The Equifax Data Breach

Equifax Site Generates Phishing Error

[Update September 20]

Equifax experienced a breach in March. Apparently they did not inform anyone. From Bloomberg:

> Equifax Inc. learned about a major breach of its computer systems in March — almost five months before the date it has publicly disclosed, according to three people familiar with the situation.
>
> In a statement, the company said the March breach was not related to the hack that exposed the personal and financial data on 143 million U.S. consumers, but one of the people said the breaches involve the same intruders. Either way, the revelation that the 118-year-old credit-reporting agency suffered two major incidents in the span of a few months adds to a mounting crisis at the company, which is the subject of multiple investigations and announced the retirement of

> two of its top security executives on Friday.
>
> Equifax hired the security firm Mandiant on both occasions and may have believed it had the initial breach under control, only to have to bring the investigators back when it detected suspicious activity again on July 29, two of the people said.

Brian Krebs, among others, has noted that the vulnerability was in Apache Struts:

The Apache Struts Project Management Committee issued a lengthy statement which you can read here. But most people just want to know what the heck this application does. Here’s the short description from the project website:

Apache Struts Project Description (click for larger image)

On a lighter note, Twitterer @PlanetKingdom found this in the thicket of the Equifax website:

Equifax Recomments Netscape and IE (click for larger image)

You read that correctly. Equifax was, at least until recently, recommending Netscape and Internet Explorer. Is it still 1999? Yet another demonstration of utter incompetence.

[Original article begins here]

143 million Americans had their identities compromised in the Equifax data breach. U.S. population 20 years and older in August, 2017, was 353.5 million. **Fully 40 percent of the adult U.S. population had virtually 100 percent of their personal data stolen**. The purpose of this article is to **summarize and pull together advice from my personal experience as well as four good sources:**

Krebs on Security “Equifax Breach Response Turns Dumpster Fire”
Krebs on Security, “How I Learned to Stop Worrying and Embrace the Security Freeze”
Krebs on Security, “Breach at Equifax May Impact 143M Americans”
ArsTechnica “So Equifax Says Your Data Was Hacked. Now What?”

Here, I’ll look at three issues. First **what should you do? And — importantly — what shouldn’t you do?** Second, **what the heck happened and how has Equifax responded?** And,

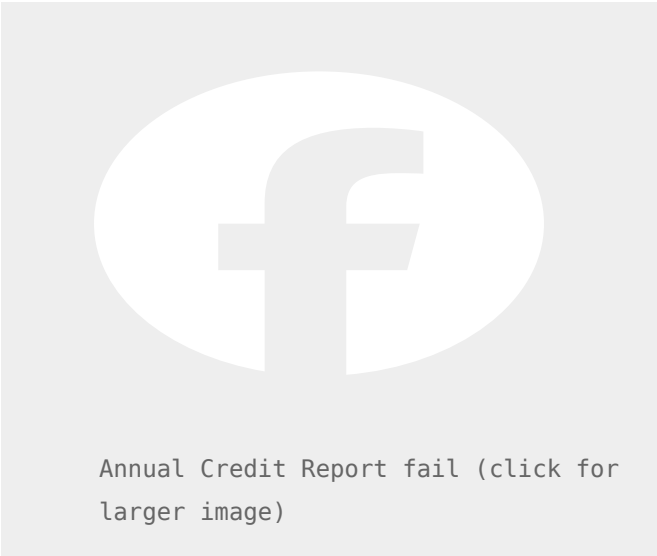
third, **why has Equifax's response been so utterly incompetent?**

What Should You Do?

Don't panic. **Yet**. First find out if you are affected. From **Krebs**:

> Equifax has set up a Web site – – that anyone concerned can visit to see if they may be impacted by the breach. The site also lets consumers enroll in TrustedID Premier, a 3-bureau credit monitoring service (Equifax, Experian and Trans Union) whichalso is operated by Equifax.
>
> According to Equifax, when you begin, you will be asked to provide your last name and the last six digits of your Social Security number. Based onthat information, you will receive a message indicating whether your personal information may have been impacted by this incident. Regardless of whether your information may have been impacted, the company says it will provide everyone the option to enroll in TrustedID Premier. The offer ends Nov. 21, 2017.

