

“2014: THE YEAR OF THE BREACH?” ... YOU ‘AINT SEEN NOTHING YET’



*Bill Palisano
President of Lincoln Archives*

I didn't make that title up, I've read that statement several times in various information security reports and breach reporting publications that I follow. Google

it, you'll see. We're all familiar with the Sony, the Target, the Home Depot, the 'Russian', the (fill in the blank)...Breach. (Even though Target happened in 2013, we started seeing the fallout in 2014). Hate to say it, but are we becoming desensitized about breaches? I hope not. Many of the breaches you've read about resulted in your credit card or debit accounts being compromised (aka: stolen). These types of thefts can be serious or merely a nuisance.

But there are much more serious type's of breaches which results in potentially life changing and even life ending events. We're talking theft of social security numbers and medical ID's. Welcome to 2015; here's a new, major one: The "Massive Anthem Data Breach." Hot off the presses.

Per the Pittsburgh Post-Gazette (2/25/15): "The (Anthem) breach, disclosed at the beginning of (February), resulted in the theft of personal information for 78.8 million people, including current customers and employees, and former customers and employees dating back a decade — plus as many as 18.8 million customers (or as few as 8.8 million) from affiliated Blue Cross Blue Shield health plans. Anthem,

the nation's second-largest health insurer, says hackers may have gained access to customers' names, addresses, medical IDs, Social Security numbers, birthdays, and even job and income data."

Now, why are these types of breaches/thefts comparatively worse? It's because once a thief has your social security number, he or she can effectively 'become you'. He/she can take out credit in your name, buy cars, houses, toys, you name it. This is known as 'the credit you don't know about'. After sixty days, if undisputed — you own the debt. You can dispute it, but you own it now. It's up to you to prove 'it wasn't you'. This is not a 'nuisance'. In 2013, stolen social security numbers were selling on the black market for \$3.00. Per "Finding a Cure for Medical Identity Theft" (published by CSID, October 2014, researched by Research Now), in 2014 that number dropped to \$1.00! Sickening, isn't it?

Breaches where social security numbers AND medical ID numbers are both compromised lead to the fastest growing form of identity theft: Medical Identity Theft. Medical Identity Theft includes fraudulent use of another's identity to purchase medical goods/services, prescription drugs, and defrauding medical insurance payers including Medicare/Medicaid.

Per Rick Kam, president and cofounder of ID Experts: "Essentially, criminals have come to understand that using your medical credentials—your name, Social Security Number and health insurance numbers—to order goods and services that are never delivered and to bill

organizations like Medicare and Medicaid, those activities are more profitable than drugs, prostitution, and other crimes they may pursue. For this reason, medical identities are 20 to 50 times more valuable to criminals than financial identities."

One of the greatest dangers of someone else 'becoming you' is the risk that they change your medical profile. There are many documented cases where people have died because medical profiles were changed including blood type, allergies, insulin use, medications, etc. If you are unconscious, you cannot say 'I am/am not a diabetic' 'I do/do not use insulin', 'I'm allergic to...' etc. This is a major concern.

Per the Ponemon Institute's: "5th Annual Study on Medical Identity Theft" (published February 2015, sponsored by MIFA – Medical Identity Fraud Alliance), in 2014, Medical Identity Theft increased by 21.7 %, over 2013! That is on top of a 19% increase in 2013 over 2012. The numbers are staggering. Do the math: that's a 44.8% increase in 2 years!

So what does all this mean to you? Per Ponemon's 2015 study, if you're a victim of Medical Identity Theft:

1. Only about 10% of you will achieve a satisfactory conclusion of the incident.
2. You will spend a lot of your time trying to resolve (more than 200 hours).
3. You will spend a lot of your money trying to resolve (65% of victims spent more than \$13,500).
4. Your reputation may be negatively impacted (45% of victims experienced embarrassment due to disclosure of sensitive health conditions).
5. You will probably consider changing the

continued from page 15

healthcare provider responsible for the breach (48% of victims in study reported this).

So what can you do to reduce your risk of being a victim? First and foremost, review any medical invoices mailed to you. If something doesn't make sense – investigate it right away. Periodically request (if necessary) and review any EOB (Explanation of Benefits) provided by your medical insurance provider, Medicaid or Medicare. If a collection letter for medical services is received and makes no sense, do NOT dispose of it, assuming it's a mistake. Investigate it, immediately. Protect your medical credentials – even from family (sadly, per the Study, 24% of victims had family members who stole and used theirs).

You may consider an Identity Theft Protection plan. There are many out there – some better than others. Honestly, like medical insurance, I feel that these types of plans/coverages will one day be pretty much widely used and/or necessary. Like medical insurance once was, nowadays we all have to have some form of it. So, if you consider an Identity Theft Protection plan, know exactly what the provider offers, and how much they will do for you versus what you have to do for yourself. There is a difference between identity theft 'resolution' and identity theft 'restoration'. Read the small print on their agreements.

Simply, be informed about Identity Theft and be prepared. With the Anthem Breach alone, we've started 2015 with possibly 79 million personal identities being compromised. The bad guys know there is money to be made. The good guys are trying to protect you. Do not be oblivious and do not become desensitized. Be proactive and vigilant, not a victim.

Auto Buying Privileges for **Medical Society Members & Their Families**

**Comparing your options is easy ...
with your West Herr *Select Concierge*.**

- ▶ VIP Personal Shopping Assistance with no sales pressure.
- ▶ VIP LOW *Select* Discount Pricing on new and used vehicles.
- ▶ VIP Privileges, extra incentives, special gifts, and more.

20 NEW Brands • 1,400 USED Vehicles



Make Your Vip Appointment Today!
716 - 202 - 3091

westherrSelect.com

WESTHERR Select
NEW YORK
Vehicle Purchase Plan

Personal - Commercial

