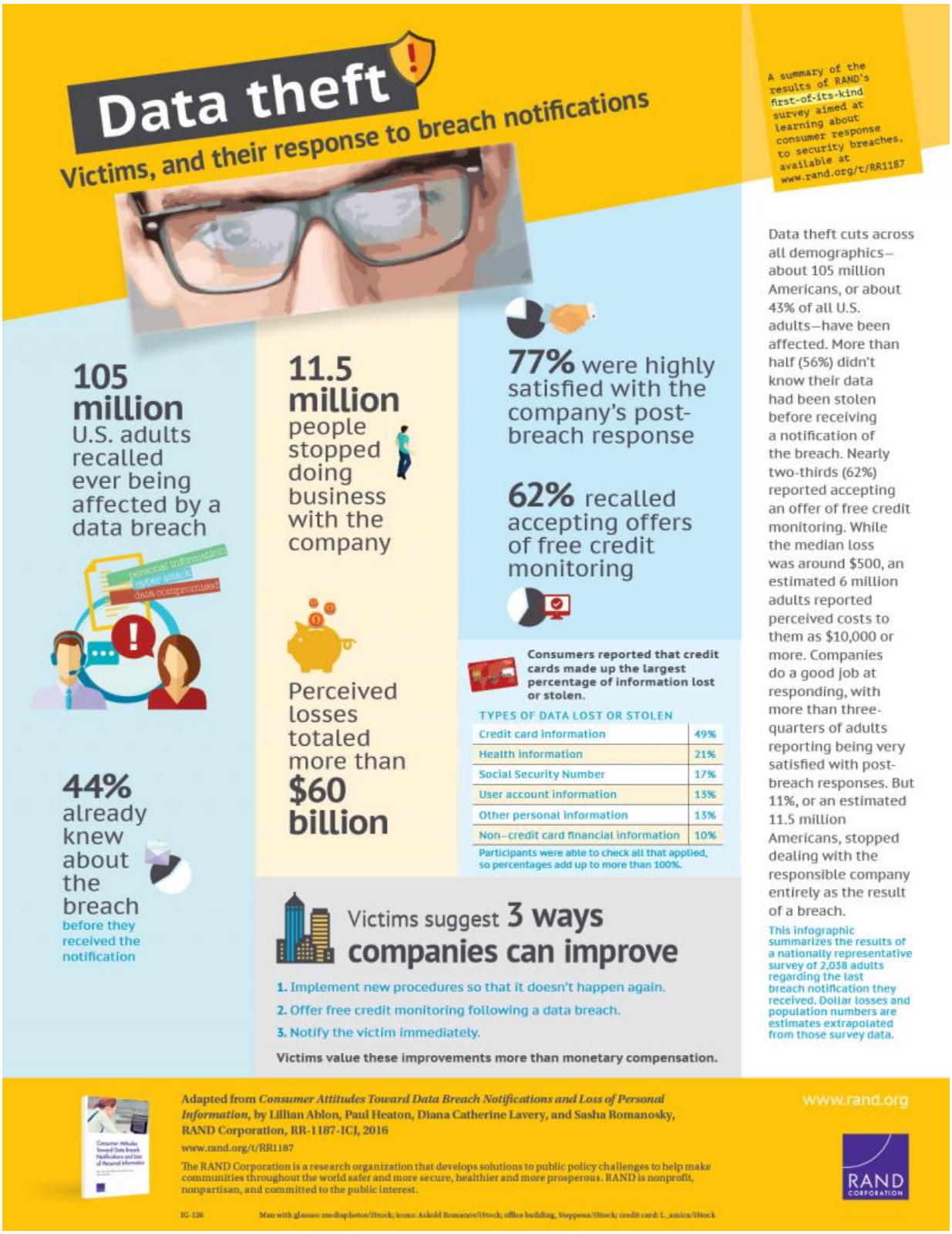
Few consumers penalize companies after data breach, study finds

April 14 2016



The first survey of consumers' attitude toward data breaches shows few quit

doing business with a company after their information is hacked. Credit: RAND Corp.

About a quarter of American adults reported that they were notified about their personal information being part of a data breach in the previous year, but only 11 percent of those who have ever been notified say they stopped doing business with the hacked company after the event occurred, according to a new RAND Corporation study.

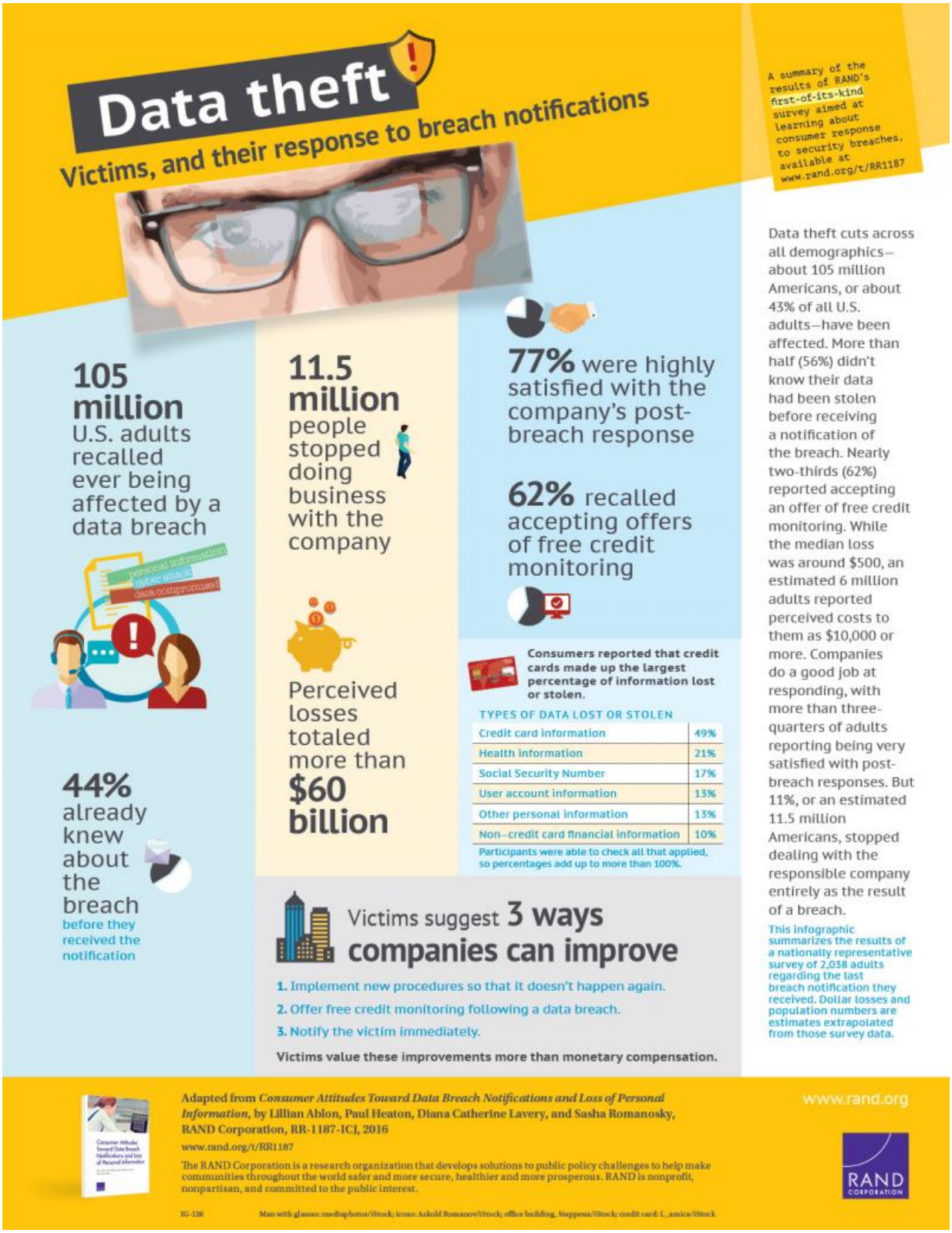
The findings are from one of the first examinations of consumers' experiences with data breaches and the impact it has on their relationships with the companies that lose their personal information.

"While data breaches have become an alarmingly common part of American life, most people appear satisfied with companies' responses to data breaches and few decide to take their business elsewhere," said lead author Lillian Ablon, a cybersecurity and emerging technologies researcher at RAND, a nonprofit research organization. "It's unclear whether this response will induce companies to improve their breach notification practices."

The RAND survey found that among those who remembered receiving a data breach notification at any time over their lifetime, about 44 percent said they were aware of the hack even before they received notification. About 10 percent discovered the breach by identifying suspicious activity themselves.

Surprisingly, 62 percent of consumers reported they accepted offers of free credit monitoring. This counters claims made by others that consumers are experiencing "breach fatigue"—where consumers become desensitized to the notices and either discount them or ignore important

information contained in the notices.



The first survey of consumers' attitudes toward data breaches shows that few quit doing business with a company after personal information is hacked. Credit: RAND Corp.

The three main reasons for declining such offers were the time and effort required to register for the service, concerns about the hacked company or the breach notification service, and whether the offer duplicated services the victim already had.

More than three-quarters of those surveyed (77 percent) said they were highly satisfied with the company's post-breach response. However, ethnic minorities were less likely to report being satisfied with the company's breach response, placed a higher dollar value on the inconvenience caused by the breach and were more likely to cease doing business with the related company.

"Our research shows the importance of legislation that requires companies to notify individuals when a breach occurs," Ablon said. "Data breach notification laws empower consumers to take quick action to reduce risk and create incentives for companies to improve data security. Unfortunately, data breach laws are not uniform or even present for every state."

While most states have laws requiring that consumers be notified of data breaches, three states—Alabama, New Mexico and South Dakota—have no such legislation. Survey participants in those three states reported lower rates of having ever received a data breach notice as compared to people from states with notification laws, although the difference was not statistically significant.

The survey questioned a nationally representative sample of 2,038 adults who participate in the RAND American Life Panel, an Internet-based survey panel.

The survey was fielded between May 15 and June 1, 2015, and designed to provide a snapshot of the frequency of breach notifications and the types of data compromised, as well as consumer reactions to the breach, the notification process and the affected company. The survey also examined estimates regarding the perceived personal cost of the breach, as well as suggestions regarding future notifications and data protection measures.

Among those experiencing a data breach during their lifetime, people with higher income and those with more education were more likely to recall being notified of a breach, as compared to younger adults (ages 18-34) and senior citizens (ages 65 and older). More than 12 percent of those surveyed received two or more notifications in the year preceding the survey.

Ablon said the low proportion of consumers who penalized a company for a data breach may highlight that while a consumer always can to choose to shop at another retailer, it is more difficult to make a switch when a data breach hits a person's health insurer, mortgage company or employer.

Among survey participants who estimated a dollar-equivalent cost for the inconvenience caused by a data breach, the median amount was $500. Thirty-two percent felt the breach imposed no dollar loss to them. Median dollar values were higher if health information ($1,000), social security numbers ($1,000) or other financial information ($864) was compromised. Just under 6 percent of those who had ever received a data breach notification (or an estimated 6 million U.S. adults) felt that the inconvenience cost them $10,000 or more. Of those who

experienced an extreme inconvenience, the breach typically involved credit card or health information.

Respondents recommended several steps companies could take to better protect personal information. The steps that would highly satisfy most respondents included taking measures to ensure a similar breach cannot occur in the future, offering free credit monitoring to make sure lost data is not misused and notifying consumers immediately. All three were valued more highly than receiving compensation for financial loss or an apology from the company.

More information: The study, "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information," can be found at www.rand.org

Provided by RAND Corporation