This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/the-capital-one-hack-life-in-the-time-of-breach-fatigue-11564824600

MARKETS

The Capital One Hack: Life in the Time of Breach Fatigue

What weary consumers should be doing to protect their data

By Julia Carpenter and Bourree Lam
Updated Aug. 4, 2019 3:49 pm ET

Chase Erwin has made credit monitoring a key part of his nightly routine.

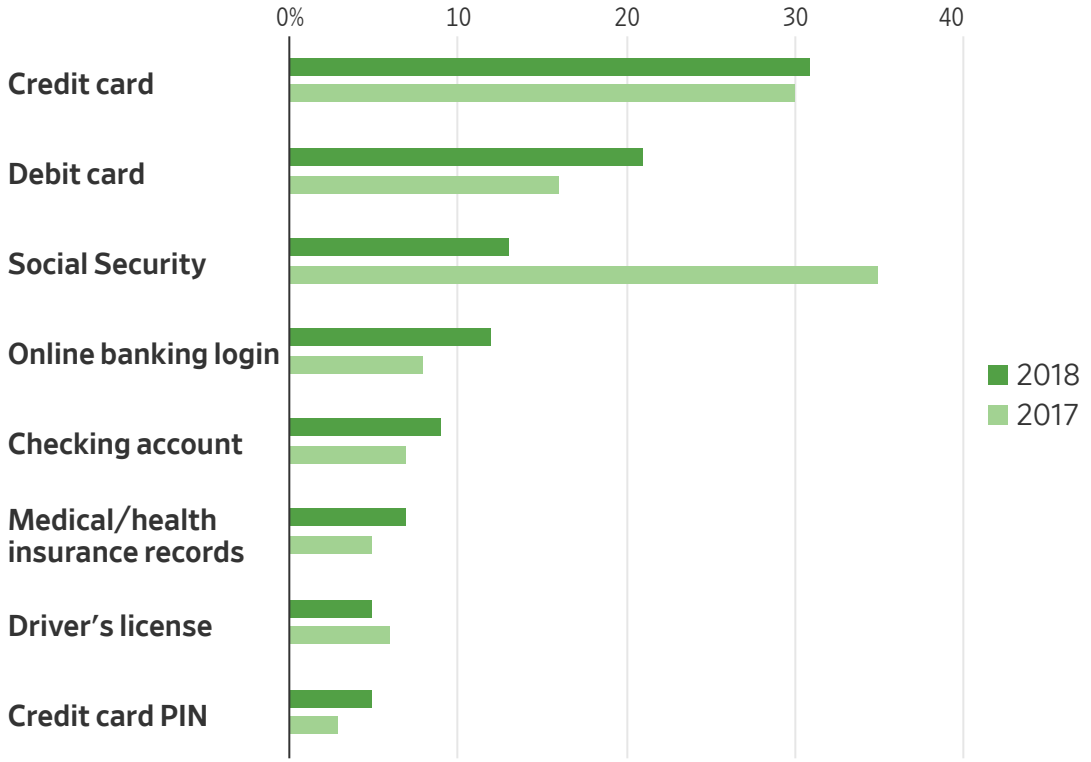
He comes home from work, opens his computer and methodically checks all his bank and credit-card statements. Living in a time of data breaches, he says, means he has to do a lot of the work himself.

"Basically, I can do a better job of maintaining my security than clearly Equifax or Capital One can," he said.

The Data Is Out There

Sensitive information about consumers is often compromised in data breaches.

Types of Data Compromised in Data Breaches



Source: Javelin Strategy & Research, 2019

Mr. Erwin isn't alone in feeling he has to do what he can, given the little control consumers have over the exposure of personal information in large-scale data breaches and hacks in recent years. He was one of the nearly 150 million consumers affected by the 2017 Equifax breach, and he said while he doesn't know if his information was compromised by other recent hacks— Target, Home Depot and most recently Capital One, among others—he said he wouldn't be surprised to find his name, bank account number, address or even his Social Security number out there on the internet.

"You hear about these data breaches over and over and over again," he said. "It's a fact of life."

