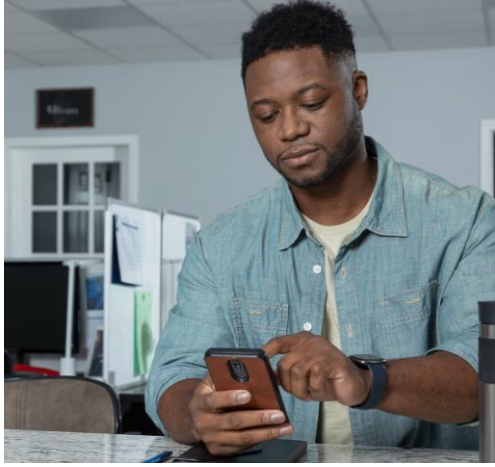
TruStage™

Protect your identity & money



Fraudsters continually find new ways to trick innocent people out of money or personal identifiable information. Whether it's an imposter scam – impersonating a credit union employee, a grandchild, debt collector, etc. – or stealing someone's identity, these fraudsters know how to pull it off.

Fraudsters will use several different social engineering techniques to acquire sensitive information such as usernames, passwords, and account or payment card details – all while trying to trick you into believing they are legit:

- Phishing (through email)
- Vishing (through phone calls)
- SMiShing (though SMS/text messages)
- Malware (malicious software)

Fraudsters will also spoof the credit union's contact info (phone number; email, etc.) to appear to be from the actual credit union.

Regardless of the fraud type or intention, fraudsters' first objective is to convince others that they are a real member. They often:

- Build victim profiles
- Change members' contact information
- Request wire transfers and withdraw funds
- Request canceled checks
- Order share drafts
- Request password resets
- Request credit/debit cards
- Set-up audio response or online banking
- Compromise login credentials including one-time-passcodes

Common warning signs

- Don't always trust the display name - criminals will spoof the email name to appear to be a legitimate sender
- Check for misspelled words, bad grammar, and/or typos within the content
- Be cautious of clicking links and opening attachments. Don't click unless you're confident of the sender or expect the attachment
- Asking you to share a one-time passcode sent to your device (when they called you)
- Check the salutation - many legitimate businesses will use a personal salutation
- Do not provide personal information when asked
- Be suspicious of urgent or immediate response needed or unauthorized login attempt of your account
- Don't believe everything you see. Brand logos, names and addresses may appear legitimate
- The recipient group seems random or unusual (e.g., all last names begin with the same letter)
- The email appears to be a reply to a message that you didn't actually send
- Monitor the sender's email address for suspicious URLs & domains – fraudsters often using similar letters and numbers
- If something seems suspicious; contact that source with a new email or phone call, rather than just hitting reply
- Always, be wary of tempting offers

Protecting yourself from fraud & scams

Recognizing scams can be difficult, especially after the impact of having personal information exposed following a data breach. But you can minimize the potential impact by knowing what to look for, taking the right action steps, and remaining vigilant.

Monitor your credit

- Check your credit report annually. Consumers are entitled to a free credit report from each of the three major credit bureaus annually. Simply go to AnnualCreditReport.com to get started. Items to watch for are "new" or "re-opened" accounts and other suspicious activity.
- A best practice is to check your credit report three times per year by requesting the report from one credit bureau every four months.

Watch for scams

- Be mindful of emails or phone requests claiming to be from a business or financial institution which was breached.
- Common member scams include those related to romance; secret shopper; advanced fee; relief; elder abuse; social security/government; and tech support.
- Avoid opening attachments and clicking on links contained in emails received from unfamiliar sources. Phishing emails often contain attachments or links to malicious websites infected with malware.
- Avoid clicking on links or calling the telephone number contained within text messages received from unfamiliar sources. Be wary of SMiSHing attacks which are like phishing but in SMS text messages.
- To avoid tax identify fraud make a point of filing annual tax returns promptly.

  Should you be notified that more than one return was filed in your name, owe additional tax, or that records indicate that your earnings were more than the amount of wage reported, complete an IRS Identity Theft Affidavit form 14039, and contact the IRS Identity Protection Specialized Unit at 800.908.4490.
- Check with the credit union to determine if account protections such as security challenge pass-phrase, account notes, and travel protections are available.
- In general, be wary of offers that are too good to be true, require fast action, or instill a sense of fear.

Your Social Security Number (SSN) is a prized possession

- Your Social Security Number (SSN) should be closely guarded – it doesn't change which makes it the ultimate prize for an identity thief. If your credit union uses your whole or part of your SSN to identify you, ask if they can use something else like an account password or recent transaction.
- Keep in mind, you may have to share your SSN if you're opening a new account or applying for a loan or credit card; but you should only share that information when you're certain it will not be overheard or used without your consent.
- Know the IRS or Social Security Administration will not contact you by phone, email, text or social media.

Protecting yourself online

- Use strong passwords that are at least 11 characters in length that are case-sensitive and include alpha-numeric characters and at least one symbol. Use a password checker to ensure you're using a strong password.
- Do not use the same password for multiple websites used to conduct online transactions.
- Be sure your home computer is protected with a firewall and antivirus/anti-malware software. A best practice is to configure the antivirus/anti-malware software to automatically check for updates at least weekly.
- Install operating system patches when they are made available.
- Avoid using public Wi-Fi and public computers (e.g., those found in libraries and hotel lobbies) to conduct online transactions. The use of a VPN can make public Wi-Fi more secure.
- When offered, use multifactor authentication for account logins or out-of-band authentication to confirm login attempts and/or transactions.

