



2018 CONSUMER SURVEY:

# **ATTITUDES AND BEHAVIOR IN A POST-BREACH ERA**





# INTRODUCTION

We are living in a world where breaches of consumer privacy are a regular phenomenon. Breaches, such as the Cambridge Analytica-Facebook snafu and the Google+ leak, have dominated headlines in 2018, exposing the personal information of millions of people and shaking our trust in big brands. Many consumers are making drastic changes to the way they interact with brands online, and they believe businesses need to take ultimate responsibility for protecting their data. Ping Identity surveyed more than 3,000 consumers across the U.S., UK, France and Germany to examine consumer attitudes in a post-breach era to help businesses maintain trust and stay ahead of their customers' expectations.

## KEY FINDINGS

- **One in five people (21%) have been victims of a breach.** Of that segment, 34% experienced financial loss.
- **Following a data breach, 78% of people would stop engaging with a brand online.** Furthermore, nearly half (49%) would not sign up and use an online service or application that recently experienced a data breach.
- **More than half of consumers (56%) are not willing to pay *anything* to application or online service providers for added security** to protect their personal information.
- **59% prioritize the protection of their personal information when interacting with an online application or service,** compared to only 12% who prioritize a convenient, straightforward user experience and 7% who prioritize a personalized user interface.

# BREACH IMPACT

## KEY TAKEAWAY

The vast majority of respondents would stop engaging with a brand after a breach, and value security above all else. More than half of those surveyed take *no action* to secure their personal data after a breach, suggesting consumers feel security is a corporate responsibility rather than a personal one.

## SUPPORTING DATA

- **One in five (21%) have been victims of a breach.** Of that segment, 34% experienced financial loss and 41% of that pool lost between \$300-\$999.
- **78% of people would stop engaging with a brand online** (and 36% would stop engaging with a brand altogether) if it had recently been breached.
- **Nearly half (49%) would not sign up for an online service or app that recently experienced a data breach.** More than one third (37%) would use an online service that had recently been breached only if they had no other way of getting the service provided.
- **47% of people have made changes to the way they secure their personal data** as a result of recent data breaches (while 53% have taken no action). See Figure 1 & 2 below.

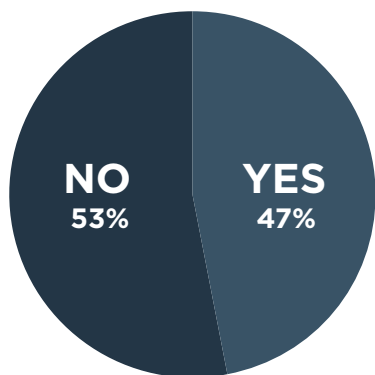


Figure 1

### BY BREAK (% YES)

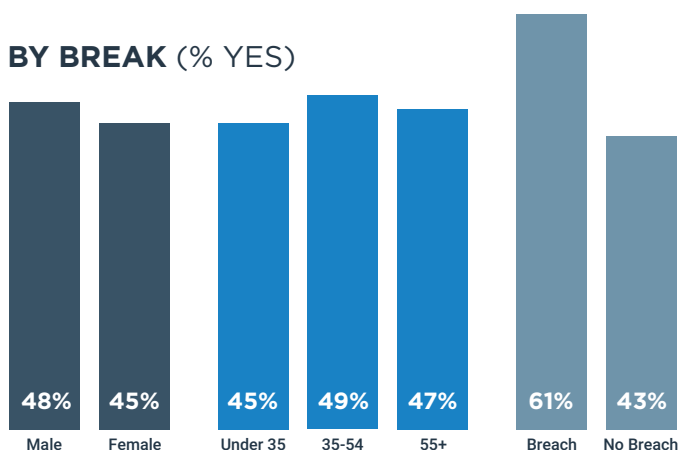


Figure 2

- **54% of people are more concerned with protecting their personal information today than they were a year ago** (vs. 2% who are less concerned and 44% who say they feel no differently now than a year ago).
- **More than a quarter (28%) plan to change how they use social platforms** to log in after the Cambridge Analytica disclosure. One third (32%) are not changing their use of social platforms to log in after the Facebook/Cambridge Analytica admission.

# WHO'S RESPONSIBLE

## KEY TAKEAWAY

Most respondents believe it's a brand's obligation to protect their privacy, and are not willing to pay extra for the protection of their personal data. While the majority of those surveyed don't want to pay anything to online service/app providers for added security, only one quarter are willing to pay a small cost. When compared with the amount people are willing to pay to generally ensure their personal information is never breached (i.e., not necessarily to online service and app providers), willingness to invest is slightly higher.

## SUPPORTING DATA

- **More than half (56%) of respondents are not willing to pay anything to app and online service providers for added security to protect their personal information;** another quarter (24%) are not willing to pay more than \$5, and 2% are willing to pay more than \$20. See *Figure 3*.

