Miscellaneous Types of Financial Fraud

Misappropriation of income or assets - A perpetrator, often a family member or caregiver, obtains access to Social Security checks, pension payments, checking or savings account, credit card or ATM, or withholds portions of checks cashed for the victim.

Fictitious relative - The perpetrator calls the victim pretending to be a relative in distress and in need of cash and asks that money be transferred either into a financial institution account or wired.

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.

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.

Power of Attorney fraud - The perpetrator requests a Limited or Special Power of Attorney, specifying that legal rights are given to manage funds assigned for investment to the perpetrator, a trustee, an attorney, an asset manager, or other title that sounds official and trustworthy. Once the rights are given, the perpetrator uses the funds for personal gain.

Advance fee fraud or "419" fraud - Named after the relevant section of the Nigerian Criminal Code, this fraud is a popular crime with West African organized criminal networks. There are a myriad of schemes and scams—mail, email, fax and telephone promises are designed to facilitate victims' parting with money, ostensibly to bribe government officials involved in the illegal conveyance of millions outside the country. Victims are to receive a percentage for their assistance.

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

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.

Telemarketing scams - The victim is persuaded to buy a valueless or nonexistent product, donate to a bogus charity or invest in a fictitious enterprise.

Internet sales or online auction fraud - The perpetrator agrees to buy an item available for sale on the Internet or in an online auction. The seller is told that he or she will be sent an official check (e.g., cashiers 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 subsequently 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.

Pharming - A malicious Web redirect sends users to a criminal's spoofed site even though the user entered a valid URL in the browser's address bar. This redirection usually involves worms and Trojans or other technologies that attack the browser address bar and exploit vulnerabilities in the operating systems and Domain Name Servers (DNS) of the compromised computers.

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 is now the property owner. The property very quickly falls back into foreclosure and the victim, now tenant, is evicted.

Small Business Grant Scams - The very small business person is often the least educated regarding how to apply for, submit or obtain a grant. A grant is frequently the best type of financing since it is a gift that doesn't have to be repaid, as does a loan. It doesn't take much marketing to sell a very small business person on applying for a guaranteed grant to help with a business expansion or upgrade.

Unfortunately, scam artists pray on these vulnerable small business people by seeming to promise the guarantee of securing a large grant.

How does it work?

A small business wants to expand but is unable to borrow enough money to do so.

They hear about a grant assistance company or are contacted directly by one.

They pay an up-front fee, usually several thousand dollars, to the grant assistance company and are verbally promised a large-dollar grant that doesn't have to be repaid.

Shortly after signing the grant assistance agreement, the business person is advised that he'll be much more successful in obtaining a grant if he restructures his business from a for-profit entity to a non-profit entity for an additional up-front fee, again usually several thousand dollars.

The small business person soon finds out that there is no guaranteed grant coming his way. His paperwork has merely been prepared and forwarded to various grant providers.

How can you protect yourself?

Get everything in writing.
Do not sign a contract without reading it first.
Check to see if the company is licensed with the appropriate local or state agency.
Check the company out with the Better Business Bureau.
Google the company's name for complaints.
Be cautious if you are asked to provide more money for services you have not yet received.

For more information on grants, visit http://www.grants.gov/help/general_faqs.jsp#12.

Source: Nevada Consumer Affairs Division and http://www.grants.gov.