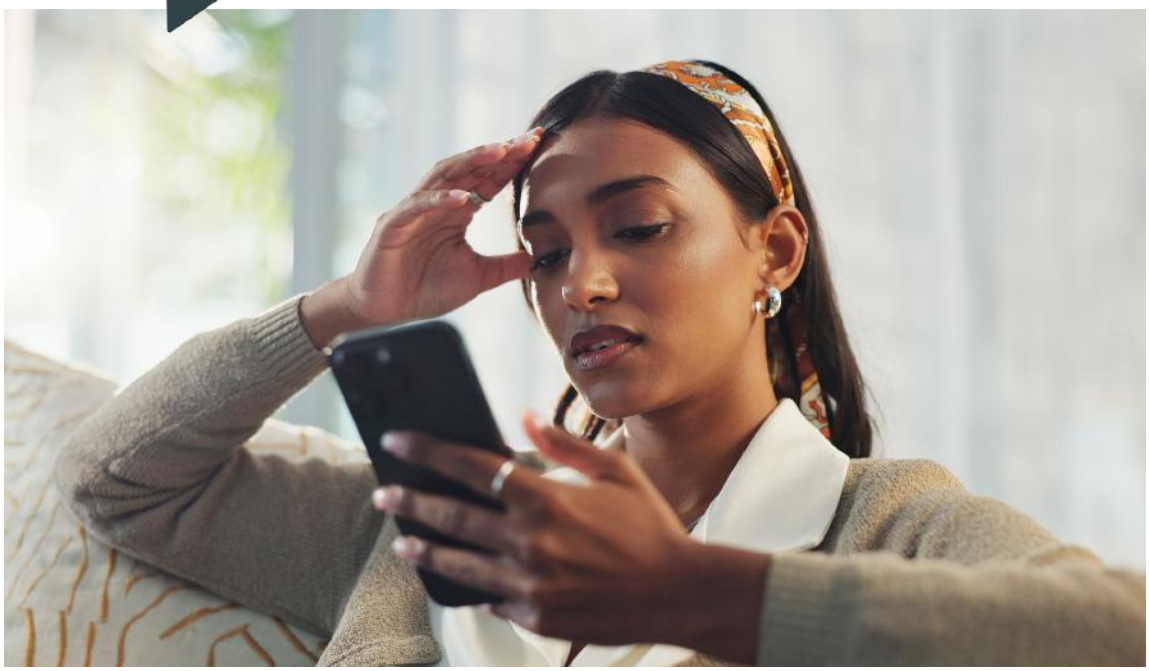
Protect Yourself Against Fraud & Scams!



RiverFall
CREDIT UNION

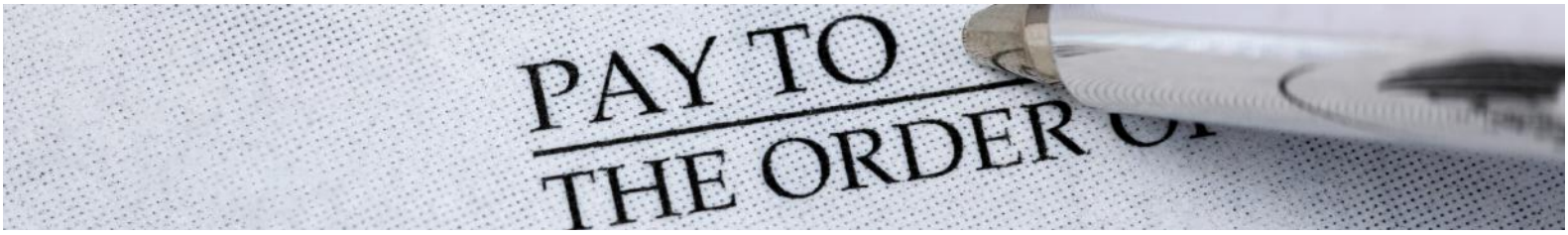
EQUAL HOUSING OPPORTUNITY

NCUA

riverfallcu.com
205.759.1505

Common Types of Fraud & Scams:

- **Financial Institution Imposter Fraud-** The perpetrator calls the victim pretending to be an employee from the fraud department of the victim's financial institution. The individual advises the victim to verify transactions on their account. Once confirmed as fraud, the victim is asked to go to a branch and withdraw cash to deposit into an ATM at another financial institution. Once this step is completed, the funds are not recoverable.



