FALL 2019 HERSHEYS MILL FRAUD PREVENTION NEWSLETTER

A Couple of introductory notes to this issue. I will cover Fitbits at work and protecting mom and dad. While many of us Millers are retired and our parents have passed that is not true for some of us, hence the topics. Also, some of you may note that a topic from previous issues may reappear because the fraudsters may have developed new techniques.
With the housekeeping out of the way, Away We Go.

IS THE NEW INK ROLLER BETTER THAN a CROSS CUT SHREDDER?

A new company – **GUARD YOUR ID** – makes a stamp that covers your key information with blocks that prevent a dumpster diver rom reading your info. In addition, the company uses an oil-based ink that it claims won't wash off. However, some users say it washes off with rubbing alcohol. Because this product is not yet proven, stick to your shredder.

ROBOCALLS

This situation gets worse by the day. Scammers can easily spoof the caller IDs for the IRS, local police etc. The primary method to control this is the phone companies themselves. They have large databases of originating spam phone numbers and the technology to greatly reduce spoofing. Not only have they only just begun to join the battle, they are still charging monthly fees for user protection. Fortunately, the FCC seems to be ending this practice by forcing them to provide the service for free and by default. To see how important this is, realize that 9% of PA adults have been scammed by a ROBOCALL.

ALTHOUGH PRIVACY LAWS MAKE IT DIFFICULT TO DO HERE ARE SOME TIPS TO PROTECT YOUR PARENTS

Before you can help by monitoring and / or freezing their accounts they will have to agree to give you two forms signed by them'
The first is an **AUTORIZATION TO MONITOR THEIR ACCOUNTS.**
The second is a **POWER OF ATTORNEY**.
There are two potential problems here. First is the issue of trust between you and your parents.
Problem two arises if they are in some stage of dementia. In that case you may have to go to court to get the necessary powers.

IDENTITY THEFT PROTECTION

- Put a **credit freeze** on all their accounts to prevent new accounts in their name
- Review their **credit reports** to ensure that hasn't already happened
- Leave their **social security card** home and refuse to give their **SSN** out. 99% of the requesters don't need and it's an unnecessary ID theft risk. PS that goes for you too.

HOW TO ROTECT YOUR PARENTS INVESTMENTS IF YOUR PARENTS WON'T GIVE YOU AUTHORITY

- Ask them to make you a trusted contact on their accounts
- If they won't ask them to approve you to receive a duplicate statemen
- Approved or not, check the records of any financial advisor **@finra.org**

UPGRADE THEIR TECH

- Make sure all their hardware and software have the latest updates
- Make sure their home WIFI has a good password
- Consider installing a **Password Manager**

A COUPLE OF ROBOCALL SCAMS WORTH REPEATING BECAUSE PEOPLE KEEP FALLING FOR THEM

Fake IRS Call

Why does this scheme continue to work? It does what the scammers call putting the victim "under the ether." What that means is the person is so threatened by the IRS and arrest They can't think rationally.
Here are some "Ether" methods:

- TWO people on the line. Usually a man and a woman
- You owe $x in back taxes and if you don't 50% immediately you will go to jail
- The dead giveaway here is that you need to buy gift cards and read them the numbers but people "under the ether" don't think correctly.
- You are warned not tell anyone why you are buying the cards or the deal is off

Free Medical Offers

The scammer's objective here is to get your **Medicare** number. They will then use it to get medical for themselves or others, use it in another scam for fraudulent **Medicare** charges (to you) steal your financial ID.

How it Works.

The caller offers free pain management classes, free bone scans, etc. All they need to sign you up is your name, address and **Medicare** Number. What could be easier?

HOW YOUR YOUNG GRAND CHILD CAN BECOME AN ID THEFT VICTIM FOR LIFE

Despite HIPPA laws which especially protect young children, the sad fact is that many small doctor's offices (and some big ones) don't have the time, money or skill to do much about cyber security. These are juicy targets because it's not likely anyone is monitoring credit reports that they don't think a child has.
Also, in this situation the child might be able to get a new **SSN** to help prevent financial fraud, his medical info is out there permanently and he will need a credit bureau monitoring service for the rest of his life.
My suggestion would be to periodically GOOGLE your grandchild's name or perhaps try getting one of the free credit reports every four months. Hopefully, they will tell you they have no one by that name on file.

BY THE WAY, HERE'S A REMINDER FOR YOU ABOUT MEDICAL ID THEFT PREVENTION

- Monitor your Insurance benefits statements for stuff you didn't have done.

- Shred any medical documents you can. This includes **Prescription labels.**

- Never share any medical info on social media
- Your **insurance ID number** is as valuable as your **SSN.**

YOUR DIGITAL PRIVACY

Your digital privacy no longer exists. There are a lot of things that I know how to do to protect my privacy, but it just makes it harder to profile me but it doesn't prevent them from tracking me
If you'll indulge me for going beyond the scope of this newsletter, I would like to describe the situation.

FACE RECOGNITION

This technology is so cheap and so available that a bar in LA is using it place people in a que so there is no more pushing to get to the bar.
While this may be a cute use, it is much more deadly. For example the US military has a room seeking exploding drone that uses face recognition to identify the target.

However, no country has developed and implemented this like the Chinese dictatorship. Their software can recognize your face even if you have a hat sunglasses and beard. In fact, they don't even need your face. They can recognize you by how you walk which is known as **Gait Recognition.**

Now back to our regularly scheduled program.

CELL PHONES

How would you react if the government demanded that you wear an electronic ankle bracelet so they always knew where you were? I'm sure you would not accept. But you have done so voluntarily if you carry a cellphone. The GPS is great for finding things but to do that it has to know where you are. And if you install phone apps without checking they default to access to your location, your contacts and just about everything on your phone. While your carrier might make doubtful claims about protecting your privacy, many of the free apps make their money from selling

your info. Some really bad apps take screenshots of what you're looking at.

WHAT SHOULD I DO IF MY WORKPLACE OFFERS ME A FREE FITBIT WITH HEALTH MONITORING?

As always it is your decision so let's just look at the Pros and Cons:

Pros

It's free
If you are the kind of person who will ignore the readings or won't use it much the corporate monitor could be useful for your health.

Cons

Keep in mind that the data generated by the company **FITBIT** is for the company's use and is not covered by HIPPA.
There is really no way for you to know if the company will see your data so it's best to assume they will. The question then becomes how much do I trust the company.

SEARCH ENGINES - I REALLY MEAN GOOGLE

Ever notice, as I did recently when I looked a site that answered questions about COPD that my in-box was quickly flooded with ads for doctors and products for COPD? **GOGGLE** not only knows everything you look at on **GOOGLE** but pretty much any other sites you look at due to sharing arrangements.

FACEBOOK

Facebook is the worst offender of all. **GOOGLE** can piece together lots of information to target you successfully to buy their advertiser's products but **FACEBOOK** is much more insidious. **FACEBOOK** knows what you think, what you believe, what interests you and much, much more. You may wonder how they know how you will vote when you've never posted anything. Piece of cake. They know what groups you belong, who your friends, previous comments on posts, etc. In fact, **FACEBOOK** has about 5,000 data points on you. Running them through sophisticated **Artificial intelligence** programs gives them an accuracy in the upper 90%. Why do you think the political campaigns all use **FACEBOOK**. It's not to identify Republicans or Democrats because they already know that. What they are paying big bucks for is the identity of uncommitted people and WHAT WILL CONVINCE THEM TO VOTE FOR US.