


Few consumers penalize companies after data breach, study finds

April 14 2016


Data theft

Victims, and their response to breach notifications


A summary of the results of RAND's first-of-its-kind survey aimed at learning about consumer response to security breaches, available at www.rand.org/t/RR1187




105 million U.S. adults recalled ever being affected by a data breach




11.5 million people stopped doing business with the company



77% were highly satisfied with the company's post-breach response



62% recalled accepting offers of free credit monitoring




Consumers reported that credit cards made up the largest percentage of information lost or stolen.


TYPES OF DATA LOST OR STOLEN	
Credit card information	49%
Health information	21%
Social Security Number	17%
User account information	15%
Other personal information	13%
Non-credit card financial information	10%

Participants were able to check all that applied, so percentages add up to more than 100%.

Perceived losses totaled more than **\$60 billion**



44% already knew about the breach before they received the notification



Victims suggest **3 ways** companies can improve

1. Implement new procedures so that it doesn't happen again.
2. Offer free credit monitoring following a data breach.
3. Notify the victim immediately.


Victims value these improvements more than monetary compensation.

This infographic summarizes the results of a nationally representative survey of 2,038 adults regarding the last breach notification they received. Dollar losses and population numbers are estimates extrapolated from those survey data.

Adapted from *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, by Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, RAND Corporation, RR-1187-1CJ, 2016
www.rand.org/t/RR1187

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

www.rand.org



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.

Data theft

Victims, and their response to breach notifications

A summary of the results of RAND's first-of-its-kind survey aimed at learning about consumer response to security breaches. available at www.rand.org/t/RR1187

105 million U.S. adults recalled ever being affected by a data breach

11.5 million people stopped doing business with the company

77% were highly satisfied with the company's post-breach response

62% recalled accepting offers of free credit monitoring

44% already knew about the breach before they received the notification

Perceived losses totaled more than **\$60 billion**

Consumers reported that credit cards made up the largest percentage of information lost or stolen.

TYPES OF DATA LOST OR STOLEN	
Credit card information	49%
Health information	21%
Social Security Number	17%
User account information	13%
Other personal information	13%
Non-credit card financial information	10%

Participants were able to check all that applied, so percentages add up to more than 100%.

Victims suggest **3 ways** companies can improve

1. Implement new procedures so that it doesn't happen again.
2. Offer free credit monitoring following a data breach.
3. Notify the victim immediately.

Victims value these improvements more than monetary compensation.

Data theft cuts across all demographics—about 105 million Americans, or about 43% of all U.S. adults—have been affected. More than half (56%) didn't know their data had been stolen before receiving a notification of the breach. Nearly two-thirds (62%) reported accepting an offer of free credit monitoring. While the median loss was around \$500, an estimated 6 million adults reported perceived costs to them as \$10,000 or more. Companies do a good job at responding, with more than three-quarters of adults reporting being very satisfied with post-breach responses. But 11%, or an estimated 11.5 million Americans, stopped dealing with the responsible company entirely as the result of a breach.

This infographic summarizes the results of a nationally representative survey of 2,038 adults regarding the last breach notification they received. Dollar losses and population numbers are estimates extrapolated from those survey data.

Adapted from *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, by Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, RAND Corporation, RR-1187-ICJ, 2016 www.rand.org/t/RR1187

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

IC-128 Man with glasses: me@aphotos/Stock; icons: Askold Romanov/Stock; office building: Steppens/Stock; credit card: C. amira/Stock

www.rand.org

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

Citation: Few consumers penalize companies after data breach, study finds (2016, April 14) retrieved 3 May 2024 from <https://phys.org/news/2016-04-consumers-penalize-companies-breach.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.