AUTHENTICATION • CALL VERIFICATION

nextcaller

2018 REPORT: BRAND TRUST IN THE AGE OF THE DATA BREACH

www.nextcaller.com

INTRODUCTION

The Identity Theft Resource Center (ITRC) reports that there were **over 1500 data breaches** in 2017, **up 45% from 2016**. These breaches led to nearly 180 million records being exposed -- many of which contained highly sensitive PII (personally identifiable information).

With the frequency and scope of breaches increasing at an alarming rate, the team at Next Caller decided to gauge the toll it's taking on the American consumer. To do so, we commissioned a study to examine the impact fraud is having on consumer trust of businesses and institutions. We surveyed 500 U.S. respondents aged 18+ and weighted for the U.S. population by age, region and gender.

WAITING FOR THE OTHER SHOE TO DROP

Ponemon Institute estimates a **27% probability** that a U.S. company will experience a breach in the next 24 months that will cost them **between $1.1M and $3.8M**. Our findings show that the majority of consumers share this concern:

51% of consumers report they are confident that breaches similar to those in 2017 will occur in 2018.

THE TOLL ON TRUST

The vast majority of consumers (80%) report that the particular way the affected organizations responded to the breaches in 2017 makes them less trustworthy. With Equifax sitting on their knowledge that the data of more than 145 million Americans had been compromised for over a month, this is not surprising.

Also not surprising is the fact that millennials (ages 25-34) have the least amount of trust in these organizations. Eighty-five (85%) report that they view the affected organization as less trustworthy. This falls in line with millennials' higher expectations for transparency amongst their brands of choice.

The way companies responded to their breaches in 2017 makes them less trustworthy:

80%	85%
Overall	Millennials

IT’S ALL ABOUT **THE RESPONSE**

Sixty-one percent (61%) of respondents report that they would not drop a business just because it was breached, but rather would make the decision based upon how the company handled the situation. This illustrates just how commonplace breaches and hacks have become -- especially for those who have grown up online. Millennials seem to be the most forgiving, with 69% saying a company’s reaction to the breach impacts their decision more than whether the breach happened at all.

WOULD YOU CONTINUE DOING BUSINESS WITH A COMPANY AFTER A BREACH?

OVERALL 61% YES

MILLENNIALS 69% YES

Interestingly, those between the ages of 45-54 were the most likely (39%) to say “No” they wouldn’t continue doing business with a company if it became a victim of a breach or hack. Perhaps with retirement in sight this group may have a lower appetite for risk when it comes to doing business with companies that may be vulnerable to breaches and exposing their personal or financial information.

Older generations might also view a data breach as a breach of trust, whereas younger generations have accepted the inevitability of breaches and base their judgments on what hacked businesses still have control over - their response.

LACK OF CONFIDENCE IN COMPANY SECURITY

Across the board, confidence in businesses taking the right steps to protect consumer information is down:

57% **Percentage of consumers NOT confident that the companies they do business with are taking the necessary steps to protect their information.**

Interestingly, this coincides with Edelman's findings that the United States showed the steepest decline in public trust in their institutions (Government, Business, Media & NGO) amongst all other countries that were polled.

Fraudulent data breaches within which industry are most concerning?

8%	**20%**	**59%**	**8%**	**6%**
Retail & eComm	Government	Banking & Finance	Healthcare	Social Media & Tech

All industries stand to gain ground with customers by taking proactive measures to improve security in 2018. However, the overwhelming majority of consumers (59%) are most concerned with the Banking & Finance industry, where trust has eroded following security breaches at prominent institutions like the Securities and Exchange Commission. Financial institutions that manage to strengthen security while improving customer experience are sure to pleasantly surprise consumers who are expecting the worst.

Social media was the industry of least concern. Not surprisingly, digitally savvy GenZ made up the majority of respondents that chose it as their top concern. Social media companies that strike the balance between security and experience have an opportunity to capture the trust and loyalty of a new generation of consumers.

CONCLUSION

Companies are working quickly to strengthen their defenses. This year, global security spending is set to reach **$96 billion.**

At the same time, experts predict that by 2020, customer experience will be regarded by consumers as the top brand differentiator--beyond price or product quality.

52% of consumers anticipate that stronger security defenses will impact their customer experience negatively.

In this Age of the Data Breach, consumers are understandably anxious about their PII being exposed. Higher fraud incident rates and the mishandling of corporate responses to breaches have only exacerbated the negative sentiment expressed by consumers.

While balancing security with customer experience presents a significant challenge, businesses that proactively respond to this challenge stand to gain long-lasting rewards. Particularly in the phone channel, reliable ANI matching before the caller reaches a live agent is paramount. Identity corroboration in the IVR has become vital because it protects businesses from bad actors that fatally compromise the policies and procedures designed to give customers the seamless experience they deserve.

METHODOLOGY

To supplement its own institutional knowledge and personal expertise in the fraud protection space, Next Caller commissioned a Google Survey “Next Caller Trust Report” of a sampling that is accurately representative of the current U.S. population, with a root mean square error (RMSE) of 5.3%.

RMSE is a weighted average of the difference between the predicted population sample (CPS) and the actual sample (Google). The lower the number, the smaller the overall sample bias.

nextcaller

46 Lispenard street, Suite #1E
New York, NY 10013

P: 1-844-698-2255
E: info@nextcaller.com
W: www.nextcaller.com