Self-Reliance Institute Newsletter

April 2014 Volume 2, Issue 4

Life Can Change Quickly

This week, I had a personal experience that I'd like to share with members of the Self-Reliance Institute.

The experience was a good reminder for me about being prepared for the type of event that we rarely talk about with our friends or even our families. I hope my experience will serve as a catalyst for you to be sure you're ready.

We often discuss what we'd do if we lost power for an extended period of time. Or, if we were caught up in a natural disaster that made our home unlivable.

We talk about how to protect ourselves and our families from intruders. We talk about what we'd do if we were cut off from a regular source of food and nourishment.

We talk about major events from the outside world that could disrupt our lives and what we can do to be self-reliant if one of those events takes place.

Life Changes : Continued page 5

IN THIS ISSUE

Spring Time is Scam Time

Although it's still snowing here at 8,000' in the Rocky Mountains, spring is just around the corner for most of the country. And every year it seems that just as the bears come out of hibernation, so do the fraud artists who try to steal your identity and money.

So I thought this would be a good time to look at some of the scams that could plague Americans this year. And while most of you would never fall for these scams, there are many people who do. So please share this information with your friends and family.

As goofy as some of these may seem to well-informed members of the Self-Reliance Institute, the reality is that millions of Americans fall for these schemes. That's why we all need to spread the word and help those we love and care about avoid falling prey to these parasites who seek to steal your hard-earned money.

Oh, before I forget, here's the link to this month's newsletter that contains all of the advisories from February. Just click → **HERE** to open and/or download the newsletter.

OK. Let's get back to the top scams. I've pulled these from a number of resources, including the Council of Better Business Bureaus who originally published some of these at

Scam Time: Continued page 3

Tax Time and Identity Theft

Today is the first day of National Consumer Protection Week. And, as has been the case for 14 consecutive years, identity theft is the top consumer complaint in the United States.

In a statement released Thursday, the Federal Trade Commission reported:

"*Identity theft continues to top the Federal Trade Commission's national ranking of consumer complaints, and American consumers reported losing over $1.6 billion to fraud overall in 2013, according to the FTC's annual report on consumer complaints released today.*

"*'Americans of all ages are vulnerable to identity theft, and it remains the most common consumer complaint to the Commission,' said Jessica Rich, director, Bureau of Consumer Protection. 'We urge consumers to visit FTC.gov/idtheft for tips to prevent and mitigate the damage from identity theft.*'

"*The Commission received more than two million complaints over*

all, as reported in the agency's Consumer Sentinel Network Data Book 2013, of which 290,056,

Identity Theft: Continued page 6

Medical and Tax ID Theft Advisory (Theft Advisory)

In last week's advisory, I talked about the most common consumer scams taking place across America so that members of the Self-Reliance Institute can be on-guard against those scams and warn their family and friends.

This week, I'd like to warn members of the Institute about two particularly aggressive forms of identity theft and fraud that are spiking right now.

The first is a tax fraud scam. And given that it's the time of year when we all sit down to prepare and file our taxes, it may not be all that surprising that identity thieves and fraudsters try to take advantage of the fact that most everyone is thinking about taxes right now.

While there are many schemes that identity thieves and fraudsters use to commit tax fraud and identity theft – the most common being filing false tax refund claims in the name of victims – there's a more direct method taking place as I write this advisory.

In fact, J. Russell George, the Treasury inspector general for tax administration, is calling this scheme "the largest scam of its kind that we have ever seen."

Here's how it works.

You get a call from an individual claiming to be from the Internal Revenue Service. The IRS "agent" claims you owe back taxes and that you must pay right away or else you'll be arrested. (In other variations, the "agent" threatens the loss business or driver's license or even deportation from the country.)

The "agent" then tells the victim that to avoid arrest they must pay immediately by using a pre-paid debit card or wire transfer.

To date, the IRS reports that more than 20,000 people have reported

Theft Advisory: continued page 4

Using A Credit Security Freeze (Credit Freeze)

As part of last week's Self-Reliance Institute Advisory about medical and tax fraud identity theft, I asked if you knew what a credit freeze is and I promised that this week I'd talk about a proactive step to combat identity theft.

Well, that proactive step is a credit freeze.

