Equifax breach: How to protect yourself from what's coming next

By: Alex Thomas Sadler, www.clark.com

Image Credit: Dreamstime

The latest cybersecurity attack is the "worst data breach in the history of the modern era," according to money expert Clark Howard.

Equifax, one of the nation's three main credit reporting agencies, announced this week it was the victim of a major hack that exposed the personal information of 143 million U.S. consumers — or two-thirds of all Americans with credit reports.

According to Equifax, hackers exploited a security vulnerability in a U.S.-based application to gain access to consumers' personal files. The company has not yet said which application or which vulnerability was the source of the unauthorized breach.

In the world of hacks, scams and data breaches, this is about as bad as it gets.

Hackers were able to gain access to consumers' names, Social Security numbers, birth dates, addresses and, in some cases, driver's license and credit card numbers.

Anyone impacted by the breach is now at risk of identity theft and fraud — as any piece of this personal information can be sold to criminals who could then use it to open credit cards, take out loans, make purchases or even drain your bank accounts.

So what can you do?

Forget Equifax's bogus monitoring service

In its statement about the breach, Equifax announced that it's offering consumers the option to sign up for credit file monitoring and identity theft protection.

It may sound like a great offer, but the company that just exposed all of your most personal and sensitive information is now going to protect you from identity theft?

DON'T COUNT ON IT.

So how can you protect your information?

The only way to truly protect yourself is with a credit freeze.

Let's say your information was exposed and criminals do try to open new lines of credit in your name — well, they won't be able to if your credit file is frozen.

A credit freeze seals your credit reports and provides a personal identification number (PIN) that only you know and can use to temporarily "thaw" your credit when legitimate applications for credit and services need to be processed. So even if criminals try to use your info, they won't be able to actually do anything with it.

And this goes for anyone, not just those impacted directly by this breach.

How to protect your identity: Take these 2 steps

1. Sign up for Credit Karma's free credit monitoring: Go to creditkarma.com to sign up for a free account and you'll get access to free credit monitoring. If they notice any suspicious activity, you'll get an alert. Plus, Credit Karma also gives you free access to your credit scores and reports, as well as tips on what factors are impacting your credit.

2. Freeze your credit with all three main credit bureaus: By freezing your credit files, you can prevent criminals from using your information to wreak havoc on your financial life. Even if your info was not exposed by the Equifax hack, this is the best way to protect your identity and your money.

Check out our Credit Freeze Guide to learn how to freeze your credit with each main agency.

What's next: Beware of related phishing & other scams

A hack of this magnitude will undoubtedly impact millions of American consumers in some way or another.

Criminals will use every tactic they've got to take advantage of this situation. With so many Americans worried about whether their information was exposed and if they are at risk, crooks are going to tap into that fear in order to trick you into handing over your personal information.

If your information was not exposed, you still may receive a fake email, text or phone call from a criminal offering to help or asking for your information to either determine whether you were affected by the Equifax hack or to help you protect yourself.

But even if you fall for one of these scams, with a credit freeze in place, the criminals won't be able to carry out fraud in your name.

That's why setting up a credit freeze with all three credit bureaus is absolutely necessary!

This data breach extends far beyond any incident we've seen in a very long time, so it's crucial that you take steps to protect yourself.

With scams related to the hack expected to pop up everywhere, here are some tips to help you protect yourself, your money and your identity:

- Be wary of unexpected emails containing links or attachments: If you receive an unexpected email claiming to be from your bank or other company that has your personal information, don't click on any of the links or attachments. It could be a scam. Instead, log in to your account separately to check for any new notices.
- Call the company directly: If you aren't sure whether an email notice is legit, call the company directly about the information sent via email to find out if it is real and/or if there is any urgent information you should know about.
- If you do end up on a website that asks for your personal information, make sure it is a secure website, which will have "https" at the beginning ("s" indicates secure).
- Look out for grammar and spelling errors: Scam emails often contain typos and other errors — which is a big red flag that it probably didn't come from a legitimate source.
- Never respond to a text message from a number you don't recognize: This could also make any information stored in your phone vulnerable to hackers. Do some research to find out who and where the text came from.
- Don't call back unknown numbers: If you get a missed call on your cell phone from a number you don't recognize, don't call it back. Here's what you need to know about this phone scam.