

## Elderly Citizens Fraud on the Rise

We need to continue our awareness campaigns to protect our elderly population. More and more of our elderly citizens are adapting to all the newest technologies, but some are still unaware of the dangers they possess. People tend to forget that criminals are not only lurking on the Internet, but they will do or say whatever is necessary to get your information. Our older citizens need to become aware of the different methods that criminals use to commit Identity theft, and how different frauds keep evolving.

Ask yourself a question, who has my personal information: Perhaps it is your elementary school, high school, first place of employment, second, third or fourth employer, your doctor(s), your lawyer, credit card company, finance company, bank, or State and Federal Government, such as DMV.

Think about all the common sources of where you store your identity and what are you storing there.

We keep personal information in our wallet/purse, home, computer, business, online, in our vehicle, in public, in data storage areas of other businesses. You need to eliminate or control the amount of information accessible, and reduce the potential for someone with the wrong intentions of using your information.

Case studies:

- A customer sent a check for special eye glasses overseas which he never received. Shortly thereafter his bank started receiving requests to wire money out of his account.
- The customer was called shortly after she answered a pop-up ad on her computer by a person purporting to be from Publishers Clearing House to inform her that she was a million dollar winner and requested her banking information for a direct deposit.
- A customer was contacted by someone pretending to be from the Social Security Administration telling the customer that they needed to make changes to her direct deposit.
- A customer recently brought in a check which she deposited. The check was accompanied by a letter stating she had won the lottery. She was to deposit the check and transmit most of it through Western Union to a person to pay the taxes on her winnings.
- I received e-mails stating that I owed back taxes and I need to click on a link to get my case information.

Customers have received checks to become Mystery Shoppers. They are given forms and the ethics code of conduct information. They are asked to spend small amounts at well-known stores and evaluate them on customer service. Then one of the places they are to evaluate is a business that can send Western Union or Money Gram type instruments; but they are to send \$2,500.00 from the \$2,900.00 check that they were to deposit into their account.

What do all these cases have in common? They are all elderly citizens.

We need to learn a new word "NO."

No, I don't want it.

No, I will not give you that.

No, I don't care what you want to give me for free.

We need to give out as little information about ourselves as necessary.

Things to do to protect your information, especially your Social Security Number:

1. Eliminate the source of unnecessary information; cancel accounts so organizations cannot lose your information and get off the mailing lists using [www.optOutPerScreen.com](http://www.optOutPerScreen.com) and "Do Not Call" registry [www.DoNotCall.gov](http://www.DoNotCall.gov). Carry as little information as possible in your wallet or purse.
2. If the information has served its purpose, destroy it.
3. Secure your computer system with virus protection, anti-spyware and strong passwords.
4. Develop a risk rating system for your own personal information. Anything that you rate has high risk, lock it up.
5. Ask questions when people ask for your information. Why do they need that? Should I give that piece of information? Everyone should be on a need to know basis. What do I carry that can hurt me if it is lost or stolen?
6. Be you own Private Eye; incorporate the same private detective type tools to monitor the signs of someone trying to access your information. For example: ID theft monitoring companies, credit report monitoring with financial alerts, and balance your check book weekly.
7. Use strong computer passwords which contain upper and lower case letters, alpha numeric characters, symbols and change it often. Avoid using the same password for all your accounts.

What to do if you're a victim:

1. Close the affected account.
2. Place an initial fraud alert with your credit reports companies (Equifax 1-800-525-6285; Experian 1-888-397-3742 and/or TransUnion Corp. 1-800-680-7289)
3. Contact the agency that issued the identification, driver's license, or government ID, if necessary.
4. File a police report in the community where the ID theft took place.
5. Watch for signs that your information is being misused.

Where do you go if you have a question that may affect your banking or credit? Contact the branch manager or the security department of your bank.

**We also need to alert our elderly citizens and their families of the possibility of their loved ones being exploited for financial gain:**

Financial Exploitation: Theft, fraud, misuse or neglect of authority, and use of influence as a lever to gain control over an older person's money or property.

***Warning Signs:***

Sudden changes in finances and accounts, altered wills and trusts, unusual bank withdraws, checks written as loans or gifts and loss of property.

***What to do:***

Report abuse to a local adult protective service agency or law enforcement; contact the National Center on Elderly Abuse at [www.ncea.aoa.gov](http://www.ncea.aoa.gov).

Keep in contact; maintaining communication will help decrease isolation, a risk factor for mistreatment.

Be aware of possibility of abuse. Take note to what may be happening to your older neighbors and relatives; do they seem to be sad, nervous or fearful, especially around certain people.

Contact your local area agency on aging to identify programs and resources.

Volunteer; there may be local opportunities to become involved with your elderly population.

Additional information can be obtained at:

[www.ncea.aoa.gov](http://www.ncea.aoa.gov)

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

[www.fbi.gov/scams-safety/fraud/internet\\_fraud](http://www.fbi.gov/scams-safety/fraud/internet_fraud)

Jeffrey G. Walding, Sr. CPP

Administrator of Corporate Security Newfield National Bank

Member of ASIS International Chapter #170

CPP (Certified Protection Professional) ASIS International

Chairman of the New Jersey Banker Security Committee

Vice Chair of the South Jersey Bank Security Officers Associates

Retire Detective Sergeant from the Gloucester County Prosecutor Office

Office: 856-691-2370

Cell: 609-381-9145

[Jeffrey.walding@newfieldbank.com](mailto:Jeffrey.walding@newfieldbank.com)