



To: Tewksbury Township Seniors  
From: Kathy Reddy, Senior Corner  
Re: Monthly Senior Scam – August 2016

## **Scams Continue to Flourish**

Identity theft occurs when someone obtains and fraudulently uses or attempts to use a victim's personal information (i.e., social security number, birth date, credit and debit card numbers, financial account information, medical information, email addresses, passwords.) A Justice Department report released in late 2015 reported that 17.6 million Americans were victims of identity theft in 2014. The total financial loss was \$15.4 billion dollars. **We may not know for years the extent of theft of children's identity, since fraudulent use of their stolen identity will show up years later when they apply for their first credit card or job.**

Protecting yourself begins by learning about the problem before you have a problem. Obtain and carefully read "Taking Charge" from the FTC, which describes what you should do if your identity has been compromised, how you can reduce your risk, and sample letters and forms. It is free and available at our municipal building and online at [www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf](http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf). I can also email it to you if you like.

Internet fraudsters can impersonate a business or other organizations to trick you into giving out your personal information. A caller or email sender might claim to be a federal or state government agency or your bank or credit card provider. The call or email may be from an imposter or hacker. Don't believe what your computer or telephone tells you.

Never reply to email, text, pop-up messages or to callers that ask for your personal or financial information. Don't click on links within them either, even if the message appears to be trustworthy. If you do, a scammer can install malware, viruses and spyware on your computer. The link might send you to a spoof site, a lookalike website set up by a scammer to trick you into entering personal information.

Never provide personal information in response to a call, text or email. If you suspect it's legitimate, visit the real company or agency in person or call using a telephone number that you know is correct, e.g. from your card or a legitimate bill or a phone book.