Identity Theft

As a member of the Yolo County Multidisciplinary Team, I volunteer my time as an attorney to give advice on legal issues, particularly financial abuse. Con artists of every stripe, including legitimate businesses, are targeting the elderly to relieve them of their money. Financial abuse schemes are becoming more sophisticated and harder to detect. Thieves can now access vulnerable seniors via computer from outside the country.

Identity theft can be effectuated over the telephone, via computer and mail, or with "skimmers" strategically placed on ATM machines, gas pumps or nefariously used in restaurants. The means are endless, and the schemes infinite. The scammer can be a complete stranger, a businessman, or a family member. Here are several scenarios that I have come across as a volunteer attorney working with senior citizens who have become victims of identity theft.

Case #1: Ms. A came to a legal clinic, complaining of an inability to obtain a mortgage. Her credit record was abysmal, with huge amounts of outstanding debt unpaid. Yet she had never so much as used a credit card or borrowed a single dollar. The woman did not believe in carrying debt of any kind. The poor lady could not understand how anyone could possibly have gotten any personal information from her to steal her identity, since she did not transact business other than by cash.

Digging into her past, it was discovered she was recently divorced from her husband of many years. He had a history of questionable behavior when it came to money. Surmising he was the most likely culprit of identity theft, he would have been the only one to have had access to this woman's personal information. The divorce had been somewhat acrimonious, and the two had not communicated since the divorce.

Unfortunately the woman had no way of proving who had stolen her identity, despite strong suspicions the ex-husband was involved. All she could do was dispute the charges to the credit reporting agencies, and go through the long process of trying to clear her name and rehabilitate her credit standing.

Case #2: Ms. B had been cold called by someone who represented themselves as an employee of her bank. The ostensible bank employee warned Ms. B there had been "unauthorized activity" on her account, insisting they needed to verify her bank account and social security number. Ms. B gave them all the information they asked for.

When I was contacted by Ms. B, at the urging of her adult daughter, I advised this naïve woman to close out her bank account; notify law enforcement and fill out a police report; notify the Federal Trade Commission; and put a stop on all credit with the three credit reporting agencies. Ms. B resisted going to all the trouble of taking these necessary steps to protect her credit - until I warned her she might be held responsible for paying debts or bills incurred in her name.

Case #3: Mr. C kept receiving emails from his internet service provider, asking him to verify his account information, warning that his service would be terminated he if failed to comply. I strongly advised him to ignore any such attempts to gain his personal information via computer. It was also suggested he

change from dial-up, to high speed internet service with accompanying up-to-date security software. On my insistence he also downloaded free Web of Trust software, which rated internet sites, warning against shady websites. Since following the hints to avoid phishing scams, Mr. C has not received nearly as many vishing (verification phishing) emails. He is also wary of any attempts to obtain either money or personal information via computer.

Case #4: Mr. D decided to search the internet for information on senior living facilities for some commission work he was doing. The elderly gentleman came upon a website that requested he register, before he could gain access to the website. They wanted to know his name and street and email address. Unwittingly giving all the information asked for, he was subsequently swamped with all sorts of unwanted scam mail, computer spam, and phishing emails.

Each of these circumstances makes it clear that preventive education of the elderly is key to protecting them from identity theft. In Yolo County, a small group of citizens called the Triad Task Force, the action arm of the Yolo County Commission on Aging & Adult Services, partnered with the Yolo County DA's Office, and assisted by the University of CA Davis IED Computer and Media Lab. The Triad Task Force created two DVDs, one on consumer fraud and the other on cyber fraud. We hope to connect with seniors where they live, to teach them how to avoid being a victim of financial predators.

Anyone can view a brief video clip to start a conversation on the subject of cyber fraud at the following link: http://www.youtube.com/watch?v=xvtXH35IeRM

Elaine Roberts Musser
Attorney at Law
P.O. Box 2366
Davis, CA 95617
email:
cell: