

## Centrify Consumer Trust Survey

### *The Corporate Cost of Compromised Credentials*

#### Methodology

This survey was conducted online, reaching N=800 adults in the US, N=800 adults in the UK, and N=800 adults in Germany. The surveys were conducted in late February and early March of 2016. In order to ensure a representative sample, the data in each country were weighted slightly by region, gender, income, and age. A random sample of N=800 respondents has a margin of error of about +/- 3.5% for the full sample. The margin of error is higher for subgroups within each sample.

#### Key Findings

##### *Perceptions of How Different Industries Handle Hacking*

- Credit cards/banks/financial institutions have the best reputation on dealing with hacks relative to other industries. Around four-in-five in each country rank them 1<sup>st</sup>, 2<sup>nd</sup>, or 3<sup>rd</sup> of seven different industries in terms of how they handle hacking. Older adults are especially likely to say these organizations do the best job.
- Medical and health organizations are a clear second place of the seven industries tested in the US (66% rank as 1<sup>st</sup>, 2<sup>nd</sup>, or 3<sup>rd</sup>) and third in the UK (68%) and Germany (64%) in terms of handling hacking.
- Faith in the government to take responsibility for hacks is higher in the UK (74% rank as 1<sup>st</sup>, 2<sup>nd</sup>, or 3<sup>rd</sup>) and Germany (72%) compared to the US (62%).
- Outside of financial institutions, health organizations, and the government, there is less relative faith for retail businesses (ranking 4<sup>th</sup> of 7 in each country) and travel sites (5<sup>th</sup> of 7 in each country).
- Membership and hospitality businesses were by far ranked as the worst. About half in the US and Germany, and close to two-thirds in the UK, ranked these as either worst or second-worst of the seven industries tested.

##### *Accepting a Culture of Occasional Hacks*

- To some degree, most adults accept hacking as inevitable. About three-quarters say it is probably or definitely normal and expected for businesses and large organizations to be hacked. However, relatively few say this is definitely normal (21% in the US, 13% in the UK, 16% in Germany.)

- However, just because adults consider this normal does not mean they are letting businesses off the hook. Fully 66% of adults in the US, 75% in the UK, and 57% in Germany say they are at least somewhat likely to stop doing business after a hack. This includes 21% in the US, 23% in the UK, and 17% in Germany who are *very likely* to stop doing business after a hack.
- Those who would be most likely to switch tend to be those who are most knowledgeable or directly experienced – such as those who have had their personal information compromised in a hack, those who are the most tech savvy, and those who do more shopping online.
- Additionally, most believe that the burden of responsibility for hacks rests almost entirely on the businesses. About two-thirds in each country rate corporations as a 9 or 10 on a 10-point scale in terms of how responsible they should be for any hacks. Significant percentages say that corporations are not taking enough responsibility (41% in the US, 50% in the UK, 38% in Germany.)

### *The Aftermath of a Hack*

- After a hack, customers/members were most likely to be asked to monitor bank transactions and change passwords (and most followed through.) They were considerably less likely to set up any kind of alerts, conduct a security freeze, or implement multi-factor authentication. Older adults were more likely to follow through on the monitoring of accounts and changing of passwords, while younger adults were more likely to follow through on all other methods.
- While the vast majority (between 86% and 91%) were at least somewhat satisfied with the handling of these hacks by the businesses and organizations, fewer were very satisfied (47% in the US, 38% in the UK, 31% in Germany.) This hints at the fact that, while there is some degree of acceptance that these sorts of things are inevitable, companies have room to go from good to great in terms of how they respond to these circumstances.

### *Vulnerable Customer Information*

- People are most fearful of their credit cards or bank statements being hacked. This was the most likely to be ranked 1<sup>st</sup>, 2<sup>nd</sup>, or 3<sup>rd</sup> of 8 in each country (78% ranking in top 3 in US, 85% UK, 78% Germany) in terms of fear that the information could be compromised.
- Older adults were significantly more likely to rank this as #1. Those over 65 were +17 points more likely in the US, +19 points more likely in the UK, and +19 points more likely in Germany to rank this as #1 compared to those under the age of 30.
- Financial investment information (58% in the US, 56% in the UK, 43% in Germany), health and medical records (46%, 45%, 48%), and family information (44%, 41%, 43%) are also more likely to be ranked in the top three in terms of concerns about hacks.
- Criminal history, web browsing history, and dating profile information are the least concerning with regards to potential hacks. This is likely because significant percentages of people may not

have a criminal record, a dating profile, or a web browsing history of which they are embarrassed.

### *Online Security Behavior*

- Consumers are increasingly vulnerable given their current digital consumption habits. Over half (and in the UK, two-thirds) do most or all of their banking online, and about one-third (or one-quarter in Germany) do most or all of their shopping online.
- Consumers do not change their passwords often. Only a quarter of those in the US change their passwords at least once a month (more than in any other country). On the infrequent side, one-quarter of Americans and over one-third of those in the UK and Germany say they change their passwords once a year, less, or never. Frequent password changes are more common among those who have had their personal info hacked in the past and those who tend to do more online shopping.
- Most adults indicate that they would invest some time in completing security measure tasks or steps. Germans have the highest tolerance for this, with over half (52%) expressing a willingness to spend more than 10 minutes on this. This is also true for 30% in the UK and 46% in the US.
- Half or more select a fingerprint ID as one of the top two security measures they would be comfortable using. The alphanumeric password, the four digit password, and the voice ID follow. People are much less likely to select the graphic password, GPS locator, or ability to shut down or erase data remotely as something with which they would be comfortable.

**Centrify Topline**  
**Online Survey among 800 adults in the US, UK and Germany**  
**February/March 2016**

*Overall Sample* ..... N=2,400  
*US* ..... N=800  
*UK* ..... N=800  
*Germany* ..... N=800

1. To the best of your knowledge, has a business or organization ever **notified** you, as the customer/member, that they were hacked?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Yes – business customer of.....	32	20	14
Yes – organization member of.....	6	7	4
Yes – both .....	13	7	7
No .....	49	67	75

2. **IF YES TO PREVIOUS QUESTION, ASK:** After you were notified, did you find out that your personal information (eg address, credit card information, etc) was in fact compromised or hacked? (N=873)

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Yes.....	52	45	53
No .....	48	55	47

3. From the following list, please indicate if the business or organization asked you to take any of these actions/steps after they notified you – and indicate if you actually followed through on taking that action/step. (N=873)

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Change your password – Yes, asked .....	59	67	71
Change your password – Yes, took action .....	53	63	65
Change passwords on other sites/accounts– Yes, asked.....	48	48	54
Change passwords on other sites/accounts– Yes, took action.....	36	41	47
Implement multi-factor authentication – Yes, asked .....	20	13	12
Implement multi-factor authentication – Yes, took action.....	15	9	6
Carefully monitor all bank account transactions – Yes, asked.....	61	55	46
Carefully monitor bank account transactions–Yes, took action...54	54	45	36
Set up text/email alerts of any unusual activity – Yes, asked.....	33	20	20
Set up text/email alerts of unusual activity – Yes, took action.....	23	12	9
Request a fraud alert – Yes, asked .....	33	23	22
Request a fraud alert – Yes, took action .....	24	15	10
Consider a security freeze – Yes, asked .....	21	14	17
Consider a security freeze – Yes, took action .....	14	9	6

4. After you were notified, how satisfied were you with the business or organization’s response to the situation? (N=873)

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Very satisfied .....	47	38	31
Somewhat satisfied.....	44	49	55
Not too satisfied .....	8	10	12
Not satisfied at all .....	1	3	2

5. Instead of finding out from the business or organization itself, have you ever found out that a business or organization which holds your personal data has been hacked via one of the following:

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Story on the news/in the newspapers.....	59	55	53
On social media.....	23	19	18
From friends/family .....	24	15	25
Other.....	14	23	16

6. Compared to 2015, do you believe you are more likely to be hacked this year?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Yes, definitely.....	17	11	12
Yes, probably .....	36	48	44
Probably not .....	41	37	41
Definitely not .....	6	4	4

7. In your opinion, do you believe it has become normal/expected for businesses and large organizations to be hacked?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Yes, definitely.....	21	13	16
Yes, probably .....	51	60	57
Probably not .....	20	20	22
Definitely not .....	7	6	4

8. How likely would you be to leave/switch from doing business (or cancel a membership) with an organization if you found out they were hacked?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Very likely .....	21	23	17
Somewhat likely.....	45	52	40
Somewhat unlikely.....	29	23	39
Very unlikely .....	5	3	5

9. Using a scale from zero to 10, with zero meaning “no responsibility” and 10 meaning “complete responsibility”, how much responsibility do you believe businesses and large organizations should be taking to secure their customers/members data or personal information?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
0, no responsibility.....	1	0	0
1.....	0	0	0
2.....	0	0	1
3.....	0	0	0
4.....	0	0	0
5.....	6	6	7
6.....	5	4	3
7.....	9	7	9
8.....	16	15	18
9.....	18	16	16
10, complete responsibility.....	45	52	46

10. Based on your rating in the previous question, do you believe that businesses and large organizations **ARE** taking enough responsibility for the security of their customers/members personal information?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Yes, definitely.....	15	7	14
Yes, probably .....	44	44	48
Probably not .....	35	41	34
Definitely not .....	6	9	4

11. Using a scale from zero to 10, with zero meaning “not a priority at all” and 10 meaning “highest priority”, how much of a priority do you believe businesses and large organizations are placing on keeping their customers/members data or personal information secure?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
0, not a priority at all .....	1	1	1
1.....	1	0	0
2.....	1	1	1
3.....	2	2	2
4.....	3	3	4
5.....	10	11	14
6.....	11	11	11
7.....	17	20	20
8.....	21	21	20
9.....	15	13	12
10, highest priority.....	19	16	14

12. Please rank the following types of businesses, organizations, or services in terms of how well you would think they handle security issues for their customers and members. Please give a 1 to the business or organization you believe would handle these issues the best and a 7 to the business or organization you think handles these situation the worst.

	<i>US</i>	<i>UK</i>	<i>Germany</i>
<i>Credit cards/Banks/Financial institutions</i>			
1, handle it best .....	40	41	45
2 .....	23	24	24
3 .....	16	14	11
4 .....	6	7	5
5 .....	6	4	4
6 .....	6	5	5
7, handle it worst .....	4	6	5
<i>Medical/Healthcare companies/Hospitals</i>			
1, handle it best .....	18	14	11
2 .....	25	22	20
3 .....	23	32	33
4 .....	13	13	15
5 .....	8	10	11
6 .....	8	6	6
7, handle it worst .....	6	4	5
<i>Retail business (i.e. department stores, Target/Tesco/Karstadt)</i>			
1, handle it best .....	7	6	6
2 .....	10	9	8
3 .....	14	15	12
4 .....	25	30	20
5 .....	18	20	22
6 .....	13	11	17
7, handle it worst .....	12	9	15
<i>Membership organizations (i.e. dating services, gyms, weight loss)</i>			
1, handle it best .....	4	4	4
2 .....	5	5	7
3 .....	8	4	9
4 .....	11	9	17
5 .....	17	14	16
6 .....	17	24	19
7, handle it worst .....	38	39	28

*Hospitality (i.e. restaurants, bars, hotels)*

1, handle it best .....	6	3	5
2 .....	6	5	7
3 .....	9	6	6
4 .....	12	7	13
5 .....	19	16	18
6 .....	29	34	25
7, handle it worst .....	19	28	26

*Travel Sites (Airline, car rental, hotel)*

1, handle it best .....	4	4	4
2 .....	9	7	5
3 .....	12	11	12
4 .....	21	22	23
5 .....	23	31	23
6 .....	18	17	22
7, handle it worst .....	13	8	12

*Government/local government/HMRC (tax office)*

1, handle it best .....	22	28	25
2 .....	22	29	28
3 .....	18	17	19
4 .....	11	11	8
5 .....	9	5	6
6 .....	9	4	5
7, handle it worst .....	9	7	9

13. From the same list as above, which business, type of organization or service do you think is changed or canceled the most due to security breaches/hacks when they occur?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Credit cards/Banks/Financial institutions .....	37	47	50
Medical/Healthcare companies/Hospitals .....	6	6	5
Retail business .....	27	11	5
Membership organizations(i.e. dating services, gym) .....	11	17	6
Hospitality (i.e. restaurants, bars, hotels) .....	6	4	5
Travel sites (Airline, car rental, hotels) .....	5	6	3
Government/local government/HMRC (tax office) ...	10	10	26



14. Please rank the following types of personal information you would **NOT** want to be hacked. Please give a 1 to the type of information that would concern you the most and an 8 to the type of information that would concern you the least (from the list).

	<i>US</i>	<i>UK</i>	<i>Germany</i>
<i>Credit cards/Bank statement</i>			
1, most concern .....	47	51	51
2 .....	19	22	17
3 .....	12	12	10
4 .....	7	5	8
5 .....	5	4	5
6 .....	5	3	4
7 .....	3	2	2
8, least concern.....	2	3	3
<i>Health/Medical records</i>			
1, most concern .....	9	9	11
2 .....	16	15	18
3 .....	21	21	19
4 .....	21	22	19
5 .....	15	18	14
6 .....	10	8	10
7 .....	5	5	5
8, least concern.....	4	2	5
<i>Family/information on children</i>			
1, most concern .....	12	14	13
2 .....	16	11	16
3 .....	16	16	14
4 .....	18	16	15
5 .....	13	16	14
6 .....	11	13	11
7 .....	9	7	11
8, least concern.....	6	6	6

*Employment information/salary details*

1, most concern .....	4	4	5
2 .....	10	10	11
3 .....	17	18	17
4 .....	20	20	17
5 .....	23	20	20
6 .....	13	13	15
7 .....	8	9	10
8, least concern.....	6	6	6

*Criminal /Police record*

1, most concern .....	5	5	6
2 .....	4	8	9
3 .....	8	8	11
4 .....	9	9	14
5 .....	12	12	14
6 .....	22	21	17
7 .....	21	19	17
8, least concern.....	19	19	12

*Web browsing history*

1, most concern .....	5	4	3
2 .....	5	5	5
3 .....	6	4	5
4 .....	9	9	10
5 .....	14	13	9
6 .....	18	22	14
7 .....	22	23	21
8, least concern.....	21	20	33

*Financial investment information*

1, most concern .....	15	11	8
2 .....	26	27	18
3 .....	17	18	17
4 .....	13	14	11
5 .....	11	11	14
6 .....	7	8	14
7 .....	6	6	10
8, least concern.....	5	4	8

*Sexual preferences/dating profile*

1, most concern .....	4	2	4
2 .....	4	3	7
3 .....	4	3	7
4 .....	4	5	8
5 .....	8	6	10
6 .....	14	13	15
7 .....	27	29	23
8, least concern.....	37	39	27

15. On average, how often do you change your online passwords for things like email, social networking, or shopping online?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
Once per day or more .....	7	3	4
Once a week or more.....	8	5	7
About one or two times a month .....	11	11	12
Once every two to three months.....	16	17	18
A few times per year.....	24	25	22
Once a year .....	10	9	10
Less than once a year.....	15	19	19
Never .....	10	9	8

16. How much time are you willing to spend on completing security measure tasks or steps before frustration sets in? \_\_\_\_\_minutes?

	<i>US</i>	<i>UK</i>	<i>Germany</i>
0-3 minutes.....	16	21	13
4-5 minutes.....	19	26	14
6-10 minutes.....	19	23	21
11-20 minutes.....	19	13	20
>20 minutes .....	27	17	32
<b>Mean.....</b>	<b>19.7</b>	<b>14.7</b>	<b>29.2</b>

17. From the following list, if they were available to you, which **TWO** security measures would you be most comfortable with using? If you have never heard of (NHO) this security measure, please also indicate so for all that apply.

	US	UK	Germany
Four digit numeric password .....	29	36	22
<i>NHO four digit numeric password.....</i>	11	9	12
Graphic password .....	12	12	14
<i>NHO graphic password .....</i>	35	39	35
Alphanumeric password .....	38	42	44
<i>NHO alphanumeric password .....</i>	17	15	18
GPS locator .....	8	8	8
<i>NHO GPS locator .....</i>	24	30	29
Ability to shut down or erase data remotely .....	19	16	7
<i>NHO ability to shut down or erase data remotely .....</i>	31	34	45
Fingerprint identification .....	51	50	58
<i>NHO fingerprint identification .....</i>	9	9	8
Voice identification .....	24	22	22
<i>NHO voice identification .....</i>	16	14	20
None of these .....	7	5	7