Identity Theft and the Elderly

The elderly are often specifically targeted for identity theft. Identity theft and fraud against the elderly is a particularly insidious problem because in many instances, after seniors realize that they have been scammed or made the victim of identity theft, they are often hesitant to report the crime out of embarrassment or shame and the belief that it is just another example of their losing their mental acuity. In fact, anyone can be scammed or become a victim of identity theft. Very intelligent people were scammed, for instance, by Bernie Madoff. A recent study by MetLife has shown a dramatic increase in scams perpetrated against people over the age of 60 in the past few years, and the problem is getting worse.

Those who are elderly are also often targeted because they have savings and pensions that can provide easy pickings for identity thieves. The elderly, as a group, are more likely to have good credit scores and are less likely to apply for more credit, so stealing their identity provides more potential for financial gain. Unfortunately, often the people stealing the identities of the elderly are members of their own family, friends, or caregivers. There have been many instances in which rogue nursing home employees have stolen the identities of the residents of the nursing homes where they work when the facility has not properly protected the residents' personal information.

Elderly people are often lonely or isolated, which can make them more likely to listen to the tale of an identity thief who calls them on the phone. They also might not have people around them to warn them of the dangers posed by identity thieves.

Interestingly, a study by the University of Iowa indicates that there might be a physiological reason that the elderly are so often the victims of scams. The study points to the ventromedial prefrontal cortex (vmPFC), which is an area of the brain that controls belief and doubt. According to the study, "In our theory, the more effortful process of disbelief to items initially believed is mediated by the vmPFC, which in old age, tends to disproportionately lose structural integrity and associational functionality." The deterioration of the vmPFC begins as

early as age 60, although, of course, the degree of deterioration can differ significantly among individuals. The study went on to conclude that "vulnerability to misleading information, outright deception and fraud in older adults is the specific result of a deficit in the doubt process that is mediated by the vmPFC." This explains how intelligent older people can often be perceived accurately as being more gullible to the entreaties of scam artists and identity thieves.

The dependency of many elderly on caregivers, whether professionals or family members, also makes them more vulnerable to identity thieves, whether family or professional criminals.

Medicare Identity Theft Threats

Despite calls from the General Accountability Office (GAO), the investigatory agency of the federal government, Medicare still uses enrollees' Social Security number as their Medicare identification number, and it is also prominently featured on their Medicare identification card. The federal government has resisted efforts to eliminate the use of the Social Security number as an identifier, often citing the cost of going to a different identifying number as being between $255 million and $317 million. A common identity theft scam involves seniors receiving calls from telemarketers who contact the senior and tell them that they can receive medical services and equipment at no cost by merely providing their Medicare identification number. A large-scale fraud involving allegedly free supplies for diabetics was used by identity thieves in 2012 to obtain the Social Security numbers of Medicare recipients, and then they used the numbers for making false Medicare claims and for stealing the identities of the Medicare recipients.

TIP

Companies that actually do work with Medicare will not make unsolicited telemarketing calls. In addition, you never should give your personal information, particularly your Social Security number, to anyone who calls you on the phone. You have no way of verifying who they are. If you suspect Medicare fraud, you should call Medicare at their fraud hotline number of 877-486-2048.

Another Medicare Scam

This scam starts with a telephone call from an organization called "Preferred Benefits to Seniors." The callers for this nonexistent group tell their victims that they need a new Medicare card. The callers then ask for personal information

necessary to process the new card. The victims are told that they will lose Medicare benefits if they do not comply. Unfortunately, if the seniors provide personal information including their present Medicare numbers, which still are the person's Social Security number (despite protests from consumer advocates), they will end up a victim of identity theft.

TIP

Never give personal information over the phone to anyone you have not called at a number that you know is accurate. You can never be sure whether the person calling you is who they say they are. In addition, Medicare will never call you by phone and ask for personal information. If you have any question about whether you have been called by Medicare, you can call them at the phone number indicated on the back of your Medicare card, whereupon you will be told that the previous call was a scam.

Medicare Open-Enrollment Scam

The open-enrollment period is the time of the year during which America's 50 million elderly Medicare beneficiaries can choose or change Medicare plans including prescription drug plans. There are often changes in Medicare plans each year and many people are confused as to what they should be doing. As always, scammers and identity thieves are ready to take advantage of this confusion, and Medicare enrollment scams occur every year. Many of these scams involve various solicitations that appear to come from either Medicare or individual insurance companies by e-mail or phone in which you are asked for personal information. Medicare will not contact you by phone or e-mail in regard to any changes in the law or your coverage. A good rule to follow to avoid Medicare scams is to never provide personal information over the phone or in response to an e-mail or text message because you can never be sure that the phone call, e-mail, or text is from a legitimate source regardless of how official the communication might appear.