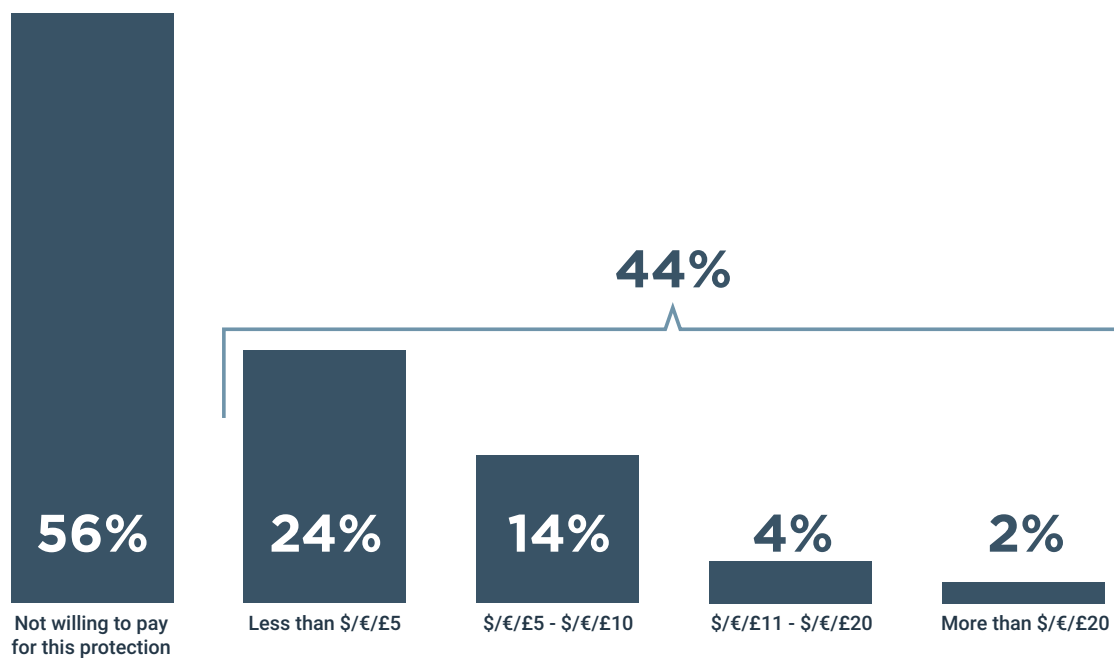


Figure 3

- **48% of people are not willing to pay anything** to ensure that their personal information will never be breached; 38% are willing to pay up to \$49.

# SECURITY VS. USER EXPERIENCE

## KEY TAKEAWAY

Consumers say they value security over a personalized, convenient user experience when dealing with brands, but growing numbers are choosing to sign in to websites via their social media accounts. The value of speed and convenience cannot be underestimated when it comes to the login process, while security is prioritized when interacting with brands.

## SUPPORTING DATA

- **59% prioritize the protection of their identity and/or personal information when interacting with an online application or service;** 12% prioritize a convenient, straightforward user experience and 7% prioritize a personalized user interface (22% prioritize cost [free vs. paid service]). See Figure 4.

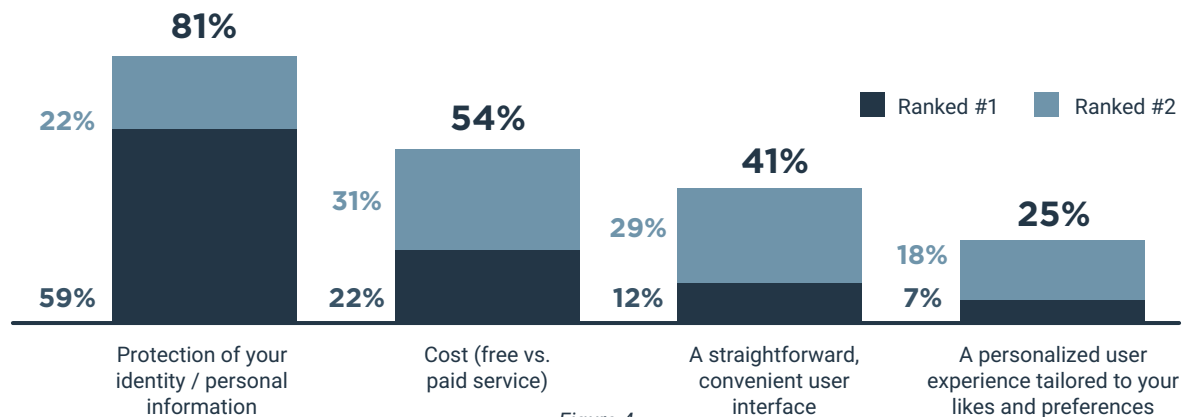


Figure 4

- **Username and password remains the primary sign-in method for 70% of people.** 13% of respondents use social sign-in as their primary login method. Of those who log in through their social sign-in, 84% do so because it is more convenient (40%) or saves them time (44%).

### Thumbprint and Facial Recognition Get a Thumbs Up but Most are Still Hands-off



Emerging technologies like thumbprint and facial recognition as a means of logging in are steadily increasing in popularity, but we are still a long way from a passwordless reality. It starts with educating consumers on the benefits and advantages of biometric login.