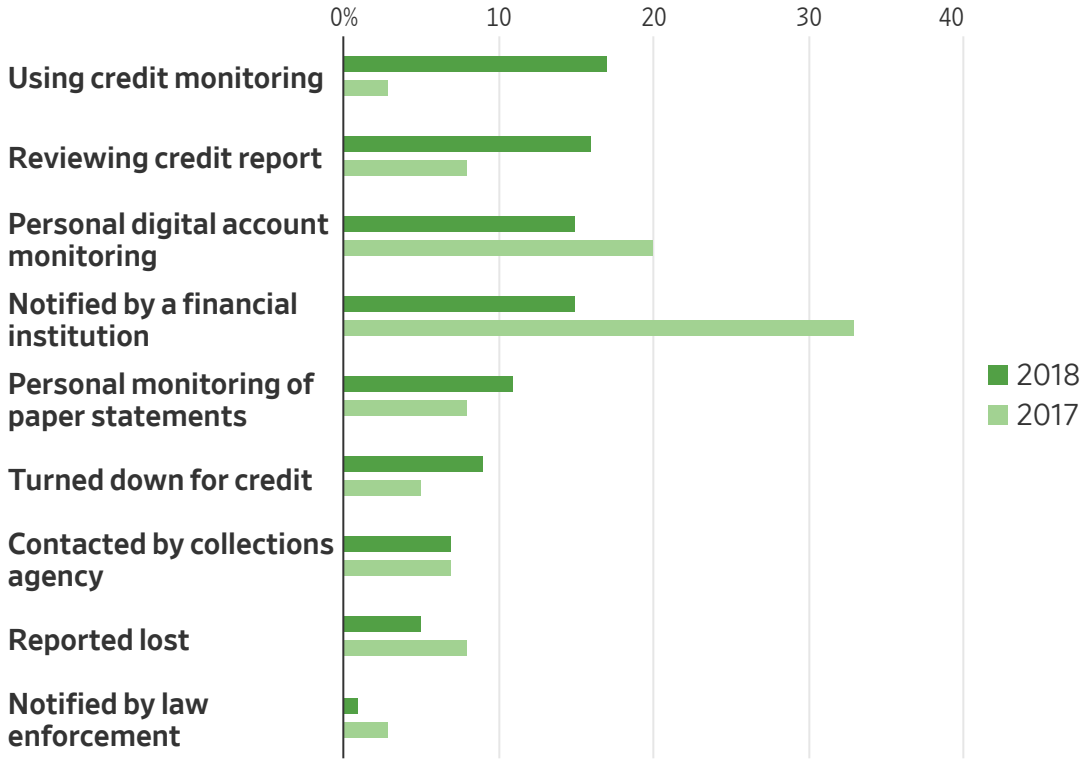
These days, when data breaches occur, the Federal Trade Commission and firms usually offer a set playbook: Freeze your credit, place a fraud alert, get credit monitoring and change your passwords.

This recent wave of data breaches reminded Mr. Erwin and others of an unfortunate lesson learned from hack after hack: When it comes to protecting your data online, a routine is a good thing.

Fraud Alert

How consumers discover their identity has been stolen

Means of detecting new account fraud



Source: Javelin Strategy & Research, 2019

Eva Velasquez, president of the Identity Theft Resource Center, a nonprofit that supports victims of identity theft and fraud, said it is important for consumers to do something themselves.

“I don’t want people to be in that point of breach fatigue,” said Ms. Velasquez. Even just doing one of the recommended steps, she said, is better than nothing.

“Not every thief has every piece of your data. There are still things that you can do that can make a difference. If your Social Security number has been compromised

four times, and you haven't done a credit freeze, you are low-hanging fruit."

Mr. Erwin's approach is common for those who fear that data breaches will lead to identity theft.

According to 2016 data compiled by the Justice Department, 85% of the estimated 26 million identity-theft victims in the U.S. that year saw the attempted misuse of a credit card or bank account. The Bureau of Justice Statistics started including in 2008 a question about data breaches in its identity-theft supplement, which is part of its National Crime Victimization Survey.

"The genie is really out of the bottle," said M. Eric Johnson, dean of Vanderbilt University's Owen Graduate School of Management, who researches information and data risk. "I think pretty much every American has had their data exposed now at some time or another."

Mr. Johnson said he does see some people becoming apathetic in the face of these breaches. Part of that, he said, is just the nonstop nature of these attacks—no one hack is ever the last hack.

According to research ITRC compiled, while the number of breach incidents in 2018 has decreased from 2017 by 23%, the number of people having personal information compromised has increased by 126%.

Having herself been part of many data breaches, Ms. Velasquez said it is important to take action yourself, despite the feeling that another data breach is inevitable.

For Mr. Erwin, this means a hypervigilant nightly routine, which he considers one of the few safeguards protecting his personal financial data.

"I decided long ago that it's up to me to notice these things," Mr. Erwin said. "If I can't trust Equifax to do their own job, I'm not going to hand them my money and say, 'Hey, watch this for me.' "

SHARE YOUR THOUGHTS

What do you do when you find out you've been affected by a data breach? Join the discussion below.

Write to Julia Carpenter at julia.carpenter@wsj.com and Bourree Lam at bourree.lam@wsj.com

Copyright © 2022 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.