Equifax Data Breach 2017

Overview

The 2017 Equifax security failure represents the single most significant data breach ever. It by far exceeds any of the previously publicized breaches and will likely cause identity theft issues for decades.

Why?

Because Equifax is a Credit Reporting Agency (CRA), and the data exposed ties your Social Security Number, Date of Birth, and Address all together. These are the three basic requirements for identity theft.

There are five CRAs (the three major ones and two smaller ones).

Experian
TransUnion
Equifax
Innovis
ChexSystems

It does not matter that you have never done business directly with Equifax.

If you have ever had a loan, lease, insurance, paid utility bills, etc., then your information was in the hands of Equifax and the other CRAs.

Equifax claim 143 million people are affected, but they are incapable of confirming who those people are. It is therefore safer to assume that over 300 million people are affected.

Suggested Remedies.

Forget about Credit Monitoring. Credit Monitoring services are not worth the money. They do not prevent anything.

You may request a free Fraud Alert but these require renewing every 90 days. It is unclear if all five agencies will obey Fraud Alerts.

The only action which may help mitigate the impact of Equifax's criminally negligent behavior is a Credit Freeze.

But, this comes with costs, caveats, problems, not to mention the moral question of succumbing to blackmail.

Credit Freeze Costs, Caveats, Problems, Blackmail.

Costs.

Each CRA must be contacted directly to request a freeze.

The big three all charge a fee to initiate a freeze and another fee to 'thaw'. The fee varies by CRA and State of residence. The average fee is $10 per action per CRA, but can be as high as $20 in some States.

ChexSystems states it does not charge a fee. Innovis does not show a fee on their web site.

Caveats.

A Credit Freeze does not prevent someone from taking out a loan in your name by using your Social Security Number (SSN) and other compromised personal information.

It does not shield your information from everyone. Various agencies and 'approved' organizations can still access your information.

Problems.

When requesting a Credit Freeze, the CRA is supposed to issue you with a PIN.

(Unbelievably, Equifax were for a while using date and time of request as a PIN).

The Equifax 'Credit Freeze' web page has been crashing due to server overload. This has left many people unsure if the freeze request had been fully implemented.

There are reports of issues with the other CRA's web sites too when requesting a Credit Freeze.

Unfreezing (Thawing) takes longer than freezing.

You will need to Thaw your credit information with each of the five CRAs if you need to take out a new loan, change Insurers, get a new apartment etc.

On top of which, you are entrusting your PIN, no doubt tied directly to your SSN, to the CRA.

Blackmail.

Demand for money from a person in return for not revealing compromising or injurious information about that person.

Assume that I decide to start collecting YOUR personal information, with the intention of making that information available to my clients for a fee.

I am not asking for your permission. I don't need to.

But, now that I've told you what I'm doing, I will agree to block your information from some of my clients if you pay me a fee.

Note that blackmail is not about revealing embarrassing information.

Surely, revealing someone's SSN, Address, DoB, etc. is compromising and injurious to that person's financial security and stability.

Quite how the CRAs, in demanding a fee to not reveal my personal information is not Blackmail, is beyond me.

Credit Freeze Fees as a Revenue Stream.

Now that Equifax have single handedly undermined confidence in the system and massively increased everyone's exposure to fraud, what is the likely impact on revenues for the big three?

Since we can not know which SSNs have been exposed, every single person born before now will now have to deal with Credit Freeze/Unfreeze costs for the rest of their lives.

Let us assume 240 million active SSNs (excluding children, whose credit files can be locked for free).

At $10 per freeze, that is a potential windfall to each CRA of $2.4 Billion.

Assume that each year, around 120 million people need to Unfreeze/Refreeze. That's another $1.2 Billion of revenue per year, per CRA - forever.

How is this not blackmail?

It is also a hell of a motive for shoddy security at Equifax to begin with.

There should be a public demand for legislation at both the State and Federal level to outlaw Credit Freeze fees.

Moving Forward.

The False Security of a Credit Freeze.

On balance, a Credit Freeze is a Band-Aid on a massive open wound.

To begin with, we need to quit using innocuous terms like Freeze and Thaw.

Let us call it what it is. Secure and Unsecure.

The default mode in any Security System is Secure.

This should be the default mode for any CRA. They should require authorization to release personal financial information.

As noted above, as things stand one has to notify each CRA independently if one wishes to invoke a Credit Freeze (five different PINs).

Additionally, the same people who can not be trusted with your personal info to begin with, are now the custodians of the PINs. This is nuts!

The Social Security Administration, or some other competent organization, should be tasked with establishing a secure central repository. CRAs would need to check with that central repository first to verify if a Credit Freeze is in place.

Social Security Administration.

The Social Security Administration (SSA) also has a degree of culpability here.

They have used the same 9 digit system of decimal numbers since day one.

Not only are these numbers inadequate to handle future populations, some of these numbers represent year issued and region.

This is not secure. For example, it is actually possible to determine if a person is in Witness Protection, just based on their SSN and apparent age. Think about that.

