NEWSLETTER #3

We'll begin with threat that never goes away - Identity Theft and some tips to reduce your exposure.

We'll then move on to another chestnut – The Travel Club Scam.

In closing we'll deal with the topic that is the basis of this newsletter -Senior Financial Fraud – but viewed from a different angle. We'll look at the impact of your health as it relates to this issue.

ALERTS AND TIPS TO PROTECT YOURSELF FROM BEING SCAMMED

REDUCING YOUR RISK OF IDENTITY THEFT

To help you avoid identity theft, here are NNN tips provided by Boston Private Company from their program to train seniors how to avoid financial problems, in this case ID theft.

Use a Credit Card Instead of a Debit Card

This tip doesn't actually help prevent ID theft. Instead it helps you deal with the issues it causes. Specifically, it will be your credit card issuer's money that gets tied up, not yours. You will still have your money available to pay bills until things are cleared up.

Lower the Limits on Your Crredit Cards

Now that you are retired you theoretically should have less need to purchase big ticket items with your credit cards. Lowering the limits helps minimize the damage if your ID is stolen.

There is Never a Good Reason for Store Personnel to Tak Your Credit Card Out of Your Sight

Stengthen Passwords

This advice is like “eat your brocoli.” Everyone agrees with but almost no one does it. Also in the brocoli genre is don't use the same password at multiple sites.

It is a pain to use different strong passwords which use letters, numbers, and symbols but there are ways to make it easier. For example, say you need an AMAZON password. You could take the last three letters - ZON - add your street address - 1141 - for me and use the symbol on your keyboard for the position in the alphabet for the first letter which in this case is an A. A is number 1 in the alphabet so just using the symbol above it - ! - Gives you the extremely strong password ZON1141!. The real beauty of using this system to create passwords is you don't have to remember them. You can simply recreate them every time you revisit a site if you have to.

Also, a great example of why you shouldn't use the same password at multiple was a recent incident for a major airline's frequent flier rewards site. Some customers of this very secure site used the same

password at another very insecure web site. The hackers who got passwords from there tried them on more secure sites where they worked just fine and they sent themselves all sorts of gifts using stolen points.

Careful with Purchases on Smartphones and Tablets

The Center for Internet Security warns people not to make purchases with these devices while connected to a public wireless network because these devices have limited security and hackers can easily intercept the network traffic to see unencrypted passwords and credit card numbers.

If the Site Accepts It Always Use PAYPAL

If you don't have an account sign up for one. Its free and you won't have to supply your credit card information on any site that accepts it and that number is increasing. I can personally vouch for PAYPAL and always use it if it is accepted.

Pop-Up Windows Are Dangerous

Pop-Up windows aren't just annoying. They are usually Phishing scams and can carry viruses.Close them immediately by pressing CNTRL and F4 for Windows or COMMAND + W for MACS.

Fake Retail Sites

Scammers set up fake retail sites to collect credit card information. To help avoid being a victim ceck the **CONTACT US** page before making a purchase. Specifically look for a phone number and physical address as well as the **TERMS and CONDITIONS** link fake websites are less likely to post these. Protect yourself further by Googling the phone number ans street address to see if they match the company.

Look for Secure Websites

This is easy to do. Simply look at the website url (address at the top of the page) to see if it starts with //:http**s** not just //:http. The **s** means secure.

On-Line Auctions

On-line auction sites like E-Bay are generally OK but if you lose an auction and a seller claims to offer the merchandise off site it is so likely to be a scam it's not worth trying.

Craig's List

This site can not only contain frauds but people have been robbed sand even murdered after showing up at a meeting point with cash for a non-existant item. In one of the latest frauds a acammer simply copies a legitimate offer of a vacation rental property, posts it on Craig's List collects, the money in advance, and you show up for vacation and the owner has never heard of you.

THE TRAVEL CLUB SCAM

The con here is pretty basic. You attend a high pressure pitch that promises you that if your join their vacation club you will receive deeply discounted vacation packages to all sorts of exotic locales.

Unfortunately, you will victimized in one of two ways.

First, despite paying thousands of dollars for these ***deeply discounted fares*** the clubs booked your travel through Expedia and Priceline which you could do yourself at no extra cost.

Second, you may get an airline ticket but when you get to your destination you find out that the club didn't pay for anything else.

