or collection notices for accounts you never opened
- Sudden drops in your credit score without explanation
- Notifications of credit inquiries you didn't authorize
- Debt collectors calling you to pay unfamiliar debts



Account & Login Warning Signs

- Password reset emails you didn't request
- Being locked out of accounts due to changed credentials
- Login alerts from unfamiliar devices or locations
- Two-factor authentication codes you didn't initiate
- Account profile details (email, phone, address) changed without your knowledge

Personal & Administrative Red Flags

- Mail stops arriving or you receive mail for accounts you don't recognize
- Address change confirmations you didn't request
- Calls or letters from the IRS or tax authority about unfiled or duplicate tax returns

Medical & Insurance Warning Signs

- Bills for medical services or prescriptions you didn't receive
- Errors or unfamiliar entries in your medical records
- Insurance claims you didn't submit
- Explanations of benefits (EOBs) for unknown treatments

What Will a Financial Institution Never Contact You For?

Credit union employees are trained to detect fraud and scams.

It's important to remember that credit unions and other financial institutions won't call you and ask for:

- Online banking information
- Passwords or PINs
- Social Security numbers
- Mother's maiden name
- Address
- Phone number

Can You Identify the Red Flags and Warning Signs?

On these next two pages, you'll review some scenarios. Read each scenario and decide whether it's a scam attempt, a warning sign of identity theft, or a legitimate communication. If you feel it's a scam attempt or a warning sign of identity theft, identify the red flags that influenced your decision.

SCENARIO 1:

"ALERT: Your [Credit Union Name] account has been locked due to suspicious activity.

Click here immediately to verify your information:

http://secure-verify-cu-123.com Failure to act in **10 minutes** will result in permanent account closure."

This scenario is:

1. A scam attempt
2. An identity theft warning sign
3. Neither

What are the red flags, if any?

SCENARIO 2:

"[Insert name]

Your mailing address and email were successfully updated on your account.

If you did not make this change, contact customer support immediately."

You did not make any changes.

This scenario is:

1. A scam attempt
2. An identity theft warning sign
3. Neither

What are the red flags, if any?

SCENARIO 3:

Your [credit union name] accont statement is ready so click this link too view it:

http://y0urcredltunion-stat3ment.com

Due to recent secuirty issues you must log in immediately to avoid service interuption.

If you have any questions reply to this message directly for help.

This scenario is:

1. A scam attempt
2. An identity theft warning sign
3. Neither

What are the red flags, if any?

SCENARIO 4:

Your [credit union name] monthly account statement for September is now available.

To view your statement, please log in using your usual method (mobile app or by typing our website directly into your browser).

As a reminder, we will never ask for your password, full account number, or one-time security code by email or text.

If you have questions, contact us at the phone number listed on the back of your card or on our official website.

This scenario is:

1. A scam attempt
2. An identity theft warning sign
3. Neither

What are the red flags, if any?

SCENARIO 5:

"Grandma, it's me. I'm in trouble. I was in a car accident and I've been arrested. Please don't tell Mom and Dad—they'll freak out. The lawyer says I need **$4,000** right now. Can you go buy gift cards and read me the numbers on the back? Please hurry!"

This scenario is:

1. A scam attempt
2. An identity theft warning sign
3. Neither

What are the red flags, if any?

How Do You Limit the Threat of Falling Victim?

Understanding how to avoid scams and identity theft empowers people to protect their money, personal information, and peace of mind. When individuals are aware of common tactics used by criminals, as well as what documents contain sensitive information, they are better-equipped to spot suspicious activity and safeguard yourself.

Below, please find some things you can do limit the threat of falling victim:

- **Slow down before responding** to any unexpected call, text, or email. Scammers use urgency to cloud your judgment.
- **Never share one-time passcodes, PINs, or passwords** with anyone who contacts you. Legitimate institutions will not ask for these.
- **Type website addresses yourself** instead of clicking on links in communications.
- **Enable multi-factor authentication (MFA)** on banking, email, and other online accounts.
- **Use strong, unique passwords** for every account. Consider using a password manager to keep them secure.
- **Set up account alerts** (transaction alerts, login alerts, card-not-present alerts) so you know immediately if something is wrong.
- **Monitor your credit reports regularly** at AnnualCreditReport.com to spot unfamiliar accounts or inquiries.
- **Be cautious with public Wi-Fi.** Avoid logging in to financial accounts or entering sensitive information unless you're on a secure network.
- **Shred sensitive documents** before disposing of them (bank statements, insurance letters, tax documents).
- **Check sender details carefully**. Their email address, phone number, spelling, and tone can show red flags of scams.
- **Hang up and call back** using a trusted phone number (like the one on the back of your card) if something feels off.
- **Never pay with gift cards, wire transfers, cryptocurrency, or payment apps** for someone you don't know personally. These are popular among scammers, as they are more difficult to trace.
- **Keep software and devices updated** to protect against malware and security vulnerabilities.
- **Review your financial statements** regularly for unfamiliar charges. Report suspicious activity immediately.
- **Limit what you share on social media.** Scammers use personal details to guess security questions or impersonate you.
- **Freeze your credit** if you want maximum identity theft protection. It prevents new credit from being opened in your name.
- **Trust your instincts**. If something feels odd, rushed, or too good to be true, it's worth pausing to think things through.

How Do You Report Fraud and Scams?