Perhaps the single best way to protect against an identity thief opening a new credit account in your name is to place a credit freeze on your credit files with all three major credit bureaus. Credit freezes are often called security freezes by the three major credit bureaus.

By placing a credit freeze on your credit files at all three major credit bureaus, you maintain control over who can access your credit report and when, thereby blocking identity thieves from using your name and credit to open fraudulent credit accounts that will harm you and your credit profile.

Through a combination of state laws and voluntary programs in place at all three major credit bureaus, anyone can place a credit freeze on their credit files. But remember, you must place the credit freeze at each of the three major credit bureaus individually.

When you place a credit freeze on your credit files, you will either select or be provided a password or PIN (personal identification number) so that you can temporarily remove the credit freeze when you want to add a new credit account to your credit file. Be sure to maintain this password or PIN in a secure location so that it will be available when you need to temporarily lift the credit freeze.

Depending on the state you reside in, and whether or not you have been a victim of identity theft, there may be a fee for initiating a credit freeze and for lifting the freeze when you need to grant access to your credit report to a potential creditor.

Credit Freeze: continued page 7

Scam Time

Continued from page 1

MarketWatch. I cut their list down to the ones I believe are most prevalent.

1 – Medical Alert Scam: "With promises of a "free" medical alert system, the scam targeted seniors and caretakers and claimed to be offering the system free of charge because a family member or friend had already paid for it. In many cases, seniors were asked to provide their bank account or credit information to "verify" their identity and, as a result, were charged the monthly $35 service fee. The system, of course, never arrived and the seniors were left with a charge they had trouble getting refunded."

"... con artists are taking advantage of technology that can change what is visible on Caller ID"

2 – Auction Reseller Scam: "Many people turn to eBay and other online auction sites to sell used items they no longer need, and relatively new electronics seem to do especially well. But scammers have figured out a way to fool sellers into shipping goods without receiving payment. Usually the buyer claims it's an "emergency" of some sort — a child's birthday, a member of the military shipping out — and asks the seller to ship the same day. The seller receives an email that looks like it's from PayPal confirming the payment, but emails are easy to fake. Always confirm payment in your eBay and PayPal accounts before shipping, especially to an overseas address." (I see people fall for this all the time!)

3 – Arrest Warrant Scam: "In this scam, con artists are taking advantage of technology that can change what is visible on Caller ID, and allowing them to pose as the office of the local sheriff or other law enforcement agency. They call to say there is a warrant out for your arrest, but that you can pay a fine to avoid criminal charges. Of course, these "police" don't take credit cards; only a wire transfer or prepaid debit card will do. Sometimes these scams seem very personal; the scammer may refer to a loan or other financial matter. It may just be a lucky guess, but don't be fooled into thinking you are about to be arrested."

4 – Home Improvement Scams: "Home improvement scams vary little from year to year, and most involve some type of shoddy workmanship from unlicensed or untrained workers. The hardest for homeowners to detect, and therefore the easiest for scammers to pull off, are repairs or improvements to the areas of your home that you can't see: roofs, chimneys, air ducts, crawl spaces, etc. Scammers may simply knock at your door offering a great deal because they were "in the neighborhood," but more and more they are using telemarketing, email and even social media to reach homeowners. Helpful videos on YouTube can add legitimacy to a contractor, but consumers have no way of knowing if the video is real or "borrowed" from a legitimate contractor. Check out home contractors before saying yes." (It breaks my heart that our elderly population falls for this all the time!)

"Helpful videos on YouTube can add legitimacy to a contractor, but . . ."

5 – Foreign Currency Scam: "Investments in foreign currency can sound like a great idea, and scammers frequently use real current events and news stories to make their pitches even more appealing. They advertise an easy investment with high return and low risk when you purchase Iraqi dinar, Vietnamese dong or, most recently, the Egyptian pound. The plan is that, when those governments revalue their currencies, increasing their worth against the dollar, you just sell and cash in. Unlike previous hoaxes, you may even take possession of real currency. The problem is that they will be very difficult to sell, and it's extremely unlikely they will ever significantly increase in value." (Watch for this to happen because of what's taking place between Russia and Ukraine!!)

