1/18/18

By Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America

On January 2, 2018 security company McAfee released the results of a survey revealing that consumers are worried about protecting their personal information. Of course they are! Not a week goes by without news about another data breach or an Internet-connected device that that's been spying on unsuspecting consumers. Forty-three percent of those surveyed feel that they don't have control over the information about them that companies collect and use. That's correct – for the most part they don't. More than half were either unsure or had no idea how to check to see if their connected devices and apps are secured. That's correct – for the most part they can't. And 63 percent said that their biggest worry about their wireless home network being hacked is that they may become identity theft victims. These concerns are real.

So what's the solution? McAfee recommended that consumers protect themselves by reviewing their accounts online regularly to spot fraudulent charges and debits (something that an impressive two-thirds of the survey respondents said they already do), talking to their children about online safety starting at an early age, and considering using an identity theft protection service. Not coincidentally, a week after releasing the survey McAfee announced that it was going to sell its own identity theft services.

To be fair, McAfee wasn't saying that subscribing to an identity theft service would keep your home network safe. It won't. But it's important to understand that while an identity theft service can alert you to some fraudulent uses of your personal information and help you resolve problems that may result, it's after the fact. These services don't give you control over who collects your information, how it's used, or how secure it is, and they can't prevent it from being stolen.

We recently released tips for consumers about how to make it harder for fraudsters to use their personal information, including placing security freezes on their credit reports to block certain types of fraud, an option that we think should be available for everyone free of charge. There's a limit to what consumers can do, however. In the case of the Equifax breach, the victims didn't even *give* their data to the company in the first place, and they certainly weren't responsible for the company's failure to fix the security flaw that hackers exploited.

Now groups representing many banks, retailers and tech companies are urging Congress to enact legislation to protect consumers' data and notify them about breaches in a timely manner. But as commenters have pointed out, they want a weak law *and* they want to block the states from enforcing their own, stronger consumer protections. They'd like to have a "flexible standard for data protection" that factors in things like the size of the company and the cost of security.

What about the costs of data insecurity? Anxious consumers are spending hundreds of dollars on identity theft services, and millions are also being spent by employers, companies and government agencies to provide these services to data breach victims. Wouldn't it make more sense to invest in better data security in the first place? And what about the emotional toll that data breaches have on consumers? If your Social Security number has been stolen, you can't stop it being sold on the "dark web," you can't change it, and you can't predict how it will be abused, let alone prevent it. A cloud of dread will be hanging over your head forever.

These industry groups also want it to be left to the companies that have data breaches to decide whether to notify those affected based on how likely they think it that identity theft or financial harm will result. Apparently we should be worried that companies "are not burdened by excessive requirements" for security and breach notice but not about the burden on consumers to deal with the fallout from lax security.

There are bills in Congress that would actually help. Senator Elizabeth Warren recently introduced legislation that would create an Office of Cybersecurity at the Federal Trade

Commission to see to it that credit reporting agencies such as Experian take adequate security measures. It would impose stiff penalties for breaches at credit reporting agencies and require them to provide compensation to consumers if their data are stolen. CFA also supports Senator Patrick Leahy's Consumer Privacy Protection Act and other efforts by lawmakers to make those who hold our personal information accountable for safeguarding it. That's the solution that we really need, not a national data breach law that would weaken, rather than strengthen, the incentive to take data security seriously.