In this the sixth issue, we share the findings of some brand new research into the 'motivators' behind consumer responses to data breaches. This research indicates how existing customers, and people who are not customer's respond when their personal data is compromised. The research findings also provide a possible insight into consumers top concerns when their data has been compromised, and what their immediate reactions to discovering a breach might be and finally what level of compensation they might expect if they have had no financial loss.

The Objectives

Our sixth round of research is focused on understanding 'consumer motivators' behind data breach responses. We asked the following questions with multiple choice answers:

1. What order would you place these concerns should you discover that a company you're a customer of, had a data breach, compromising your personal data?
2. If you discover a company that you're a customer of had a data breach in which your personal data had been compromised, what would you immediately do?
3. As a result of a breach you're offered a compensation package to the value of (x). What would be an appropriate value, if you had no financial loss?

Methodology and sample

In order to get a robust, representative spread of respondents, we used a specialist consumer engagement platform, OnePulse, which enables quick market research by sending little bite-size surveys known as 'pulses' to its panel via a mobile app. We sent the 'pulses' to a cross section of individuals from the entire UK based panel to secure a statistically robust and representative sample of the wider population. We stopped the research when we had secured 1,000 respondents. Amazingly, all responses were received within 1 hour 36 minutes.

Research findings

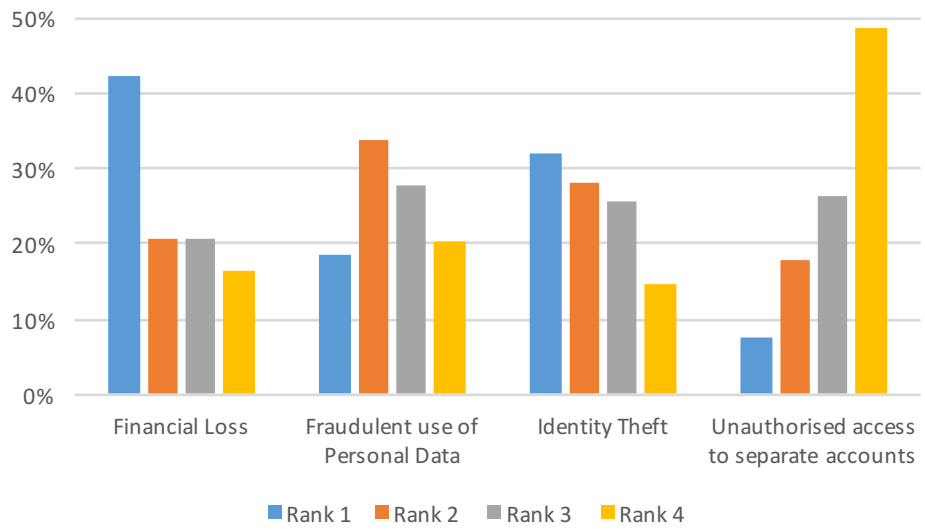
Question 1: What order would you place these concerns should you discover that a company you're a customer of, had a data breach, compromising your personal data?

The concerns that respondents were asked to rank were.

- Financial Loss
- Fraudulent use of personal data
- Identity theft
- Unauthorised access to separate accounts

We seperated 'fraudulent use of personal data' from 'identity theft' to differentiate misuse of personal data in mailing lists and online information where 'identity theft' specifically relates to imposters utilising personal data for the purposes of creating an alternate identity. We also created a comments section for respondents to communicate any other responses not listed . We only received 3 comments (0.03%) stating that all answers were equally important.

Our research uncovered that 42% of respondents ranked 'financial loss' as their greatest concern as a result of a data breach. 'Identity theft' is the next largest concern with 31% of respondents ranking it number 1. 'Unauthorised access to separate accounts' was least of respondents worries, with the smallest proportion of being ranked 1st (7.5%) and the largest proportion for being ranked 4th (48%).



This is interesting because this is the only response where the responsibility is placed in the respondents hands given that they are capable of controlling the passwords and identitfiers for each account, so if one account is compromised it doesn't lead to the domino effect on their other accounts.

Question 2: If you discover a company that you're a customer of had a data breach in which your personal data had been compromised, what would you immediately do?

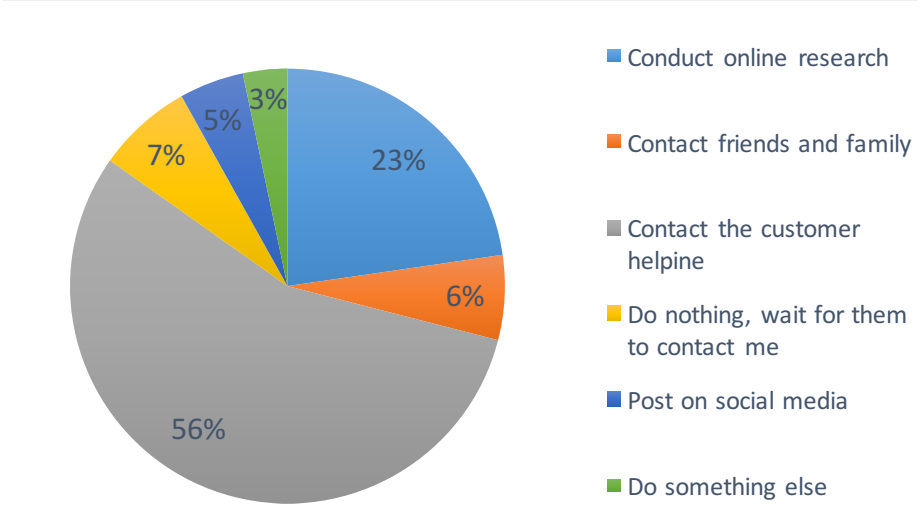
Here we wanted to investigate consumers' immediate priorities following notification of a data breach from a company where they are a customer..
The options we gave were:

- Conduct online research
- Contact friends or family
- Contact the customer helpline
- Do nothing wait for them to contact you
- Do something else

Interestingly, the most frequently added comment for this question was 'change all similar passwords' of which 2% of respondents gave that comment whilst also selecting another immediate action. We also had comments suggesting they would contact the FCA, change to a more secure provider and close down their account.

What is most significant from this round of our research is that 56% of respondents stated there immediate response to the notification of a data breach relating to a business that they were a customer of, would be to contact the customer helpline.

From the breached company's perspective, this response represents an immediate challenge that can be managed through their 'incident response plan' (PCI DSS Requirement 12.10) and if not part of existing plan's should be added as an outcome of this research.



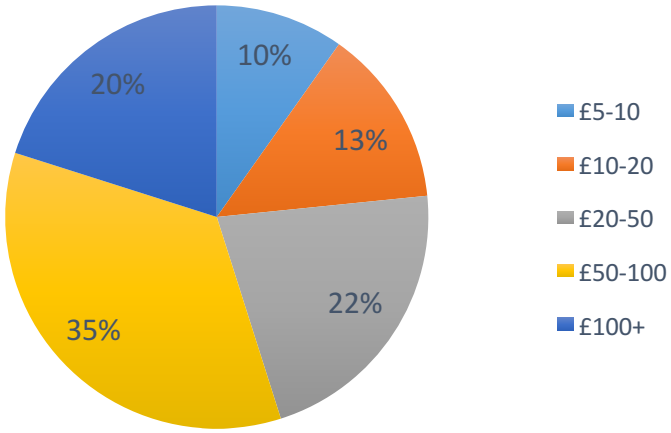
For companies with large volumes of customer data at risk (and therefore having the potential to create a mass response scenario), solutions would include the use of IVR and automated announcements as well as deploying other proven 'call avoidance' strategies involving proactive customer contact.

When breaking the information down further, we identified that a larger proportion of women (61%) would contact the helpline vs. men (49%). Within our respondents we also identified that there is a higher percentage of males (28%) that would conduct online research vs females (19%).

Question 3: As a result of a breach you're offered a compensation package to the value of (£ x). What would be an appropriate value, if you had no financial loss?

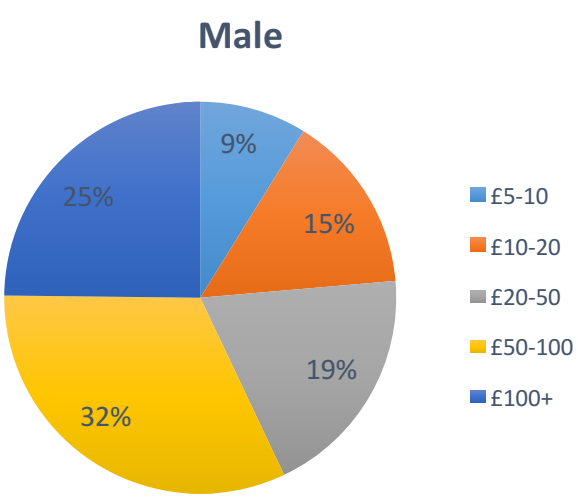
Noting that 'no financial loss' occurred we suggested the following amounts for our respondents to choose from. This time we only requested comments above our largest suggested amount (£100 +).
The options were:

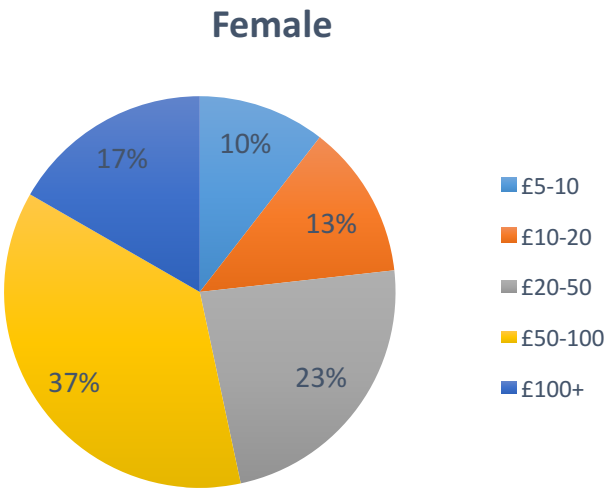
- £5-10
- £10-20
- £20-50
- £50-100
- £100+



The most frequent response was £50-100 (35%), and with our third highest response at £100+ (20%), an overall 55% of respondents stated that even in the event of NO FINANCIAL LOSS, adequate compensation for their data loss was valued at £50 +.

This is supported by comments received observing that the largest majority stated that the compensation package would need to be large enough to regain trust dependent upon the type of data lost. We should also note that only 23% of respondents would be happy with a compensation package totalling less than £20. This was supported by just 4 respondents commenting that they would expect no compensation after a breach occurred. Overall 99.6% of respondents would expect some level of compensation from a company they traded with as a result of a breach, even when they incurred no immediate financial loss.





The variance between male and female responses is most prominent within this question. 25% of males vs 17% females would feel more than £100 would be an appropriate compensation package, where as 37% of females vs 32% males feel £50-100 is appropriate.

Conclusions and implications

It feels like no surprise that respondents are most concerned about a financial loss when a data breach occurs and that they are least worried about unauthorized access to their accounts, where they have greater control of passwords. It is also no surprise that 93% of respondents would 'do something' before waiting for the breached company, with whom they had a relationship, to contact them.

However, the stand out finding of this round of consumer research is that that 56% of respondents stated that their immediate response to a data breach, in a company they were a customer of, would be to pick up the telephone and call the company helpline. Planning for this level of potential call volume hitting a call centres local telephone exchange, never mind the call centre itself, is something that larger consumer brands should pay immediate attention to,

Time is of the essence given the clear text in Article 34 of the new EU General Data Protection Regulation, which, irrespective of the EU referendum outcome, will impact the UK on May 25th 2018.
Article 34 states '*when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay'.*

Article 34, combined with the outcomes of round 5 of our research (impact of data breach on future purchasing behaviors) means that planning around data breach communication is now a significant business requirement. This will be a significant challenge for ALL consumer facing brands, but especially so for those 'online brands' without significant call handling capacity.

What this round of consumer research also highlights is that even in a data breach in which impacted customers suffered no immediate financial loss, 99.6% of respondents expected some level of compensation with 55% stating that compensation over the value of £50 would be appropriate. Clearly given these outcomes, offering no compensation at all is likely to risk customer dissatisfaction and, based on our research findings in round 5, may significantly impact on both customer churn and the brands ability to attract new customers.

This research is consistent with earlier rounds and shows that consumers clearly value their personal data and take data breach seriously. Consumers trust companies to store and manage their data securely and when this isn't the case consumers are quite clear about their expectations.

Contact us for more information on how Compliance3 can support your planning and the preparation required to meet customer expectations as a knowledgeable part of your incident response team.

Further consumer research

For the results of earlier rounds of consumer research, please visit our website
http://www.compliance3.com/resources/