6 – Smishing: (Say what?) "With online and mobile banking skyrocketing, it isn't a surprise that scams quickly follow. One major tactic recently is the use of scam texts, known as "smishing," to steal personal information. They look like a text alert from your bank, asking you to confirm information or "reactivate your debit card" by

Scam Time : continued page 8

Theft Advisory

Continued from page 2

this fraud scheme and victims have paid more than $1 million dollars to the tax fraudsters.

So please remind your family and friends that the IRS would never call you by phone and demand immediate payment. And to stay up-to-speed on other forms of tax fraud and report fraud to the IRS, you can bookmark this Tax Fraud Alerts web page at the IRS by clicking HERE.

"report fraud to the IRS . . . http://www.irs.gov/uac/Tax-Fraud-Alerts "

Now let's talk about Medical Identity Theft.

I've been investigating, consulting and testifying before Congress on identity theft since 1998. When I first started, medical identity theft was almost unheard of and rarely took place. But, it did exist and I constantly warned in my public testimonies that I believed medical identity theft would grow.

I'm sorry to say I was correct.

Here's what Adam Levin reported this week at Credit.com and was reprinted at MarketWatch.com.

"*If recent disclosures regarding the massive wave of breaches suffered by retailing icons Target, Neiman-Marcus and Sally Beauty haven't scared you enough, try to wrap your brain around the new Ponemon Institute Patient Privacy and Data Security study. The study has found a 100% increase in criminal attacks on health care organizations since 2010. But if that weren't enough, they also found something far more disturbing.*

"*'Despite concerns about employee negligence and the use of insecure mobile devices, 88 percent of organizations permit employees and medical staff to use their own mobile devices such as smartphones or tablets to connect to their organization's networks or enterprise systems such as email. Similar to last year more than half of (these) organizations are not confident that the personally-owned mobile devices or BYOD are secure.'*

"*According to the report, very few organizations require their employees to install anti-virus/anti-malware software on their smartphones or tablets, scan them for viruses and malware, or scan and remove all mobile apps that present a security threat before allowing them to be connected their networks or systems. …*

"*What should concern you about these findings (and several others in the report) is that assaults on health care systems don't simply create the potential to have credit cards stolen or checks redirected: it's that hackers are getting access to your health care data ("protected health information," or "PHI" in regulatory speak), and the real world consequences of that are far more devastating.*"

"very few organizations require their employees to install anti-virus/anti-malware software on their smartphones or tablets. . ."

Now get this.

"*Medical identity theft is on the rise, just as the rise in criminal breaches of health care providers is spiking. Medical identity theft accounted for 43% of all identity theft reported in 2013, and the U.S. Department of Health and Human Services estimates that somewhere between 27.8 and 67.7 million people's medical records have been breached since 2009 (and that's before the flawed rollout of the Affordable Care Act).*"

Read those statistics again.

--Medical identity theft accounted for 43% of all identity theft reported in 2013.

--Between 27.8 and 67.7 million people's medical records have been breached since 2009.

Folks, that's a, pardon the pun, epidemic of medical identity theft.

And, in my opinion, it's all because of a deeply flawed medical records system that is being worsened by the Affordable Care Act – also known as ObamaCare.

Further, you and I can't count on the government or the health care industry to fix this problem.

So before I sign off for this week, let me ask you a few questions so that next week I can share information on how to combat both tax fraud/identity theft and medical identity theft.

Theft Advisory: continued page 7

Life Changes

Continued from Page 1

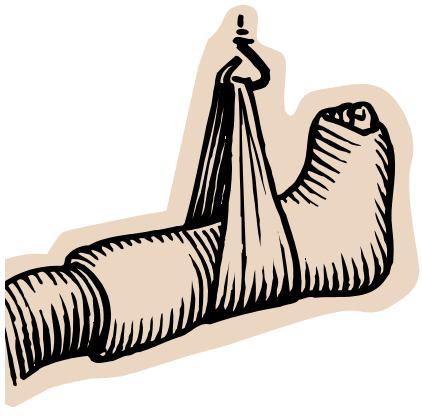
But sometimes it's the smaller aspects of life that we forget to prepare for so that, if the unexpected arises from within, others can easily take care of those details.