- 51% believe login tech like thumbprint and facial recognition are more secure than usernames and passwords. (40% think they are equally secure.) Only 10% of people use biometric tech (thumbprint and facial recognition) as their primary login method – likely because this is an emerging tech that is not offered by the majority of platforms.



# SPOTLIGHT: BREAKDOWN BY AGE

## UNDER 35

## OVER 55



### Trust in brands is relatively high

- **53% feel confident** or very confident in online service and application providers' ability to protect their personal information.

### Trust in brands is relatively low

- **Only 27% feel confident** or very confident in online service and application providers' ability to protect their personal information.



### More carefree with their sensitive personal information

- **54% are willing to input their bank information** on a website or app.

### Guard their sensitive personal information more carefully

- **41% are willing to input their bank information** on a website or app.



### More likely to experience a financial loss as a result of a data breach

- **41% experienced a financial loss** as a result of a breach.

### Less likely to experience a financial loss as a result of a data breach

- **27% experienced a financial loss** as a result of a breach.



### More likely to spend more to ensure their personal information is protected

- **42% are not willing to pay more** to online services/apps for added security to protect their personal information.
- **37% are not willing to pay anything** to ensure their personal information is never breached.
- **42% are willing to pay between \$1-49** to ensure their personal information is never breached.

### Less likely to invest extra to ensure their personal information is protected

- **75% are not willing to pay more** to online services/apps for added security to protect their personal information.
- **62% are not willing to pay anything** to ensure their personal information is never breached.
- **32% are willing to pay between \$1-49** to ensure their personal information is never breached.



### Following Cambridge Analytica, Facebook Connect is losing substantial portions of users — of all ages

- **37% will abstain from using Facebook Connect** to log in to online services and apps. While not as high as the older generation, Facebook Connect will still lose one third of this customer base.

### Following Cambridge Analytica, Facebook Connect is losing substantial portions of users — of all ages

- **56% will abstain from using Facebook Connect** to log in to online services and apps.



### More open when it comes to biometrics adoption

- **46% use biometrics like thumbprint or facial recognition** to sign in to online services and apps.

### Less open when it comes to biometrics adoption

- **13% use biometrics like thumbprint or facial recognition** to sign in to online services and apps.

# SPOTLIGHT: BREAKDOWN BY COUNTRY



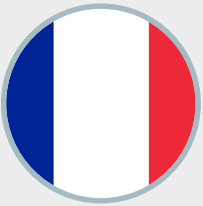
## Over-sharers:

More likely to share their sensitive information with brands than those in other countries, including:

- Social security number (16% U.S., vs. 9% France, 6% Germany, 4% UK)
- Credit card info (40% U.S., vs. 36% France, 26% UK, 13% Germany)

## Big spenders — on services, not security:

- Americans spend money on online services and apps (e.g., Spotify, Netflix, etc.) at higher rates than other countries (62% spend money on services/apps in U.S., vs. 53% UK, 49% Germany, 47% France).
- Americans are the most willing to pay to ensure that their personal information is never breached (64% U.S., vs. 54% Germany, 46% UK, 40% France). *\*corrected stat*



## Trust is low:

- The French are the least confident in online services and app providers' ability to protect personal information. (Only 34% are confident/very confident in providers vs. 48% U.S., 48% UK, 42% Germany). *\*corrected stat*



## Least likely to be breached:

- UK residents (15%) are less likely to have experienced a breach than those in the U.S. (27%), France (21%) or Germany (17%). However, of those who have experienced a breach, 42% experienced a financial loss as a result (vs. 24% in U.S., 38% in Germany and 43% in France).

## Unwilling to pay more for security:

- People in the UK are the least willing to pay more to online services/apps for added security to protect their personal information (64%) vs. those from France (61%), Germany (52%) and U.S. (48%).



## Abandoning Facebook Connect:

- Germans take a harder stance when it comes to making modifications following Cambridge Analytica. 50% will no longer use Facebook Connect to log in to online services and apps as a result of the revelation (compared with 42% U.S., 41% France and 39% UK).



# CONCLUSION

Data breaches and privacy issues are more pervasive than ever, and brands are at risk of losing consumers' trust—and ultimately their business—if security isn't at the core of their operations. With the majority of people unwilling to pay for added security to protect their online identity, companies must protect them by default. In the same way that brands are expected to provide personalized, user-friendly experiences, they must understand the value and importance of strong identity management strategies and show consumers what they are doing to keep their online identities safe.

To learn more about how identity and access management can help you protect your customers' personal data, visit [pingidentity.com](https://pingidentity.com).

## METHODOLOGY

Ping Identity commissioned MarketCube to conduct a survey of 3,264 consumers in the United States, United Kingdom, France and Germany who are at least 18 years old and use at least one of these online sites or services: shopping, banking, movie/TV, music, government services, travel or Uber/Lyft-type apps. Additionally, respondents must have entered at least one of the following on a website or app in the past 12 months: address, date of birth, phone number, credit card number, bank information, social security number or driver's license number. The geographic breakdown of survey respondents is as follows: U.S. - 1,004; UK - 753; France - 754; Germany - 753. The survey was conducted online between May 21 and May 25, 2018. The margin of error is plus or minus 1.7 percentage points.