So the question arises – how disd they get you to attend these high pressure sales pitches in the first place? The answer is with scammers trick that should always go in the recycling bin as soon as you see what it is. **YOU HAVEWON TWO FREE AIRLINE TICKETS** which spells FRAUD.

Basically there are so many conditions that the tickets are worthless, but your big exposure is you have to attend the **FREE INFORMATION SESSION** to get your "free" tickets. Another Red Flag for Fraud.

On the good news side of this, State Attorney Generals in Mass, NJ, and Illinois have become very proactive in suing these clubs and getting refunds for customers into the millions of dollars but it's much safer not to get scammed in the first place and anyone can be a target. I get about one per month Below we'll provide some warning signs from Consumer Reports.

You've Won

You receive mail saying you've won a prize but you have to pay to get it.

Must Attend a Sales Pitch

The pitch for the pitch is that you will learn how to get hugh vacation discounts, exclusive perks and more when you must attend this mandatory pitch at a hotel or restaurant.

High Pressure

You must act immediately or special discounts available today only are screaming FRAUD!

Loopholes

Contract specifies benefits are subject to availability. This means you are agreeing to get nothing for your money. Another flag is that using the club's benefits involve long advance notice which makes it very difficult for you to use your alleged benefits.

High Costs

Membership costs thousands of dollars and requires high annual fees to keep you membership from expiring.

Protect Yourself With Some On-Line Research

If you've read up to this point, this section should be unnecessay. You shouldn't ever get this far with these crooks but if you insist here a few on-line checks. Google the **Club Name + Complaints**. Check the Better Business Website www.bbb.org.

HEALTH AND FRAUD

The Issue

Most seniors are aware of the grim statistics. Last year people 60 and older accounted for 27% of fraud complaints last year, up from 22% in 2011. Also, this number is certainly too low because seniors may not report theft because it was by their older children, or they will be deemed incapable of managing their financial affairs, or because of dementia they may not realize they have been victimized.

Making the situation worse that the number of investigators and prosecutors are not increasing to keep pace with this rapidly rising epidemic.

Why Seniors are More Vulnerable to Scams?

Seniors, as Willie Sutton said are where the money is so they are targeted. But why are they such inviting targets? Some significant reasons are social isolation, health conditions that may diminish financial deciion making, and Federal Reserve policy on interest rates.

As an example of dimished financial decision making an 80 year old blind woman who couldn't drive bought an auto club policy.

The Feds decision to keep interest rates low has pinched seniors living on fixed incomes so they have to take on some risk to boost returns, so enter the con men (or women.)

The Interplay of Health and Fraud

According to Duke University research more than 1/3 of people 71 and older have some form of dementia or mild cognitive impairment. This is a problem because even mild cognitive impairment will more problems performing basic money managent tasks such as paying bills or managing bank accounts than those without these conditions. In fact, problems managing your finances can be an early sign of developing dementia.

Unfortunately, it's not only cognitive impairment that can make you more likely to be scammed. A recent AARP study found that victims of on-line scams were more likely to have had a serious illness or injury in the ptreceeding 2 years than those who were not scammed. The study claims that the ill or injured people have weakened immune system which can affect judgement.

How to Protect Youself

How Does it Work?

The scam itself is pretty simple. You receive a call, voice mail message, or E- Mail from a "Debt Collection Agency." They say that you allegedly owe money to a scary Federal Agency (IRS), law enforcement (Police, Courts, Attorney General), or your utility company.

The basic pitch is that you owe money and if you don't pay up or call back IMMEDIATELY terrible things will happen to you. You will be arrested, your car will be repossessed , or your gas or electric will be turned off immediately.

The people running these shows were trained in the high pressure penny stock boiler rooms of the 1990s so they are relentless and shrewd. They will use legal sounding phrases the best of which is "the statute of limitations has run out on your civil and legal rights." Truly a classic.

They will also send fake documents that look quite legitimate.For example, they may name government criminal collections task forces that simply don't exist.

Signs That It's a Scam

This section is really unnecessary. This approach is always a scam. First, real government agencies and utilities will almost always contact you with registered mail and try to collect before turning you over to a Debt Collection Company.

Second, the legitimate agencies first attempt may ask for money and spell out consequences, but the demands are not immediate on first contact. And, since using the postal mail for fraud is a serious offense, scammers use E-Mail or phone calls. Also, don't be fooled by the official-looking caller ID. Using computer-based calling, scammers can display any caller ID they want.