In the 21st Century, SSNs need to be, at the very least, Hexadecimal or Alpha-Numeric.

Quite frankly, now that Equifax have compromised every single active SSN, the Social Security Administration needs to step up by issuing new numbers to everyone.

While they are at it, the flimsy paper card needs to be replaced with something more appropriate, such as chip on card.

And, please also note, it is insecure to require a signature on any card.

Since SSNs are so important in today's world, the SSA should have a protocol in place for issuing new SSNs in the event a person has been exposed to identity theft.

Currently, they will not do that because, as far as they are concerned, SSNs should not be used as a personal identifier. This is despite the fact that other Federal and State Agencies affirmatively use SSNs as identification.

Requesting a Person's SSN.

It really is far too easy for anyone to request a SSN.

Currently, there is no verification system of a person or entity requesting a SSN. Although this situation is unlikely to change, in a truly secure system, there would be a method of verifying the credentials of those who may request this information.

Digital Security.

Rules need to be placed upon how SSNs and related identifying data are used stored.

Yes, some rules exist for personal data. But they are not SSN specific.

SSNs should never be the database identifier and should never be placed in the same physical database with Date of Birth and Address. All data relating to SSNs should be encrypted on the server.

Yes, this makes data retrieval slower. But, when it comes to digital security, speed compromises security.

The Bottom Line.

CRAs have ruled with impunity and without oversight or control for decades. Even in the Equifax response, we see greed in place of shame and remorse.

This problem, which will absolutely be an issue for the lifetime of every person born before 2018, was caused by the same culture of arrogance that exists within each of the major Credit Reporting Agencies - and this is something which needs to be reigned in.

As far as the CRAs are concerned, you are not their customer. Their customers are financial institutions, insurance companies, etc.

You are merely their product.

When I was a kid, I worked in a retail fruit and veg store. Even as a kid in that environment, I knew I had to handle the product with care if I expected to keep my job and the boss wanted to keep his business.

These clowns have such disdain for people, they can't even grasp the simple logic behind 'Handle With Care' when it comes to their 'product'.

It is also regrettable that in the USA, television media reporting has been mostly inadequate. Print media has recognized this as a major issue, despite some the glib and ill informed 'how to repair your credit' articles.

As far as raising mass audience awareness, TV Media has a role and a responsibility.

Unfortunately, for the most part, the Equifax breach has been treated with the same 'ho hum' attitude as other important hacks.

Interestingly, the Sony hack, which in level of importance to most people is virtually zero, probably received more TV Media attention than most of the other important ones combined.

In part, this is because TV Media producers are clueless about the subject, as are many others.

There is a pervasively lax attitude when it comes to identity theft and personal information security in general.

Common misconceptions include the notion that credit monitoring is all one needs, or that some magical agency such, as a CRA, or the Social Security Administration has it all taken care of.

Nothing could be further from the truth.

Without pressure on legislators to create stronger laws and protections, coupled to a complete overhaul of the current way of doing things, nothing will change except the frequency of such data breaches.

Gary Rockley
September 2017
Austin, TX.

Let's assume you work for Equifax as a mid-level IT guy.

You just find out you got hacked. Who do you tell?

Absolute first person: Geezer in charge of IT (**Joseph Loughran**)

Who does he tell?

CEO (**Richard Smith**, AKA Rick)

Who else absolutely needs to know?

CFO (**John Gamble Jr.**).

Obviously, gotta hire some new guys to handle all the pissed off consumers. Need to tell the guy in charge of Workforce (**Rodolfo Ploder**).

These guys sold stocks & shares within five days of Equifax discovering the breach.

John Gamble Jr.	**Chief Financial Officer**
Joseph Loughran	**U.S. Information Solutions President**
Rodolfo Ploder	**Workforce Solutions President**

Ricky Boy does his umpteenth corrective apology and says "guys, we're doing all we can. We just hired 2,000 new people to handle all the calls".

Really? How do you do that in Atlanta? How do you do all the background checks needed for all those people, who will be handling sensitive info? How do you get them all Fidelity Bonded that quickly?

Answer, You Don't. It can not be done that quickly. You go to India and hire a call center crew.

So now, when people call to try to find out if they were compromised, or to get a credit freeze, the customer service rep says, "okay dear customer, please give me all that confidential info that you would have to be freakin nuts to just hand out over the phone to someone half a world away, coz I would never sell that info to someone else, even though it's worth 10 times my annual salary to a criminal."

What else does Ricky Boy say? **Free Credit Freezes for a Whole Month for Everybody!**

Wow, Ricky Boy, your generosity is just so flat out inadequate.

How about free for the next 20 years? - and you pick up the tab for credit freezes with your lame-ass fellow cartel members, TransUnion and Experian, for the next twenty years too?

Too rich for your blood, Ricky Boy?

Okay, you and your three co-conspirators will be pariahs for the rest of your lives. Just hope to your God that you never meet me or about another 280 million of the people you have insulted in person. I think we will have some choice words for you if we do.

You, sir, are an idiot - and a disgusting representation of a human being.