Let me be specific and share my experience.

I have a friend (to protect my friend's privacy, I'm going to avoid sharing any information that might give away my friend's identity) who needed to take care of a medical issue right after the beginning of the year. My friend lives alone and the extended family is scattered around the country.

This friend is highly successful and the type of individual who normally is the most organized person you could ever meet. The medical issue, while serious, was not a complete surprise and there was time to be prepared for the needed medical procedure and the impacts it might have on day to day life.

Like everyone else who knows this individual, I assumed my friend was prepared in case things did not go as well as everyone hoped. In other words, we assumed our friend had considered the possibility that the medical treatment might not go exactly as planned and there could be a period of time when others would need to take care of the day to day issues that arise in life.



Sadly, after several weeks of doing well, my friend's medical condition has taken a dramatic turn to the downside and I've just returned from a hastily arranged 36-hour trip to see my friend for what may be the last time.

In addition to the obvious concerns my friend's family has about the serious medical challenges they are dealing with, they are now learning that my friend didn't prepare to be incapacitated. Now they are trying to figure out all the issues that must be addressed to maintain my friend's day to day life so that if my friend does recover that life won't be in a shambles.

While it seems mundane to most of us, issues like being sure monthly bills are monitored and paid can suddenly become major problems if the proper information is not easily located and useable by family or someone designated with power of attorney.

In fact, as I've seen first-hand more than once in my life, not being prepared for an extended illness can result in substantial stress on family members and friends who need to step in while the individual is incapacitated.

So here's my suggestion for everyone who belongs to the Self-Reliance Institute. At least once a year, be sure to create a list of all the day to day items that must be taken care of in your life in the event you are incapacitated for several days, a week, a month, or longer.

Once you've created the list, be sure you provide it to a trusted family member or friend. And, if you don't have an immediate family member who has the ability to pay your bills while you are incapacitated, be sure to grant power of attorney to a responsible individual who can act in your place if the need arises.

I'll address all of these issues in more detail in future advisories. But, having just returned from seeing a friend who is fighting for life, I am struck by how much additional stress the extended family is dealing with as they try to piece together what needs to be done to keep my friend's home and daily life in order.

As always, I'd love to hear your thoughts on this issue. Have you faced a similar crisis in your life or the life or a family member or close friend? Have you taken steps to be prepared in case you are incapacitated? Do you have suggestions I can share with other members of the Self-Reliance Institute?

Please email me at
Rob@SelfRely.com

Be safe and secure,

Rob Douglas

Identity Theft

Continued from Page 1

or 14 percent, were identity theft related. Thirty percent of these incidents were tax- or wage-related, which continues to be the largest category within identity theft complaints."

As members of the Self-Reliance Institute know, there is no one more skeptical of the federal government and the services it provides than me.

But, as many of you also know, I've advised the federal government – along with a number of states, private individuals, and the media – on identity theft and information security issues for many years.

In fact, I first provided testimony and consultation to Congress and the Federal Trade Commission on identity theft and information security issues in 1998 – before the feds even started keeping track of identity theft as a consumer complaint.

So I can tell you with confidence that the materials and information the FTC makes available to the public when it comes to understanding and combating identity theft is worthwhile because I've played a role in bringing this issue to the national spotlight.

Bottom line: I highly recommend that you check out the FTC's identity theft materials at FTC.gov/idtheft and share that web address with your family and friends. And, if you've been a victim of identity theft, you can file a complaint with the FTC by going to FTC Complaint Assistant and clicking on Identity Theft in the upper right hand corner.

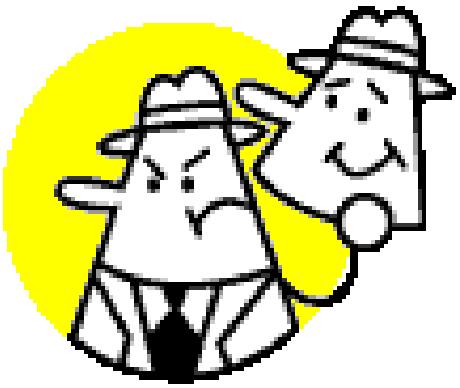
While National Consumer Protection Week prompted me to share this information with members of the Self-Reliance Institute this week, there's an even more important reason. In recent years, identity theft and other forms of associated fraud have spiked around tax time and often involve tax-related schemes.