Finally, another sign of the scam is the payment method. Either they want you to wire them the money or let them deduct it from your checking account. ABSOLUTELY NEVER do this.

What Should You Do if They Call?

The answer is pretty simple. Tell them to put their claim in writing with ID and phone numbers as well as physical addresses for everyone involved with this case so you can discuss it with your attorney. Most likely they will hang up. If not, do so immediately and whenever they call again. If they were legitimate they would have no problem complying with your request.

While the response above sounds simple you might need to be prepared for an arduous battle.Keep in mind that this is their job and they work on commission. Just keep on ignoring them and eventually they'll realize they are wasting their time with you, and time is money to them. If it becomes too difficult, talk to the police department for suggestions.

THE MICROSOFT (OR OTHER VENDOR) SCAM

I especially appreciate the opportunity to discuss this one because several HM residents have called or E-Mailed me on this one.

How Does It Work?

There are actually two versions of this deception. The first is not so much a typical illegal scam but an attempt to sell you something you don't need from a somewhat legitimate vendor. The second version is more insidious in that they charge you for stealing your identity.

Version 1 - The Vendor Scam

You place a technical support call to the 800 number for a software product installed on your computer. A very polite person offers assistance which usually works. However, in working on your computer he has found there are some significant issues affecting your computer's performance that he can fix remotely for usually $100 to $300. Alternatively, he has discovered that your computer is infected with malware with the same fix pitch. If you refuse, he will offer to show you error logs that prove his claim, but of course they wouldn't mean anything to you and are almost always normal anyway. If you still refuse, your polite technician can become quite pushy.

What Should you Do?

Actually, quite short and sweet. Reply **No Thanks, if I need help I'll call back. Bye.**

Version 2 - The Real Scam

In this version, identity thieves have gotten hold of a software vendors customer list which is quite easy to do. The difference here is that the scammer is not interested in stinging you for a couple hundred bucks. He's after your identity so his approach is different He will call you and to describe a scarey bug or infection in their software that he will fix for free. All he needs is for you to allow him to have remote access to your computer and everything will be fine. If you allow this, everything will be fine for him because he will have infected your computer with invisible software that will silently send him every account number and password you enter.

What Should I Do?

In this case, if you didn't initiate this call just follow the old 70s line and **Just Say No** and hang up.If you are still concerned, call your software company's hotline and ask if they are aware of any such issue.

TIMESHARE FEE ELIMINATION

How Does it Work

Scammers are acutely aware of your pain points. One of the biggest regrets many people have is the yearly fee for a timeshare they no longer want or use. Therefore they are vulnerable to a letter like the one I recently got. It was specifically addressed to me at HM. It even said "Dear Allan" They nicely informed me that I was eligible to eliminate all future timeshare fees including 2015 if I acted by 12/1/2014. They also said this was my last opportunity because they had unsuccessfully tried to contact me previously. They even gave me a reference number for when I called them.

What they didn't explain was how they would get the Timeshare management company to drop fees I was legally required to pay them.

For those who get this letter the sender is **Property Management Services in Rockville, Md.**

What Should I Do?

Most HM villages provide paper recycling. This should go there immediately.

A POTPOURRI OF LITTLE TIPS TO MAKE FOR A SAFER HOLIDAY

1. Never post your travel plans on social media. You can do that along with pictures and descriptions after you're home. Burglars and scammers love to know when you're house is empty and your mail will be uncollected.

2. Open a **PAYPAL** account and use it instead of your credit card wherever it's accepted. It's always a good idea to not give out your credit card number, expiration date, but especially your security code.

3. Sign up for on-line account access at your bank and credit card company and check charges weekly. If you're compromised the less time you give the scammers the less you will have to undo.

4. To avoid receiving credit card applications that can be stolen from your mailbox and used, sign up to opt out credit card mailings by going to **optoutprescreen.com** or call **888-567-8688**. Scammers frequently steal these from mailboxes and open credit cards in the recipients name.

5. Put your landline and cellphone on the National Do Not Call List at **donotcall.gov** or call **888-382-1222**. That way solicitation calls can usually be assumed to be scams.

That's it for this newsletter but there's much more to come as scammers never rest.

Have a great Holiday and stay safe. See you in the next issue.

Allan Pomerantz