- **Check Fraud-** Refers to various illegal activities involving the manipulation, alteration, or forgery of check(s) to obtain money or goods dishonestly. It can take several forms including:
    - **Forgery-** Signing someone else's name on a check without permission.
    - **Alteration-** Changing the amount or payee on a legitimate check to benefit the fraudster.
    - **Counterfeit Checks-** Creating fake checks that appear legitimate, often using sophisticated printing techniques.
    - **Check Kiting-** Writing a check on an account with insufficient funds and covering it with another check from a different account before the first check clears.
    - **Stolen Checks-** Using checks that have been stolen from someone's mailbox or personal belongings.

Check fraud can lead to significant financial losses for individuals, businesses, and financial institutions, prompting the implementation of various security measures to prevent it.

- **Account Takeover-** Type of fraud where a criminal gains unauthorized access to an individual's online account. This can happen through various methods, including:
    - **Phishing-** Fraudsters send emails or messages that trick users into providing their login credentials.
    - **Credential Stuffing-** Attackers use stolen usernames and passwords from one site to gain access to accounts on other sites, especially if users reuse passwords.
    - **Social Engineering-** Manipulating individuals into divulging personal information that can be used to access their accounts.
    - **Malware-** Installing malicious software on a victim's device to capture login details.

Once an account is compromised, the attacker can make unauthorized transactions, change passwords, or steal sensitive information. This can result in financial losses, identity theft, and significant disruption to the victim. To mitigate the risk, it's essential to use strong, unique passwords, enable two-factor authentication, and monitor accounts regularly for suspicious activity.

- **Remote Deposit Fraud-** This involves criminals tricking people into depositing fake checks into their account via mobile app. Scammers will use a variety of tactics to manipulate victims including social engineering, impersonation, etc. Scammers will exploit the time it takes for financial institutions to verify checks allowing them to receive the funds before the financial institution discovers fraud.

- **Elder Financial Exploitation-** Specifically involves the unauthorized use of an elderly person's financial resources. This can occur through:
    - **Fraud-** Deceiving older adults into giving away money or personal information.
    - **Scams-** Targeting seniors with schemes like fake lotteries, prize promotions, or phishing emails.
    - **Misuse of Power of Attorney-** Abusing the authority granted to manage an elder's finances for personal gain.
    - **Coercion-** Pressuring an elder to change wills or financial documents against their wishes.

Both elder abuse and financial exploitation can have severe emotional, physical, and financial consequences for the victim. It is essential to recognize the signs and report any suspected cases to protect vulnerable older adults.

- **ACH Fraud-** Perpetrators initiate fraudulent transactions that divert funds from legitimate accounts. The scammer will often use a variety of tactics such as account takeover, phishing, malware, or social engineering to compromise sensitive information and setup fraudulent payments.

- **Money Mule-** A person who, often unknowingly, helps facilitate the transfer of illegally obtained money. Criminal organizations typically recruit money mules to move funds through various methods, creating a layer of anonymity for the criminals. Here's how it usually works:
    - **Recruitment-** Money mules are often targeted through job ads, social media, or even direct messages, offering seemingly legitimate work-from-home opportunities or high-paying jobs with little effort.
    - **Transfer of Funds-** Once recruited, money mules receive money in their bank accounts (often from scams or fraud). They are instructed to withdraw the funds and send them to another account, often keeping a portion as "payment."

- **Types of Scams-** The funds moved by money mules typically come from various fraudulent schemes, such as romance scams, lottery scams, or business email compromise.

- **Legal Consequences-** While some money mules may be unaware that they're participating in illegal activities, they can still face serious legal repercussions, including criminal charges and financial liability.

To protect against becoming a money mule, individuals should be cautious of unsolicited job offers, verify the legitimacy of companies, and avoid sharing personal banking information.

- **Spoofing-** When someone disguises an email address, sender name, phone number, or website URL – often just by changing one letter, number, or symbol – to convince you that you are interacting with a trusted source.