Recently, the Internal Revenue Service released a list of the most frequent tax-related scams in "Uncle Sam's 'Dirty Dozen' List of Tax Scams."

I want to highlight six of the 12 scams the IRS discusses as they are the six where innocent Americans taxpayers are most likely to be a victim. Those six, with a portion of the IRS description are:

1) Identity Theft – *"Tax fraud through the use of identity theft tops this year's Dirty Dozen list. Identity theft occurs when someone uses your personal information, such as your name, Social Security number or other identifying information, without your permission, to commit fraud or other crimes. In many cases, an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund*."

2) Pervasive Telephone Scams – *"The IRS has seen a recent increase in local phone scams across the country, with callers pretending to be from the IRS in hopes of stealing money or identities from victims. These phone scams include many variations, ranging from instances from where callers say the victims owe money or are entitled to a huge refund. Some calls can threaten arrest and threaten a driver's license revocation. Sometimes these calls are paired with follow-up calls from*



people saying they are from the local police department or the state motor vehicle department."

3) Phishing – *"Phishing is a scam typically carried out with the help of unsolicited email or a fake website that poses as a legitimate site to lure in potential victims and prompt them to provide valuable personal and financial information. Armed with this information, a criminal can commit identity theft or financial theft…It is important to keep in mind the IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels*."

4) False promises of "free money" from inflated refunds – *"Scam artists routinely pose as tax preparers during tax time, luring victims in by promising large federal tax refunds or refunds that people never dreamed they were due in the first place*."

5) Return preparer fraud – *"About 60 percent of taxpayers will use tax professionals this year to prepare their tax returns. Most return preparers provide honest*

Identity Theft: Continued page 8

Credit Freeze

Continued from Page 2

The three major credit bureaus are Equifax, Experian and TransUnion. To learn more about placing a credit freeze (also called security freezes) with each of the three major credit bureaus please click on each of the following links:

Equifax Security Freeze

Experian Security Freeze

TransUnion Credit Freeze

The combination of large and small database breaches have statistically put all Americans personal identifiable information at risk. With the digitization of medical records, database breaches will become even more common and raise the odds of each individual's risk of becoming an identity theft victim.

For additional information about credit freezes, I recommend you check the Consumers Union's Guide to Security Freeze Protection. It includes a state by state listing of how credit/security freezes work for individual states.

The Federal Trade Commission (FTC) is also a good resource for additional information about Extended Fraud Alerts and Credit Freezes.

Let me close with a word about children, seniors and credit freezes.

While everyone should consider placing a credit freeze on their credit files maintained by all three of the major credit bureaus, it is especially important that seniors, those responsible for incapacitated seniors and parents of children give extra consideration to initiating credit freezes.

Identity thieves specifically target children and seniors as they are much less likely to monitor their credit files and are also less likely to detect if a fraudulent account has been opened in their name. This is because children and seniors do not typically open new credit accounts and therefore have little need to check their credit reports.

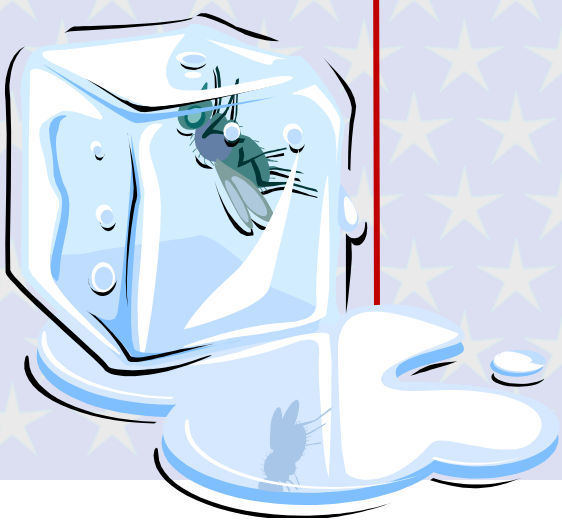
I hope you find this information of use.

