BUSINESS › TECHNOLOGY

Clearing up confusion on the Equifax data breach, no thanks to Equifax

What the hack happened is unclear, but best to live like your personal data was stolen

Mike Stewart, The Associated Press

This July 21, 2012, photo shows Equifax Inc., offices in Atlanta. Credit monitoring company Equifax says a breach exposed social security numbers and other data from about 143 million Americans. The Atlanta-based company said Thursday, Sept. 7, 2017, that "criminals" exploited a U.S. website application to access files between mid-May and July of this year.

By **TAMARA CHUANG** | tchuang@denverpost.com | The Denver Post

PUBLISHED: September 8, 2017 at 5:55 pm | UPDATED: September 8, 2017 at 6:17 pm

Let's just go ahead and assume that some stranger now knows your Social

Security number, credit card numbers, home address and birth date.

Because even if you weren't among the 143 million consumers whose private data was potentially exposed in the Equifax Inc. breach, the person next to you probably was since it affected more than half of all U.S. adults.

The Equifax hack, which became public Thursday, angered and confused people everywhere, especially after the massive credit reporting agency apologized on Twitter saying, "Once discovered, we acted immediately to stop the intrusion." Equifax took six weeks to notify the public, which many of the 1,300 people who replied to the Tweet — including Massachusetts Sen. Elizabeth Warren — pointed out.

"The grim truth is your personal information is probably already in someone else's hands," said Tom Hegel, a senior threat researcher with ProtectWise in Denver.

> It's also outrageous that @Equifax waited so long to disclose the breach — needlessly leaving nearly half of America at risk for a month.
> — Elizabeth Warren (@SenWarren) September 8, 2017

So what happened?

Equifax tells us this much: As early as mid-May, criminals broke in through a "U.S. website application vulnerability." There's no word yet on whether this vulnerability was something simple to fix, like a Windows security update, or if hackers had found a previously undiscovered new hole and then took advantage of it before anyone noticed. The New York Post reported Friday that it was the open-source Apache STRUTS software.

Equifax, which declined to comment further, did not notice it until July 29. By then, criminals had siphoned out Social Security numbers, birth dates, addresses, driver's licenses, credit card documents and other files with personal identifying information. Most victims are in the U.S., but some live in the United Kingdom and Canada. Equifax said the delay in telling consumers was because it was investigating the breach with the help of hired cybersecurity professionals.

"Six weeks is pretty typical," to go from discovery to investigation to public disclosure, said Andrew Lewman, vice president of Denver's Owl Cybersecurity, which scrapes the darknet underworld where cyberthieves often sell stolen credit card numbers and credentials. "I think they went legal and their lawyers were trying to find out what the breach notification laws are. It would also take time to investigate how bad was the impact."

In the past, hacked companies have taken days to weeks from discovery to disclosure. Sometimes, companies don't say anything before news outlets — in particular, KrebsonSecurity.com — report on breaches.

Lewman said that if the Equifax data was encrypted, it would be much more difficult for hackers to use the personal data. But if Equifax had encrypted the data, it probably would have said so.

"The stuff that's heavily encrypted, there's little value to it. It's like I have this secret box of stuff, and trust me it's gold, not coal," said Lewman, adding that Owl is now going over its own darknet archive to see if anyone had tried to sell 143 million consumer accounts.

Fallout continued Friday as consumers found little comfort in Equifax's tool to check whether their personal data was affected. At equifaxsecurity2017.com, Equifax encourages consumers to "Check Potential Impact" by typing in a last name and the last six digits of a Social Security number.

So The Denver Post typed in "Smith" and six random digits. The result was the same information everyone was getting: "Thank You. Based on the information provided, we believe that your personal information may have been impacted by this incident."

Equifax then asks users to enroll in its identity-theft protection and credit-monitoring service for free for one year. But even that prompted confusion and outrage as some astute consumers and New York Attorney General Eric T. Schneiderman read the fine print that those who sign up for the service give up their right to sue. Schneiderman said Friday it is investigating the Equifax breach.

This language is unacceptable and unenforceable. My staff has already contacted @Equifax to demand that they remove it. https://t.co/vT0x7f5Xhc

— Eric Schneiderman (@AGSchneiderman) September 8, 2017

"They should consider themselves lucky that the General Data Protection Regulation, (which) enforces the protection of consumer privacy information, is not yet in effect," said James Carder, chief information security officer at LogRhythm in Boulder, referring to a pending European Union rule. "Otherwise, Equifax could have been looking at fines in excess of $100 million."

Still, if you tried to enroll for Equifax's free monitoring, you get a date on when to return the site. The Post's date was Nov. 12. It's also on the user to remember to return to complete enrollment.

"I cannot recall a previous data breach in which the breached company's public outreach and response has been so haphazard and ill-conceived as the one coming right now from Big 3 credit bureau Equifax," Brian Krebs, a cybersecurity reporter, wrote on his blog. "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."

TAGS: **CREDIT CARDS**, **CUSTOMER SERVICE**, **CYBERSECURITY**, **ELIZABETH WARREN**, **EQUIFAX**, **EQUIFAX BREACH**, **IDENTITY THEFT**, **LEVEL 3 COMMUNICATIONS**, **LOGRHYTHM**, **MORE BUSINESS NEWS**, **SCAMS**, **SOCIAL SECURITY**

Tamara Chuang of The Denver Post.

Tamara Chuang

Tamara Chuang covers personal technology and local tech news for The Denver Post. She loves figuring out how things work and explaining them either through words, graphics or video. Find out how to contact her at dpo.st/tamara

Follow Tamara Chuang **@gadgetress**