Equifax Data Breach May Be Largest in History - Proves CRAs Should Be Dismantled

September 8, 2017 - Equifax, one of the three primary credit reporting agencies (CRAs), has announced the company suffered a three month long data breach earlier this year. The breach exposed highly sensitive information - including names, addresses, SSNs, driver's license numbers and credit card numbers - on 143 million Americans. It may be the largest single data breach ever; covering nearly half of all Americans. And it is proof that the CRAs as they are now structured should be broken up.

We've been saying for many years that large databases containing the personally identifiable information of consumers make attractive targets for identity thieves. Because of this you might think that the CRAs would have the best data security availableâ€¦ and they may. Regardless of the circumstances behind this breach, we believe it proves our point. Large consumer databases - even when they are maintained by CRAs - are dangerous.

Not too many years ago, there were around 2,300 independent credit bureaus in the United States. These bureaus were owned by local merchants and they made it fairly simple for consumers to dispute and correct inaccurate information on their credit reports. And because they were independent, they only had access to data in their area. If all of these bureaus were still in business, a data breach on the scale of the one announced by Equifax would have been an impossibility.

But with the advent of cheap computing Equifax and the two other major players in the industry - Experian and TransUnion - have consolidated the industry. They have used a variety of tactics to do this including buying out many of the smaller bureaus and in our opinion, predatory pricing to run other credit bureaus out of business when they refused to sell to them. Less than 300 independent credit bureaus remain in business. None of this ever should have been allowed.

The Fair Credit Reporting Act requires the CRAs to accurately maintain credit reports and to adopt procedures to protect them. Section 602 of the FCRA reads, in part:
(3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.
(4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumerâ€™s right to privacy.
(b) Reasonable procedures. It is the purpose of this title to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper

utilization of such information in accordance with the requirements of this title.

This breach clearly places Equifax in violation of the FCRA. The hacked information contained in the breach means that Equifax failed to maintain the confidentiality of consumer data or insure proper use of that data. Moreover, it indicates that all of the CRAs may be incapable of complying with the law.

Equifax is attempting to control the spin placed on this data breach. As a damage control measure, the company is offering all Americans one year of free (and in our opinion, worthless) credit monitoring. But now that all of this data has been released, it is out there forever. At the very least, the company should be offering some form of protection to affected consumers for life.

Perhaps we're a bit cynical but it looks like the company is using this breach to increase the size of its credit monitoring business. Yes, the first year will be free. But how many consumers that sign up for the free service will elect to pay for the service in years to come?

The company is also attempting to limit consumers' ability to sue. Anyone signing up for the free credit monitoring offer is told that any complaints must go to binding arbitration. There is an opt-out available but it requires that you write to the company within 30 days of signing up. Bottom line here is that if you are considering taking the company up on their offer, you need to read the fine print.

It is time to force the CRAs to comply with the Fair Credit Reporting Act. Part of that requirement should entail forcing them to shut down their credit monitoring services - which only tell you that you have become a victim of fraud of identity theft after you become a victim, but which do nothing to help you clean up your credit record after victimization. Ideally, the large CRAs should be broken apart; turned into local or regional entities that would significantly reduce the size and scope of any data breach involving the CRAs.

At the state level, we urge the Attorneys General of each state to review this data breach and ensure that the company is in compliance with their state data breach notification laws. According to the Denver Post, the company only plans to make notifications to a very limited subset of affected consumers. We don't believe that this complies with most state data breach notification laws. There is absolutely no reason that Equifax shouldn't have to comply with those laws.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS