Protecting Your Identity From Fraud

- Clarissa Goins, VP Compliance
- Karen Osterhoudt, VP Operations

BANK OF MILLBROOK
The Strength of Relationships

Agenda

- How To Secure Your Identity
- Top 5 Financial Frauds Against Seniors
- Baby Boomers and Identity Theft
- IRS Fraud
- Protection from Scams
- Victim of Fraud
- Checking Your Credit Report

How To Secure Identity

Identity theft occurs when someone uses another consumer's personal information (i.e. name and social security number) with the intent of conducting transactions to commit fraud.

Secure identity by:

- Be selective when using stand alone ATM machines.

- Be wary of shoulder surfers when using ATMs.

-Shred unwanted receipts, credit offers, account statements, and expired cards

- Check credit report often at least annually

Top 5 Financial Frauds Against Seniors

- 1. Medicare/Health Insurance - (i.e. perpetrator poses as a Medicare representative)
- 2. Counterfeit prescription drugs
- 3. Telemarketing/Phone Scams
  - Charity Scams – usually occurs after a natural disaster
  - Fake Accident Ploy – fraudster alleges that child or another relative is in the hospital and needs the money
- 4. Internet Fraud – (i.e. pop up browsing windows that simulating virus
- scanning software, e-mail phishing scam).
- 5. The Grandparent Scam

Note* (According to the National Council on Aging, over 90% of all reported elder abuse is committed by an older person's own family members!)

Baby Boomers and Identity Theft

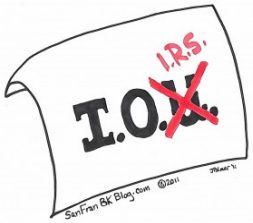
- In 2014, there were 15 million individuals who were victims of identity theft. Thirty-seven percent of the targeted victims were baby boomers.

- Baby boomers are being targeted because of the following:

  - Well established credit histories
  - Sizeable savings and retirement accounts
  - They have a number of credit cards

IRS Fraud Scams

- IRS warns consumers that impersonation scam has seen a 400% surge in recent years. Signs of potential IRS scam include:
  - Scammers make unsolicited calls
  - Use scare tactics (i.e. arrest)

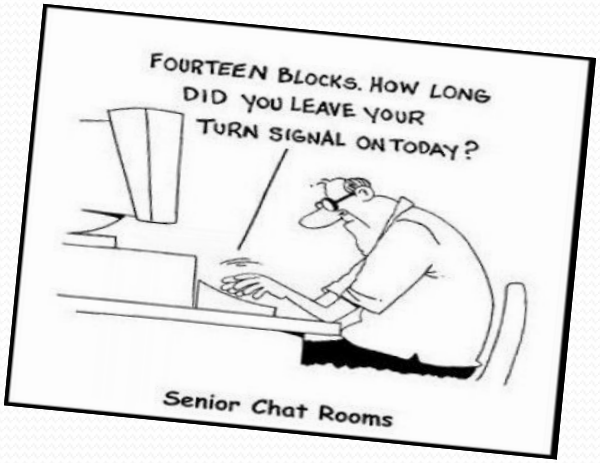


  - Scams using caller ID spoofing – (appears that the call is coming from the IRS or Department of Treasury)
  - Demands a particular type of payment such as prepaid cards and costs victims over $23 million per year

Remember the IRS will not demand immediate payment, you will be sent a bill in the mail first.

Protection from Scams

- Do not give any personal information over the phone unless you are certain with whom you are speaking with.
- Do not carry your social security number.
- Do not open unfamiliar emails or click on links located within the email.
- Do not use an unsecure network when accessing personal information on the internet. (***Keep anti-virus software on your computer up to date.)***
- Do not discard of mail or prescription bottles with personal information listed on it.
- Have paper checks delivered securely.
- Keep your personal information in a secure place at home, especially if you employ outside help, or are having work done in your house.



I'm A Victim of Fraud – Now What?

- Immediately place an initial fraud alert on your credit report*
  - (initial alert stays on credit report for 90 days and its free)
  - Contact 1 of the following Credit Reporting Agencies:
    - Equifax
    - Experian
    - TransUnion
  - Contact your financial institution and ask them to place an alert on your bank accounts

Credit Report

- Where can you get a free credit report?
  - creditkarma.com (includes overview of your credit scores and credit accounts from Equifax and TransUnion)
  - www.annualcreditreport.com – will be asked to answer a series of questions to confirm your identity
  - Other credit reporting services:
    - Freecreditreport.com – Initial credit report is free with your Fico score. (Monthly charges do apply for credit monitoring.)