Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

The Equifax Data Breach – A Historic Data Disaster

by *Andrew L. Bareham, CPA*

Like most Americans, you probably have a credit report stored on the computers of the three main credit reporting agencies (CRA) – Equifax, Experian, and TransUnion. These credit reports show in detail your financial credit history and personal data. Starting in May of this year **Equifax's data files were breached** and the very sensitive personal information of 143 Million consumers was stolen. Listed below are some steps you can take to reduce your chance of identity theft.

- Check your three credit reports for accounts or activity you don't recognize. File a dispute for anything you believe is not accurate. You can check your credit reports for free once a year at:

https://www.annualcreditreport.com/index.action

- Considering placing a credit freeze on your files. This will make it harder for someone to open a new account in you name. Get more information and phone numbers for the CRAs from the Federal Trade Commission at:

https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

- Consider placing a fraud alert on your files. Read more about this at:

https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#difference

- File your taxes early. File as soon as you have the tax information you need, before a scammer can file as you. Many tax professionals expect an increase in tax-related identity theft this year because of Equifax. If your tax identity is stolen, it can take over a year to correct the problem.

- Protect your kids too. In Maryland parents are permitted to place a freeze on a minor child's file. You can get information at this link to one of the CRAs:

https://www.experian.com/blogs/ask-experian/requesting-a-security-freeze-for-a-minor-childs-credit-report/

- Use a service. Consumers Advocate lists the 10 best Identity Protection Services:

https://www.consumersadvocate.org/id-theft-protection/a/best-id-theft-protection?matchtype=e&keyword=credit%20protection&adpos=1t3&gclid=EAIaIQobChMI75Cb9bzI1gIVwrftCh0d-w9PEAAYAyAAEgJ-aPD_BwE

- One caution – If you enroll in Equifax's Free Identity Protection Service you may be limiting your future rights to sue Equifax.

- If you are a victim of identity theft the Federal Trade Commission has a step-by-step recovery guide at:

https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf

Data breaches have become very common. However, the Equifax breach is different because of the number of Americans impacted and sensitivity of the data that was stolen. Be safe!

Andrew L. Bareham, CPA at Bareham CPA, PA in Lutherville Maryland. Specializing in tax consulting and proactive advice for small business owners.
andrew@barehamcpa.com

Technology: What Happened?

by Jerry Stern, PC410.com

I've been asked many times "Can I be hacked?" The answer is "generally not without your help." Hackers of low-value targets (any small business) are sending you links to malware and hoping you'll click into something that installs software that will search and monitor your computer and online activity for email account logins and credit card numbers. That's pretty-well blocked by good 'antivirus' software, unless you click to let it in. Hack attempts for high-value targets, like global companies and government angencies, are custom-tailored hack attempts, and they're looking for network access to a lot more than an email account or credit card. Both of these situations are hack attempts at the level of a worker's computer.

That's not what happened at Equifax. They had unpatched software ("Apache Struts") on a web server, open and available to the outside world through their set of web sites; Apache Struts was widely-installed, with a patch available on March 7th, but not installed at Equifax. Once the patch was announced by Apache, the hackers knew where the problem was on many servers, and some time later, found that issue at Equifax, and used it to gain access to Equifax servers.

Web sites are scanned by hackers continuously for known security gaps, and that's what happened to Equifax. They didn't monitor, patch, or detect the problem, the invasion, or the downloads in a way that any other company in financial services would have. If we were their customers, we would leave, and they would be gone. That's not the case here. They sell their services to banks and other credit monitoring companies, not us. We are a commodity, not a client.

Put simply, Equifax profits from the breach. They are.offering free credit monitoring to anyone

impacted by the breach. That credit monitoring won't be free forever, although their sign-up page is not currently asking for any card numbers. BoingBoing.net estimates that if 1% of the free users continue their monitoring next year, Equifax will make an extra $200 million per year. Equifax will also receive millions from other credit monitoring companies that pay Equifax for credit reports, and from the Federal government, who pays Equifax as the exclusive provider of identification confirmation services. Here's their analysis:

https://boingboing.net/2017/10/05/failing-up-and-up.html

What To Do

Andrew Bareham has listed the financial steps above. Remember that the stolen data doesn't expire. Prevention is key; cleaning up after identity theft takes years. Freezes are less hassle than cleaning up later.

For better protection against hacks that happen on your own systems, there's a one-page document from KnowBe4.com that summarizes what you need to know about social engineering. That's the set of tricks used to convince you to click a fraudulent message. As I visit your offices, ask me for a printout. Or download it now, and share it with your employees:

https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf

---

Contact

Address all editorial and unsubscribe requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158

Phone (410) 871-2877