In wake of Equifax breach, what to do to safeguard your info

September 8 2017, by Ken Sweet

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. (AP Photo/Mike Stewart)

There's no way around it: The news from credit reporting company Equifax that 143 million Americans had their information exposed is

very serious.

The crucial pieces of personal information that criminals may need to commit identity theft—Social Security numbers, birthdates, address histories, legal names—were all obtained. And once your personal data is out there, it's basically out there forever.

Unlike previous breaches at Yahoo, Target and Home Depot, Equifax's role in the financial industry makes this breach far more alarming. The company is basically a storehouse of Americans' most personal credit information, knowing everything about people from when they opened their first credit card, to how much money they owe on their houses, to whether they have any court judgments against them.

Lenders rely on the information collected by the credit bureaus to help them decide whether to approve financing for homes, cars and credit cards. Credit checks are even sometimes done by employers when deciding whom to hire for a job.

Atlanta-based Equifax, one of three major U.S. credit bureaus, said Thursday that "criminals" exploited a U.S. website application to access files between mid-May and July of this year. Equifax discovered the hack July 29, but waited until Thursday to warn consumers.

For consumers, it may be time to take even more extreme measures to lock down their information, outside of the routine advice like checking your credit reports regularly and seeing if there are any abnormal transactions on your bank accounts and credit cards.

The strongest possible option a person can take immediately is placing what's known as a credit freeze on their credit files with the major credit bureaus—Equifax, TransUnion and Experian. A credit freeze locks down a person's information, making it impossible to open new accounts

and bank cards in their name. But locking your credit also locks you out from opening new accounts as well.

"The credit freeze is the nuclear option of credit protection. But in the wake of a breach this big, it's worth considering," said Matt Schulz, an analyst with CreditCards.com.

Consumers will need to be even more diligent about checking their credit reports. U.S. law gives every American the right to pull their credit reports for free once a year from the major credit bureaus. It's best to spread those requests out over the year—do one every four months, experts say.

There are a lot of websites that market access to your credit reports, but the official one is annualcreditreport.com

Expect to check this information not just in the immediate future, but for the long term—potentially years. Once your personal data is out there, it can be used at any time.

"Bad guys can be very patient with data. This should be a wake-up call to be even more diligent with your information," Schulz said.

An even more extreme step? People can request to change their Social Security number with the Social Security Administration if they have repeatedly been a victim of identity fraud under their original number.

This isn't the biggest data breach in history. That indignity still belongs to Yahoo, which was targeted in at least two separate digital burglaries that affected more than 1 billion of its users' accounts throughout the world.

But no Social Security numbers or drivers' license information were

disclosed in the Yahoo break-in.

Equifax's security lapse could be the largest theft involving Social Security numbers, one of the most common methods used to confirm a person's identity in the U.S. It eclipses a 2015 hack at health insurer Anthem Inc. that involved the Social Security numbers of about 80 million people.

Any data breach threatens to tarnish a company's reputation, but it is especially mortifying for Equifax, whose entire business revolves around providing a clear financial profile of consumers that lenders and other businesses can trust.

In addition to the personal information stolen in its breach, Equifax said the credit card numbers for about 209,000 U.S. consumers were also taken, as were "certain dispute documents" containing personal information for approximately 182,000 U.S. individuals.

Equifax has established a website, www.equifaxsecurity2017.com/ , where people can check to see if their personal information may have been stolen. Consumers can also call 866-447-7559 for more information.

The company warned that hackers also may have some "limited personal information" about British and Canadian residents. The company doesn't believe that consumers from any other countries were affected.

Three Equifax executives sold shares worth a combined $1.8 million just a few days after the company discovered it had been hacked, according to documents filed with securities regulators. Equifax said the three executives "had no knowledge that an intrusion had occurred at the time they sold their shares."

Equifax shares fell about 13 percent to $123.75 in heavy trading. The decline equates to about $2.28 billion in lost market value.