The Equifax Data Breach: Where Do We Go From Here?

It is becoming an all-too-common event, each occurrence seeming to grow in scale and impact. The Equifax data breach is just the latest in a long history of such violations that have affected consumers as well as businesses.

Regardless of whether your personal information has been breached or not, incidents like this are becoming more common and they will likely continue to occur.

Data Breaches in Perspective

Several industry sources have documented data breaches affecting U.S. consumers since 2005. This, they say, is due largely to the fact that the volume of data available online has been growing exponentially year after year since around that time, giving cyber criminals the opportunity to expose ever-increasing amounts of data in a single breach.

Indeed, over that past decade the number and severity of breaches has grown steadily. For instance, according to Statista, an organization that compiles data on breaches, 157 such instances were reported in 2005, with 66.9 million records exposed. In 2014, the number of breaches reported ballooned to 783, with at least 85.61 million total records exposed -- an increase of nearly 500% in the number of breaches.[1]

Fast forward to September 2017 and the Equifax breach. It is estimated that the credit reporting agency's cyberattack affected some 143 million people -- nearly half of all Americans -- exposing crucial identifying information such as Social Security numbers, addresses, birth dates, driver's license numbers, and, in some cases, credit card numbers.

The hack -- and what many critics believe was Equifax's belated and botched response to it -- have angered many and prompted lawmakers and regulators to take a close look at what happened, how it happened, and ways to help mitigate the potential impact that some believe will continue to play out for years to come.

The Potential Economic Fallout

What makes this data breach different from other large-scale attacks? The potential economic impact it could have on the financial industry. Some experts believe that if consumers opt to make their credit reports and the information they contain off limits by default via a credit freeze -- which is the first line of defense being promoted by cybersecurity analysts (see "What to Do Now" below) -- such a change in behavior could disrupt the flow of credit and have a host of potential implications for consumers and the financial institutions that lend money to them.

The Aftermath

Nearly a month after the Equifax announcement, the situation continues to evolve. Key executives, including the chief executive officer, have resigned. Following intense public criticism for its customer service -- specifically its process for helping consumers determine whether their personal information had been violated and what to do if it had -- the company has announced that it would allow consumers to freeze and unfreeze their credit information at no charge for life, starting next year. Company officials will face congressional lawmakers on Capitol Hill who are expected to push for new, stronger data security standards in the form of data breach legislation.

What to Do Now

Regardless of whether your personal information has been breached or not, incidents like this are becoming more common and they will likely continue to occur. While it's true that there is only so much you can do to protect your personal information and identity (the rest is up to the companies that house your information), you owe it to yourself to do your part to keep your personal data personal.

Here are some steps that experts in cybersecurity/identity theft recommend you take now:

- Place a freeze on your Equifax credit report. A credit freeze will lock your credit files so that only companies you currently do business with can access them. In this way a freeze is designed to prevent someone other than yourself from applying for credit in your name. As mentioned earlier, Equifax is offering free freeze/unfreeze services for life starting in 2018. Log on to the Equifax site and follow the instructions to learn if your personal information has been impacted and to sign up for free credit monitoring features.
- To be safe, consider placing freezes on your credit reports with the other two credit reporting agencies -- Experian and TransUnion. (Fees and restrictions may apply.)
- Use fraud alerts. You can also go directly to each of the three reporting agencies and request that a free fraud alert be put on one or more accounts. Fraud alerts notify you if someone has accessed or tried to access your account without your permission. Consider putting fraud alerts on your credit and debit cards as well.
- Check your credit reports. Make a habit of checking your credit reports at least once a year -- and much more frequently if you fear any of your accounts may have been involved in a security breach. Each of the three credit reporting agencies provides a free annual report. Just go to annualcreditreport.com to request your free reports.

[1]DigitalGuardian.com, "The History of Data Breaches," July 27, 2017.