# Financial Scams to avoid

**Power of Attorney Fraud.**
The perpetrator obtains a "Limited or Special Power of Attorney", which specifies that legal rights are given to manage the funds in your account. Once the rights are given, the perpetrator uses your funds for personal gain.

**Pigeon Drop**
The victim puts up "good faith" money in the false hope of sharing the proceeds of an apparently large sum of cash or item(s) of worth which are "found" in the presence of the victim.

**Financial Institution Examiner Fraud**
The victim believes that he or she is assisting authorities to gain evidence leading to the apprehension of a financial institution employee or examiner that is committing a crime. The victim is asked to provide cash to bait the crooked employee. The cash is then seized as evidence by the "authorities" to be returned to the victim after the case.

**Inheritance Scams**
Victims receive mail from an "estate locator" or "research specialist" purporting an unclaimed inheritance, refund or escheatment. The victim is lured into sending a fee to receive information about how to obtain the purported asset.

**Fake Prizes**
A perpetrator claims the victim has won a nonexistent prize and either asks the person to send a check to pay the taxes or obtains the credit card or checking account number to pay for shipping and handling charges.

**Internet Sales or Online Auction Fraud**
The perpetrator agrees to buy an item for sale over the Internet or in an online auction. The seller is told that he or she will be sent an official check (e.g., cashier's check) via overnight mail. When the check arrives, it is several hundred or thousand dollars more than the agreed-upon selling price. The seller is instructed to deposit the check and refund the overpayment. The official check is later returned as a counterfeit but the refund has already been sent. The seller is left with a loss, potentially of both the merchandise and the refund.

**Government Grant Scams**
Victims are called with the claim that the government has chosen their family to receive a grant. In order to receive the money, victims must provide their checking account number and/or other personal information. The perpetrator may electronically debit the victim's account for a processing fee, but the grant money is never received.

**Spoofing**
An unauthorized website mimics a legitimate website for the purpose of deceiving consumers. Consumers are lured to the site and asked to log in, thereby providing the perpetrator with authentication information that the perpetrator can use at the victim's legitimate financial institution's website to perform unauthorized transactions.

**Phishing, Vishing, or Smishing**
Technology or social engineering is used to entice victims to supply personal information (i.e., account numbers, login IDs, passwords, and other verifiable information) that can then be exploited for fraudulent purposes, including identity theft. These scams are most often perpetrated through mass e-mails, spoofed websites, phone calls or text messages.

**Information provided by Eagle Federal Credit Union**

To report a crime or fraud, file a report with your local police department. You may also file a report with your state's Consumer Protection Office. For additional information and reporting links, visit https://www.usa.gov/stop-scams-frauds.