Next, **get your credit reports** from all three credit reporting agencies (Equifax, Experian, and TransUnion). You can do this fairly efficiently via . But beware. **Some of the security questions are obscure.** For example, "In which of the following years did you take out a mortgage?" Even worse, **some of the answers the site thinks are correct are wrong.** One question asked while I was trying to get a credit report for my lovely wife: "Have you ever used any of these last names?" One choice was her ex-husband's last name – which she never used. I checked "None of the above" and was promptly told I had failed the security questions and would have to call the company to get the report. Even worse, **after that the Annual Credit Report website crashed** so I couldn't get the report from the third agency.



Annual Credit Report fail (click for larger image)

My advice is to **print these reports to pdf files and put them somewhere safe.** All three have a section just below your personal information that flags any problems that may exist. If that's clear, so are you. At least for today. **Remember, a credit report is a snapshot at a point in time. The report could change ten minutes after you download it.**

Third, **take advantage of Equifax's offer of one year free enrollment in TrustIDPremier credit protection service.** You can find out whether your information was stolen here: — in fact, **there are two questions that determine whether you're a likely victim before you can proceed to the enrollment page:**

Equifax Questions to Determine Eligibility (click for larger image)

Once you enroll, you'll be given a date on which you can actually complete enrollment. As of August 9, the wait was five days. It's probably longer now. **And beware: the free protection only lasts for one year. After that, Equifax will undoubtedly try to sign you up for the paid version of this service. Reasons why anyone would do that escape me.**

Fourth, **if you don't have a Discover card, get one.** (Disclaimer: my only connection with Discover is as a satisfied customer.) Discover offers a zero-price service that will monitor thousands of risky websites as well as Experian's credit reporting. **They look for your Social Security number on those sites.** Experian is used to see if anyone is trying to obtain credit in your name. Search for Social Security Number and New Account Alerts. The link will take you here:

Discover security message (click for larger image)

Fifth, **consider freezing your credi**t. I won't go into details on this, but Krebs on Security has a great article about why you shouldn't be afraid to do this and how to proceed.

Equifax has their own special site for their security freeze.

But beware: some users report that entering a random last name and an equally random last six digits of a Social Security number is treated as a regular account with the usual response.

You may be charged a fee for each credit reporting service where you place a freeze. These fees vary by state and, perhaps, age. In California, the fee is $10 each unless you are 65 or older. In that case the fee is $5. Click here to see the complete table (downloadable pdf). State by state fees for security freeze:

Finally, **if you are a victim of identity theft, the Federal Trade Commission is the government agency acting as a clearinghouse for these reports. First, file a police report. Then visit the FTC identity theft website.**

What Happened?

Equifax screwed up bigtime. The problem began when they failed to install a security patch. Oops.

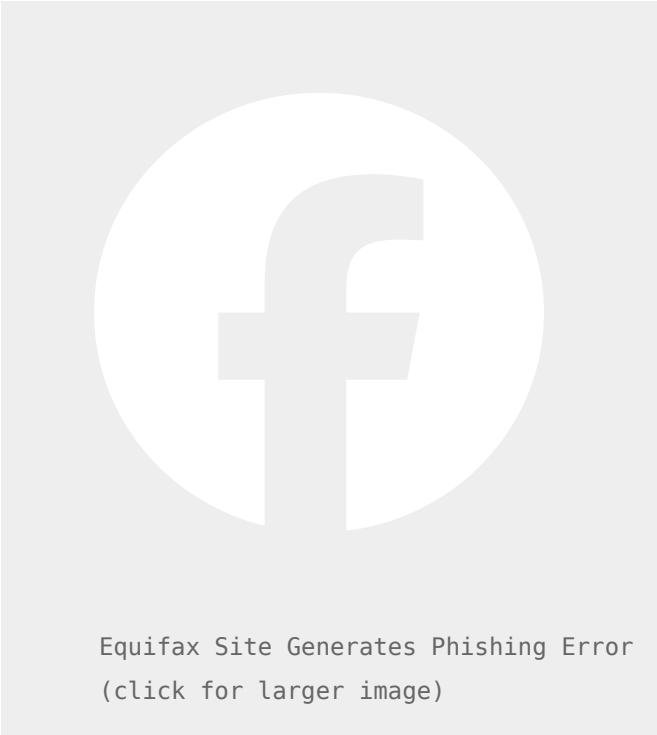
Equifax said the attackers were able to break into the company's systems by exploiting an application vulnerability to gain access to certain files. It did not say which application or which vulnerability was the source of the breach.

