The New York Times | http://nyti.ms/1Soaozn

Edited by David Leonhardt

The Upshot

Stolen Consumer Data Is a Smaller Problem Than It Seems

JULY 31, 2015

Economic View

By NATHANIEL POPPER

At Target, 40 million customers had their credit card information exposed to hackers. At JPMorgan Chase, personal details associated with 80 million accounts were leaked. Last month, a hacker gained access to 4.5 million records from the University of California, Los Angeles, health system.

Enormous numbers like these can make it feel as if we're living through an epidemic of data breaches, in which no one's bank account or credit card is safe. But the actual effect on consumers is quite different from what the headlines suggest. Only a tiny number of people exposed by leaks end up paying any costs, and for the rare victims who do, the average cost has actually been falling steadily.

How could that be? For starters, several laws protect consumers from bearing almost any financial losses related to hackers (though not the headaches of having to enter new credit card numbers into Amazon and elsewhere). Instead, banks and merchants, like Target, must bear the cost. But even their losses have been dropping in recent years, as data security experts have learned new strategies to prevent intrusions from turning into theft.

"The bad guys are getting good," said David Robertson, the publisher of The

Nilson Report, a data provider for the card industry, “and the good guys are getting even better.”

It’s true that data breaches, particularly those in which Social Security numbers are compromised, can lead to a more devastating sort of identity theft, in which criminals open new financial accounts in a person’s name and do damage that can take years and a lot of work to clean up. But consumers are almost never on the hook for financial losses in these sorts of episodes, which, by the way, have also been on the decline.

This relatively sanguine picture of the impact of data breaches is an example of a threat that looks worse than it turns out to be. The sheer size of hackings shocks and startles when the attacks are first reported, but it’s rare that journalists check on the actual consequences.

Moreover, consumer fears can be stoked by the incentives of the people providing the data. Many of the statistics on identity fraud and online attacks come from security firms that want more people to buy their services. It’s not so different from the soap company that advertises how many different types of bacteria are on a subway pole without mentioning how unlikely it is that any of those bacteria would make you sick.

One of the most memorable statistics on identity fraud comes from advertisements that say a new victim is created every two seconds. That figure, which comes from Javelin Strategy and Research, is largely attributable to standard credit card fraud, in which criminals use a stolen credit card number to buy goods — not the sort of thing most people imagine when they think of identity fraud. The more troubling identity theft, in which new accounts are opened in an unsuspecting person’s name, make up only 5 percent of the total figure given by Javelin.

These statistics do not mean that data security is not a real issue for authorities and consumers to think about. Even if the hackers don’t use your credit cards, there are instances in which leaked data of other kinds can be damaging in itself, as was clear in the recent episodes at Sony Pictures and Ashley Madison, the website that connects prospective adulterers. There are also serious geopolitical concerns about foreign hackers compromising national security if they get a hold of

military maps or staff lists from the C.I.A.

For the companies and banks that bear the cost of stolen credit card numbers, the expenses are very real. Criminals racked up $7.8 billion in fraudulent purchases last year, with banks paying 62 percent of that amount and merchants the rest, according to The Nilson Report.

The banks, though, have managed to curtail their costs as they have devised new methods to detect fraudulent purchases. The most prevalent strategy involves looking for patterns in card purchases, but some banks have even taken to buying stolen cards on the black market to identify breaches, security experts say.

In the aftermath of the Target breach, in late 2013, the American Bankers Association said that the biggest expense for the banks was not the fraud but rather the cost of reissuing the cards and dealing with concerned customers.

For JPMorgan, the costs after the 2014 intrusion were much more limited because the attackers took only email addresses and phone numbers, the type of information that is not hard to attain through other, legal channels.

Consumer advocates generally say that the most important thing to pay attention to after a data breach is the type of information stolen. Karen Barney, a program director at the Identity Theft Resource Center, said that to commit true identity theft, hackers generally need to get a hold of Social Security numbers.

“Social Security numbers are the be-all and end-all for successful attempts at identity theft,” Ms. Barney said.

While those nine-digit identifiers weren’t made vulnerable in any of the big data leaks at retailers, they were exposed in this month’s intrusion at U.C.L.A.’s health system and in the recent break-in at the federal government’s Office of Personnel Management.

To prevent fraud in the first place, banks are currently introducing cards with so-called E.M.V. chips, which make counterfeiting cards — currently the most prevalent sort of fraud — much more difficult.

Though serious identity theft has been on the decline in recent years, many

security experts are expecting that to change as dedicated criminals, whose easy counterfeiting is foiled by E.M.V. chips, start to focus on getting Social Security numbers and other data that enables them to open new accounts, said Mr. Robertson, of The Nilson Report.

"For the bad guys, your five-year growth plan is not data breaches and stealing credit cards," Mr. Robertson said. "It involves stealing all the info you can and opening legitimate accounts in people's names."

Ultimately, the problem will still require businesses, and individuals, to stop the thefts from happening in the first place.

The Upshot provides news, analysis and graphics about politics, policy and everyday life. Follow us on Facebook and Twitter. Sign up for our weekly newsletter.

A version of this article appears in print on August 2, 2015, on page BU6 of the New York edition with the headline: A Hacking Epidemic That Hits Few Consumers in the Wallet .