Northeast Family Federal Credit Union

TYPES OF FINANCIAL SCAMS. Although this is not an exhaustive list, this is a list of popular scams worldwide.

(A) **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 the account. Once the rights are given, the perpetrator uses the funds for personal gain.

(B) **Advance Fee Fraud or "419" Fraud.** Named after the relevant section of the Nigerian Criminal Code, this fraud involves a multitude of schemes and scams – mail, e-mail, fax and telephone promises that the victims will receive a percentage for their assistance in the scheme proposed in the correspondence.

(C) **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.

(D) **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.

(E) **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.

(F) **Financial Institution Employee Fraud.** The perpetrator calls the victim pretending to be a security officer from the victim's financial institution. The perpetrator advises the victim that there is a system problem or internal investigation being conducted. The victim is asked to provide his or her Social Security number for "verification purposes" before the conversation continues. The number is then used for identity theft or other illegal activity.

(G) **International Lottery Fraud.** Scam operators, often based in Canada, use telephone and direct mail to notify victims that they have won a lottery. To show good faith, the perpetrator may send the victims a check. The victim is then instructed to deposit the check and immediately send (via wire) the money back to the lottery committee. The perpetrator will create a "sense of urgency," compelling the victim to send the money

before the check, which is counterfeit, is returned. The victim is typically instructed to pay taxes, attorney's fees, and exchange rate differences in order to receive the rest of the prize. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

(H) **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.

(I) **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.

(J) **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.

(K) **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.

(L) **Phishing/Vishing/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.

(M) **Stop Foreclosure Scam.** The perpetrator claims to be able to instantly stop foreclosure proceedings on the victim's real property. The scam often involves the victim deeding the property to the perpetrator who says that the victim will be allowed to rent the property until some predetermined future date when the victim's credit will have been repaired, and the property will be deeded back to the victim without cost. Alternatively, the perpetrator may offer the victim a loan to bridge his or her delinquent payments, perhaps even with cash back. Once the paperwork is reviewed, the victim finds that his or her property was deeded to the perpetrator. A new loan may have been taken out with an inflated property value with cash back to the perpetrator, who now owns the property. The property very quickly falls back into foreclosure and the victim/tenant is evicted.