Here's what Krebs has to say:

> That the intruders were able to access such a large amount of sensitive consumer data via a vulnerability in the company's Web site suggests Equifax may have fallen behind in applying security updates to its Internet-facing Web applications. Although the attackers could have exploited an unknown flaw in

those applications, I would fully expect Equifax to highlight this fact if it were true – if for no other reason than doing so might make them less culpable and appear as though this was a crime which could have been perpetrated against any company running said Web applications.

The problem has now been compounded by total incompetence by Equifax management and IT people. For example, just after was opened, some browsers were giving invalid certificate errors. Users of OpenDNS were affected. It's unnerving to get this error message at that site:



Equifax Site Generates Phishing Error
(click for larger image)

Management beara a big chunk of the blame. Their former head of IT security, Susan Mauldin, has two degrees in music composition – and zero in any computer-related field.. Accompanying her out the door is former CIO David Webb. Ms. Mauldin is being scrubbed from the internet as fast as Equifax can manage it. Too bad they didn't devote the same effort to handling this data breach. Luckily the folks at Reddit did a screen grab of her Linkedin profile:

Susan Mauldin LinkedIn bio from Reddit (click for larger image)

Equifax deserves to be sued out of existence. Frankly, I hope a few executives go to jail. As Krebs puts it,

> My take on this: The credit bureaus — which make piles of money by compiling incredibly detailed dossiers on consumers and selling that information to marketers — have for the most part shown themselves to be terrible stewards of very sensitive data, and are long overdue for more oversight from regulators and lawmakers.

And the markets are already punishing them. The stock price has fallen by 1/3 since the incident:

EFX stock price from Yahoo finance

Why Has The Response Been So Incompetent?

I've already explained part of the problem: giving someone with zero qualifications a sensitive job in IT. This is similar to what happened at the Office of Personnel Management.

Incompetence starts at the top. CEO Richard F. Smith was previously an executive at General Electric. His responsibilities there had little to do with data security:

> Prior to joining Equifax, Smith spent 22 years with GE holding several president and chief executive officer roles across numerous businesses including Engineering Thermoplastics, Asset Management, Leasing, and Insurance Solutions. GE appointed Smith an officer of the company in 1999.

But there is a connection with Ms. Mauldin via the great state of Georgia. **Recall that her degrees are from the University of Georgia. Mr. Smith**:

> In May 2010, Smith was inducted into Georgia State University's J. Mack Robinson College 'Business Hall of Fame.' He was the 2013 chairman of the Atlanta Committee for Progress where he is a current board member, and also serves on the board of directors for the Commerce Club. Smith was the 2009 chairman of the Metro Atlanta Chamber of Commerce and now serves on its board of directors and executive committee. As co-chairman of the Atlanta Super Bowl Bid Committee, Smith was part of the team instrumental in Atlanta's winning bid for Super Bowl LIII in 2019.

Sounds like a bit of **quasi-nepotism.** But also **consider former CIO David Webb (emphasis added):**

> Dave Webb is chief information officer for Equifax, where he is responsible for leading a global team of IT professionals in delivering the technology strategy as well as support for the company's innovative consumer and business solutions. He joined the company in 2010.
>
> A 30-year veteran of the IT and financial services industries, Webb joined Equifax from Silicon Valley Bank, where as chief operations officer he led the company's IT strategy. He also served as a vice president at Goldman Sachs, supporting the investment and merchant banking divisions, and held technology leadership positions at Bank One and GE Capital's auto finance business.
>
> Additionally, Webb has served as a technology consultant to several large corporations in the U.S. While living in Europe, he held positions at companies servicing the oil industry, including Kestrel Data Limited, Marathon Oil UK

> Ltd., and Brown and Root Ltd.
>
> **Webb earned a bachelor’s degree in Russian from the University of London and a master’s degree in business administration from the J.L. Kellogg Graduate School of Management at Northwestern University.**

Russian and an MBA. Sounds ideal for a CIO. Experience is no substitute for education when hiring people in IT. Ah, but note that last phrase in the third paragraph: “and held technology leadership positions at Bank One and GE Capital’s auto finance business.” **Another guy from GE, Mr. Smith’s former employer. More quasi-nepotism.**

Incompetence plus hiring for sensitive positions based on who you know. If there’s a better formula for disaster, I haven’t heard about it yet.