TIP

The best places to go if you have questions about Medicare are the government's official Medicare website of www.medicare.gov or www.shiptalk.org, which is the website of the State Health Insurance Program, which uses the acronym SHIP. The people at SHIP provide personal advice and counseling in regard to Medicare. The website www.shiptalk.org will provide contact information for the SHIP offices in your state.

Contests and Lotteries

One of the most common scams affecting the public in general, but also preying on seniors in great numbers, are phony contests and lotteries. In this scenario the victims are told that they have won a contest that they have not entered, but they have to pay certain administrative fees or taxes as well as provide certain personal information in order to claim their prize.

TIP

It is hard enough to win a legitimate contest that you have entered. The chances of winning one that you have not entered are nonexistent. Yet by providing personal information to someone who claims you have won a contest, you can make yourself a victim of identity theft. Never give out personal information on the phone to someone you have not called, and always check out the legitimacy of any contest before providing any information.

How to Help Prevent Elderly Identity Theft

There are many things you can do to help elderly family members or friends become less likely victims of identity theft.

- Monitor your elderly family members or friends often. Caution them about giving personal information to people who don't need it, and make sure that their personal information is secure and away from the prying eyes of people who might come to their home.
- Keep income tax returns in a secure location, and make sure that the person who prepares the senior's income tax return not only is reputable but also maintains a good security system for protecting the senior's information and records.
- If the elderly family member or friend is in a nursing home or an assisted living facility, discuss with the management of the facility the security measures that the facility takes to protect the privacy of the personal information of the resident.
- If an elderly family member or friend is in a nursing home, arrange for the person's mail to be sent to you so that you can keep important mail secure.
- Do not allow caretakers to open mail or deal with any financial transactions on behalf of your elderly family member or friend.
- Consider handling the person's bill paying online and avoid paper checks that can be stolen and used for identity theft.

- On behalf of the elderly family member or friend, monitor his or her credit report annually from each of the three major credit-reporting agencies.
- Register the elderly family member or friend for the National Do Not Call list to prevent telemarketers from calling; however, recognize that scammers do not comply with the Do Not Call list.
- To be taken off the mailing and telemarketing lists, call 800-407-1088. You also can go to the website of the Direct Marketing Association at www.dmachoice.org, to register as a caretaker and stop direct marketing advertising from coming to an elderly person in your care.
- Eliminate preapproved credit card offers, which can be used by identity thieves to get credit cards in the elderly person's name, by going to www.optoutprescreen.com.
- The credit bureaus sell the names and contact information for the people in their data banks. You can eliminate this as a problem, and the resulting junk mail and offers that present threats of identity theft when they fall into the wrong hands, by calling 888-567-8688.
- Shred unnecessary personal and financial records. Many elderly tend to hoard old records that they do not need but that can provide fodder for identity thieves.
- Do not have elderly family members or friends carry their Medicare or Social Security card with them. Keep the cards in a secure place. Snatching of the purse or wallet of an elderly person can give a thief the information necessary to make the senior a victim of identity theft if the purse or wallet contained the person's Medicare or Social Security cards.
- Put a credit freeze on the elderly family member's or friend's credit report.
- Check Medicare and medical insurance bills regularly to make sure that there are no improper charges.

Signs of Elderly Identity Theft

If you are looking out for a family member or friend in order to keep them from becoming a victim of identity theft, here are some warning signs for which you should be on the lookout:

- The elderly person has no awareness of a newly issued credit or debit card.
- The elderly person's checkbook has missing checks.
- The elderly person's bank account is suddenly overdrawn.

- Large withdrawals are made from accounts.
- There is a sudden increase in monthly charges on behalf of the elderly person.

The FTC Study on Elderly Identity Theft

Recognizing the seriousness of the problem of identity theft and seniors, the Federal Trade Commission began a detailed study of the problem in 2012, seeking to identify the following:

- The prevalence of identity theft targeting senior citizens
- The extent to which seniors are vulnerable to identity theft
- The types of identity theft schemes and the extent to which thieves use them to target seniors, such as phishing schemes, power of attorney abuse, and tax, Medicare, and nursing home–related identity theft
- The extent to which seniors are victims of familial identity theft
- Precautions seniors can take to protect their identity when seeking accountants, financial advisors, nursing care, home care, and other medical services
- Public- and private-sector solutions to senior identity theft

The study is still ongoing.