If you have specific questions about Credit (Security) Freezes, please email me at Rob@SelfRely.com

Also, I'd love to hear your personal experiences involving Credit (Security) Freezes and/or identity theft.

Be safe and secure,

Rob Douglas



Theft Advisory

Continued from page 4

Have you ever been a victim (or know someone who has) of tax fraud or tax identity theft?

Have you ever been a victim (or know someone who has) of medical identity theft?

Do your health care providers have your Social Security Number?

Do you know what a Credit Freeze is?

Do you have a Credit Freeze in place on your accounts?

You can email me at Rob@SelfRely.com with your answers (I'll keep them anonymous as always!!) and next week we'll discuss proactive steps to fight tax fraud/identity theft and medical identity theft.

Until then, be safe and secure and share this information with your family and friends!

Rob Douglas

Identity Theft

Continued from Page 5

service to their clients. But, some unscrupulous preparers prey on unsuspecting taxpayers, and the result can be refund fraud or identity theft. It is important to choose carefully when hiring an individual or firm to prepare your return. This year, the IRS wants to remind all taxpayers that they should use only preparers who sign the returns they prepare and enter their IRS Preparer Tax Identification Numbers."

6) Impersonation of charitable organizations – *"Another long-standing type of abuse or fraud is scams that occur in the wake of significant natural disasters. Following major disasters, it's common for scam artists to impersonate charities to get money or private information from well-intentioned taxpayers. Scam artists can use a variety of tactics. Some scammers operating bogus charities may contact people by telephone or email to solicit money or financial information. They may even directly contact disaster victims and claim to be working for or on behalf of the IRS to help the victims file casualty loss claims and get tax refunds.*"

To see the entire list and complete descriptions, please go to: "Uncle Sam's 'Dirty Dozen' List of Tax Scams."

For many folks, tax time is stressful enough. The last thing I want to see happen is for you to become a victim of identity theft at this time of the year when identity criminals are very active. So, please use the resources I've provided here today from the FTC and the IRS.

And, if you've been a victim of identity theft – especially if it was a tax-related scheme – I'd like to learn of your story. As always, you can email me at Rob@SelfRely.com

Be safe and secure,

Rob Douglas

Scam Time

Continued from Page 3

following a link on your smartphone. Banks of all sizes have been targeted, and details of the scam vary, but the outcome is the same: scammers get your banking information, maybe even your ATM number and PIN. You may even inadvertently download malicious software that gives the scammer access to anything on your phone." (Relatively new scam, but it will grow!)

7 – Affordable Care Act (ObamaCare) Scam: "Scammers had a field day with the Affordable Care Act, or Obamacare, using it as a way to fool Americans into sharing their personal information. Scammers would call claiming to be from the federal government and saying the would-be victim needed a new insurance card or Medicare card. However, before they can mail the card, they need to collect personal information. Scammers do a lot to make their requests seem credible. For example, they may have your bank's routing number and ask you to provide your account number. Or, they may ask for your credit card or Social Security number, Medicare ID, or other personal information. But sharing personal information with a scammer puts you at risk for identity theft." (One of the biggest scams in recent months and it will grow!)

OK. These are some of the biggest scams underway this spring. In coming weeks, I'll dig deeper into identity theft scams and specific tactics you can use to prevent identity theft and resulting financial fraud.

Be sure to share these with your friends and family. And pay close attention to your elderly loved ones as they are prime targets for these scams. My Mom got targeted during her senior years and, more than once, I stopped a criminal in his tracks as he was trying to steal from my Mom.

By being aware of the types of scams that are making the rounds – and understanding the psychology that makes them work – we can assist our loved ones in avoiding financial tragedy.

Have you noticed any new scams?

Have any of your friends or loved ones been victimized by a fraudster?

I'd love to hear your story. Email me at Rob@SelfRely.com

As always, be safe and secure!

Rob Douglas

Self-Reliance Institute Newsletter

Privacy:
HERE'S THE BOTTOM LINE: WE WILL NOT EVER GIVE, SELL, OR RENT YOUR INFORMATION TO ANYONE – EVER.

Questions or comments?

Please email me at Chris@SelfRely.com or call me at my Freedom Writer's Publishing office at 970-367-7624.

http://www.SelfRely.com