Notify Your Credit Union or Credit Card issuer

If the fraud or scam involves your credit union account, credit card, or any other financial accounts, immediately contact the institution. Inform them about the fraudulent activity and follow their instructions on how to proceed.

Document the Details

Gather all relevant information, such as emails, phone numbers, messages, receipts, or other evidence related to the fraud or scam. This will be important information to have when you report the incident.

File Reports

In the United States, you can report fraud and scams to the **Federal Trade Commission (FTC)**, which collects data on deceitful activities to identity trends and patterns. You can file a report by visiting the **FTC's website** or by calling:

1-877-FTC-HELP
(1-877-382-4357).

Contact your local police department or law enforcement agency and file a report. Provide them with all the evidence you have gathered. Even if they might not be able to investigate every case, reporting the incident can help build a case against the scammer or fraudster by identifying patterns of criminal activity.

If your information was stolen, such as your Social Security number, credit card, account details, or other personally identifiable information, go to **IdentityTheft.gov.** On this website, you can report what happened, obtain a recovery plan, and receive guidance through each recovery step.

Safeguard Your Credit

If your personal information was compromised through fraud or a scam, contact the three major credit bureaus (Experian, TransUnion, and Equifax) to initiate fraud alerts and freeze your credit. By adding a fraud alert to your credit report, it will warn lenders that you may be a victim of fraud. This is an extra precaution and will let potential lenders know they should contact you before opening any new lines of credit in your name. You can also freeze your credit for free at each of the major credit bureaus. Freezing your credit prevents any new credit accounts from being opened in your name. Even if identity thieves have accessed all of your personal information in a data breach, they can't open new accounts in your name if your credit is frozen.

Common Red Flags of Scams

You Need to Act Fast

Acting in urgency is a warning sign of a scam. Scammers want you to act quickly and make payments without taking the time to think the situation through.

They're Using Fear Tactics

If someone threatens to arrest you, sue you, or subject you to any other consequences if you don't pay them, it's likely a scam. Scammers know that fear can lead to poor judgement.

Unusual Payment Methods Are Requested

If you are asked to send a payment via a wire transfer, prepaid card, or cryptocurrency, do not do it. These methods are nearly untraceable, and once the money is sent, it's usually gone for good.

Pre-payment is Requested

If someone offers you a prize or debt relief, if you have to pay an upfront fee or shipping costs in order to get it, it's most likely a scam.

They Want Your Personal Information

If you are contacted and asked to verify sensitive information over the phone, hang up. Never provide personally identifiable information like your birthday or Social Security number in response to an unsolicited call, email, or text message.

You Need to Keep It a Secret

If you are asked to keep a transaction a secret, it's likely because the scammer doesn't want you to share the situation with someone who might detect it as a scam.

Common Types of Scams

Lottery or Prize Scams: Never provide personal or financial information if you've been contacted about winning a prize, especially if you didn't enter to win one. Scammers may try to get you to pay an upfront fee or taxes before receiving the "prize," or they may ask for your account information—that way they can "deposit the money." This is likely a scam.

Imposter Scams: This is when a scammer pretends to be someone else, such as a government official, police officer, credit union or bank employee, friend, or family member—with the intention of obtaining your money or personal information. Always confirm the identity of the person contacting you. To avoid phone spoofing, hang up and call the person back directly. Your credit union won't call you for online banking information, passwords, Social Security numbers, addresses, phone numbers, or other private personal information.

Wire or Money Transfer Fraud: Never transfer money to someone you don't know. If you are asked to send a payment via a wire transfer, prepaid card, or cryptocurrency, do not do it. These methods are nearly untraceable, and once the money is sent, it's usually gone for good.

Check Scams: If you're selling something, do not accept a check for more than the requested amount. After the sale, scammers will ask you to send back the difference they "mistakenly" overpaid. The check will later bounce, and you've lost both the money and whatever item you sold.

Romance Scams: These are deceptive schemes where scammers create fake online personas, pretending to be potential romantic partners, to exploit individuals looking for love or companionship. After building emotional connections with their victims over time, they gain their trust and affection. Once that trust is established, they ask for money.

Charity Scams: Always verify that a charity is legitimate before donating. Check their website, look for reviews, and never donate if you're feeling pressured. You should also be suspicious if a charity asks you to make a donation via cash or wire transfer.

Debt Settlement or Relief Scams: Don't pay upfront fees to any company that guarantees the can settle or eliminate your debts. Scammers will promise to negotiate with creditors on your behalf to settle your debts for a fraction of the amount owed, or even wipe the debt out entirely. They charge an upfront fee but fail to deliver on their promise, leaving you in a worse financial situation and without any real debt relief.

Protecting Your Money Starts With People Who Care

Fraud is on the rise, but Maine Credit Unions are here to help you stay one step ahead. With trusted tools, clear guidance, and knowledgeable staff, credit unions across Maine are committed to protecting what matters most: you.

As a member, you have access to resources such as fraud alerts and account monitoring that help you recognize red flags, safeguard your personal information, and take action if something doesn't feel right. Maine credit unions help members avoid scams, protect their identities, and keep their money secure.

Visit www.mainecreditunions.org to learn more.

Presented By

Thank you!

Thank you for participating. We hope you found it educational, insightful, and even fun!

Do you want to learn more about money? Scan this QR to head to the Maine Credit Unions website, where you can learn more about finances and preparing for your future!

MAINE CREDIT UNIONS

mainecreditunions.org