- **Phishing-** Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving personal information to criminals. You may receive an email that appears to be from a legitimate business, asking you to update or verify your personal information by visiting their website or replying to the email. The URL might look like one you have seen before, and the email is designed to be convincing enough to get you to take the action that is being requested. Once that link is clicked, you are sent to a website that might look identical to the real one (your financial institution or credit card site) and asked to enter in sensitive information. Phishing is designed and used solely to steal your information.

- **Romance Scams-** Fraudulent schemes in which a scammer pretends to be a potential romantic partner to exploit victims emotionally and financially. Here's how they typically work:
    - **Online Interaction-** Scammers create fake profiles on dating sites or social media, often using stolen photos and fabricated identities to appear attractive and trustworthy.
    - **Building Trust-** They engage in conversation, building emotional connections and trust over time. This often involves sharing fake personal stories and expressing deep feelings for the victim.
    - **Isolation Tactics-** Scammers may attempt to isolate their victims from friends and family, encouraging them to rely solely on the scammer for emotional support.
    - **Requests for Money-** After establishing a bond, the scammer will invent a crisis or urgent need for money, such as medical emergencies, travel expenses, or legal issues. They often ask for money to be sent via wire transfer or prepaid gift cards, as these methods are harder to trace.
    - **Continued Exploitation-** Once the victim sends money, the scammer may continue to create new emergencies to extract more funds, often leading to significant financial loss for the victim.

- **Warning Signs of Romance Scams:**

    - Quick declarations of love or intense emotions.
    - Requests for money or personal information.
    - Inconsistent or vague details about their life.
    - Avoidance of in-person meetings or video calls.

To protect against romance scams, it's important to be cautious when interacting online, conduct background checks on potential partners, and consult friends or family before sending money.

Tips to Protect Yourself:

- Never give out your account information, including usernames, passwords, verification codes, and card numbers. We will never call you and ask for this information.
- Never give out personal information, such as your Social Security Number, unless you know who you are dealing with.
- Never purchase gift cards in which you provide the number to others.
- Be cautious about who you communicate with through digital means (phone, email, etc.).
- Do not accept funds from people you don't know.
- Do not reply/respond to or click on links within unknown or unrequested messages.
- If you didn't initiate contact, go directly to the company, organization, or person to verify.

What to do if You Have Been Scammed?

If you feel like you have been a target or victim, contact RiverFall Credit Union immediately.

- If your debit card is compromised, we will issue a new one.
- If your online banking credentials have been compromised, we can assist you.
- To protect you and your funds, we may need to issue you a new member number.

If your personal information has been compromised, take the following steps now:

- Add freezes to your credit report to help prevent identity theft or fictitious loans:
  - **TransUnion-** 888-909-8872
  - **Experian-** 888-397-3742
  - **Equifax-** 888-298-0045
- Monitor your credit report regularly to ensure nothing fraudulent has been added.
- Consider filing a police report with local law enforcement.

If you have confirmed identity theft, contact the following offices:

- **Federal Trade Commission (FTC) Identity Hotline:**
  877-438-4338
- **Alabama Attorney General's Office:**
  800-392-5658

- Most importantly, stop communicating with individuals you don't know or who seem suspicious. They likely are not who they say they are and may not even reside in the country they say they do. If you are unsure, please contact us.
- Fraudsters may use many tools to gain your information and trust. You can be contacted by phone, text, email, mail, and social media messages. Scams may involve a variety of products and services, including checks, debit cards, gift cards, wire transfers, cryptocurrency, external transfers, etc. If you are asked to purchase any of these, don't.

If you think this will never happen to you, or you can't believe you fell victim to a scam, you are not alone!

- According to the Federal Trade Commission (FTC), one in four people reported losing money to a scam in 2023. A total of 298,878 scams were reported overall, resulting in a loss of approximately $19 billion for the year.
- Sometimes this results from being too friendly or nice to people online, or you may be targeted through no fault of your own.
- Even if you don't incur a financial loss, your actions could help criminals defraud others or fund other illegal activities. If you are unsure about what is being requested, stop communicating and contact RiverFall Credit Union, law enforcement, or the stated organization directly to confirm.

For More Information:

Visit mycreditunion.gov for more financial resource information and more about fraud prevention.

RiverFall
CREDIT UNION