  Multifactor authentication uses more than one authentication method, such as user password (something you know) and a one-time-password token (something you have), or biometrics (something you are).

  Out-of-band authentication typically involves the user receiving a passcode via text message which the user must enter to complete a login or a transaction.
- Be wary of what you're sharing - openly sharing information on social media can provide an identity thief with the necessary information to impersonate you or answer certain challenge questions. Keep social media accounts private and be cautious who you're connecting with.
- Be wary of offers that appear too good to be true, require fast action, or instill a sense of fear.
- Never share anything related to your credit union account, transactional history, or identifying information in unprotected public forums.

27 million

American consumers were victimized by identity fraud-related financial losses

Source: Javelin 2022 Identity Fraud Study "The Virtual Battleground"

Protecting yourself following a breach

Data breaches pose a potential risk to consumers in the form of identity theft, account takeover, and fraud when personal and sensitive information is compromised.

Credit reports

If any portion of your member's Social Security Number was compromised, you should consider ordering a credit report and closely review it.

Consider placing a security freeze on your credit report with each credit bureau - Equifax, Experian, TransUnion, and Innovis. A security freeze, also referred to as credit freeze, protects you by restricting access to the credit report. During a freeze, the credit union, along with other financial institutions or lenders, are blocked from ordering the member's credit report unless a pre-set PIN is provided to lift the freeze.

You will have to allow for extra time for a loan or credit approval after placing a freeze. In some states, the credit bureau charges a fee to freeze, temporarily thaw, and/or unfreeze a credit report.

Fraud alerts

Request a fraud alert be placed on your credit report if you were a victim of identity theft. When a financial institution or lender pulls a credit report containing a fraud alert, they are required to call the phone number contained in the alert or use other reasonable means to verify it was actually the member that applied for an account or loan.

An initial fraud alert remains on your credit report for 90 days and must be renewed while an extended fraud alert remains on the credit report for seven years. You can contact one of the credit bureaus to have a fraud alert placed on your credit report and that credit bureau is required to notify the other bureaus.

Military personnel on active duty can place an active-duty alert on their credit report following the same process.

Online login or password information

If any of your online login or password information was compromised, you should:

- Log in to the member account as soon as possible and change the login and password.
- Make changes to accounts that use the same logins and passwords for multiple sites.
- Use strong passwords that are at least 11 characters in length that are case-sensitive and include alpha-numeric characters and at least one symbol.
- Use a password checker to ensure you have implemented a strong password.

Debit or credit card information

If your debit or credit card information was compromised:

- Call the credit union and request the old card to be canceled and request a new one.
- Review account activity and report any unauthorized transactions on a timely basis

Credit union account information

- If credit union account information was compromised; review account activity and report any unauthorized transactions.
- Consider closing the account and request a new one; but be mindful of potential delays and interruptions to any automatic payments or deductions.

Protecting your children and minors

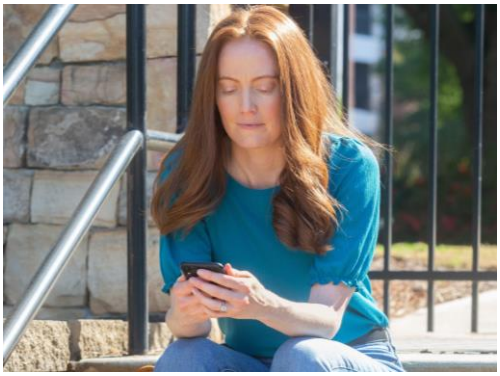
Most minors under the age 18 may not have a credit report available for review. However, children are regular targets of identity theft, and parents should take care to protect their children's financial future.

Warning signs

- Collection notices or calls products or services in your child's name.
- Notice declaring your child owes back income tax, or that their identifying information was used on multiple tax returns.
- Offers for pre-approved credit in your child's name. Marketing offers arriving in your child's name could be a sign that an account was opened at a financial institution).
- Be careful about sharing your child's private identifying information especially Social Security Number. If asked to share that information, ask and understand how it will be used.

Check your child's credit

- Contact each of the three nationwide credit reporting bureaus – Equifax, Experian, and TransUnion - and request a credit report in your child's name. Each has their own process, and it will take time, but it will be worth it.
- If there is a credit report in your child's name, request a fraud alert, and consider placing a credit freeze.
- Contact your local law enforcement or Attorney General's Office to file to report the identity theft and request a copy of any report generated.
- Contact any financial institution and business listed on your child's credit report and explain the account was opened because of theft and request it be closed. You may need to produce documentation from the credit bureaus and law enforcement.
- Keep a detailed list of any phone calls made and/or documents received as you may need to produce them later.



Looking for additional insights?

- Fraud.org
- FBI Internet Crime Complaint Center (IC3)
- Consumer.gov: Scams & Identity Theft
- Stop. Think. Connect.