



## The objectives

This third round of research was focused on understanding consumer views on payment card fraud responsibility and how consumers would behave in the event of a data breach. The questions we asked were the following:

1. If your payment card data is compromised or stolen after you've used it, whose fault is it?
2. What impact would payment card fraud have on your perception of the brand?
3. Who would you tell if you were the victim of payment card fraud?

## Methodology and sample

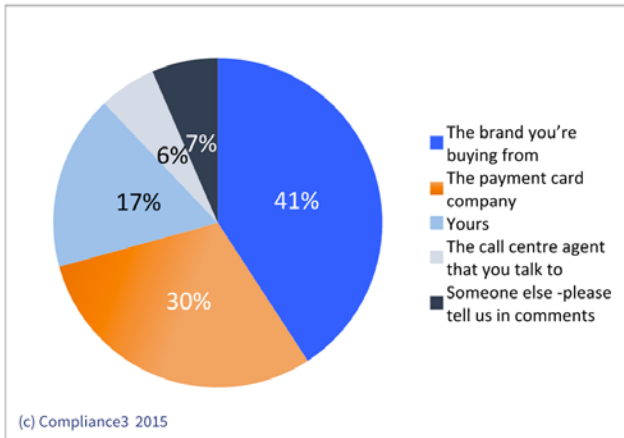
In order to get a robust, representative spread of respondents, we used a specialist consumer engagement platform, OnePulse, that enables quick market research by sending little bite-size surveys known as 'pulses' to its panel via a mobile app. We sent the 'pulses' to a cross section of individuals from 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 providing a margin of error of c. +/- 2.7%. Amazingly, all responses were received within 2 hours 18 minutes.

In this the 3<sup>rd</sup> third issue, we share the findings of some brand new research into the frequency with which consumers make payments via a contact centre and reveal what they think about doing so. The research tells us very clearly who respondents think should be responsible for their card payment security and how comfortable they would feel if they knew that the agent taking payment could not access or hear their payment card details.

## Research findings

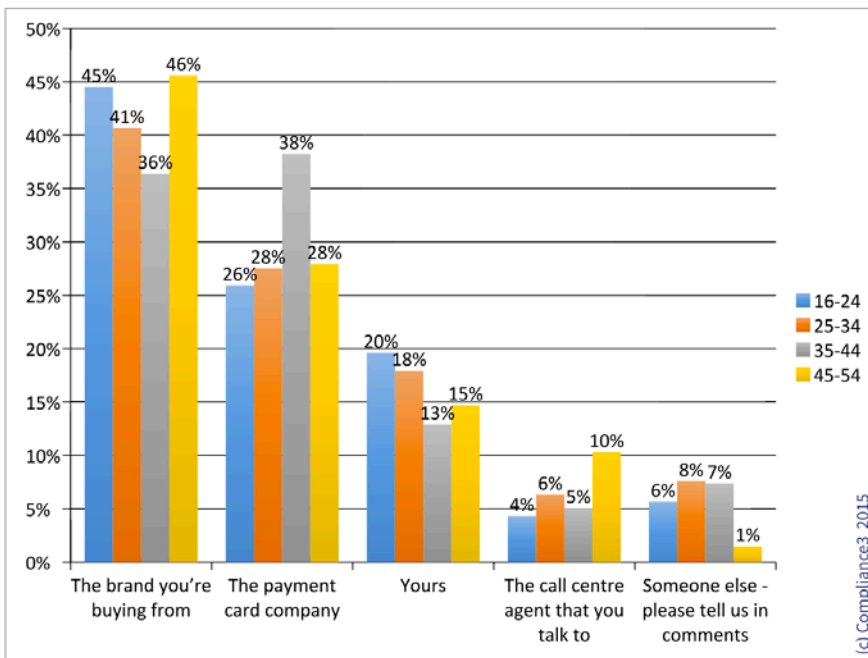
### Question 1: If your payment card data is compromised or stolen after you've used it, whose fault is it?

If the payment card data was stolen or compromised after use, 41% of respondents felt that it was the fault of the brand that they were buying from. A further 30% of respondents felt that the payment card company was to blame. 17% believed that they were to blame, 6% believed that the call centre agent was to blame and finally, 7% thought it was somebody else. Examples of 'somebody' else included: "The thief" and "Fraudsters". Remarkably similar results were witnessed for male and female respondents.



The lion's share of the blame is attributed to the brand the customer buys from, closely followed by the card company. 20% of males and 15% of females believe that they themselves would be to blame, whereas a minority (6% combined) attributed the blame to the call centre agent.

This shows very clearly that brands (and payment card companies) need to take credit card fraud extremely seriously as any blame is very clearly laid at their door by their customers.



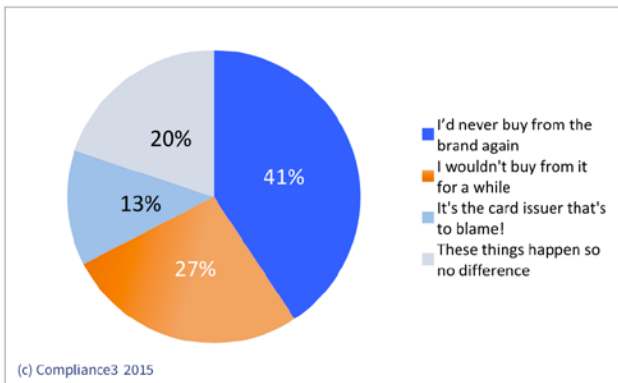
Results don't really differ significantly by age group. However, 35-44 year olds appear to be the only segment that holds the brand and payment company equally responsible, whereas the other age groups are more likely to hold the brand primarily responsible. Overall, all age groups are less likely to hold the call centre agent responsible than either the brand, the payment card company or themselves. And with a response of 10%, 45-54 year olds represent the highest scoring age group holding the call centre agent responsible.

Somewhat surprisingly, between 13% and 20% of respondents believe that they themselves would be responsible in the event of a breach, with 35-44 year olds

being the least likely and 16-24 year olds being the most likely.

There are only slight differences of opinion between men and women, with younger men in the 25-34 age category seeming to lay more blame on the brand and men generally being more tolerant of the payment card company and more likely to blame themselves.

## Question 2: What impact would payment card fraud have on your perception of the brand?

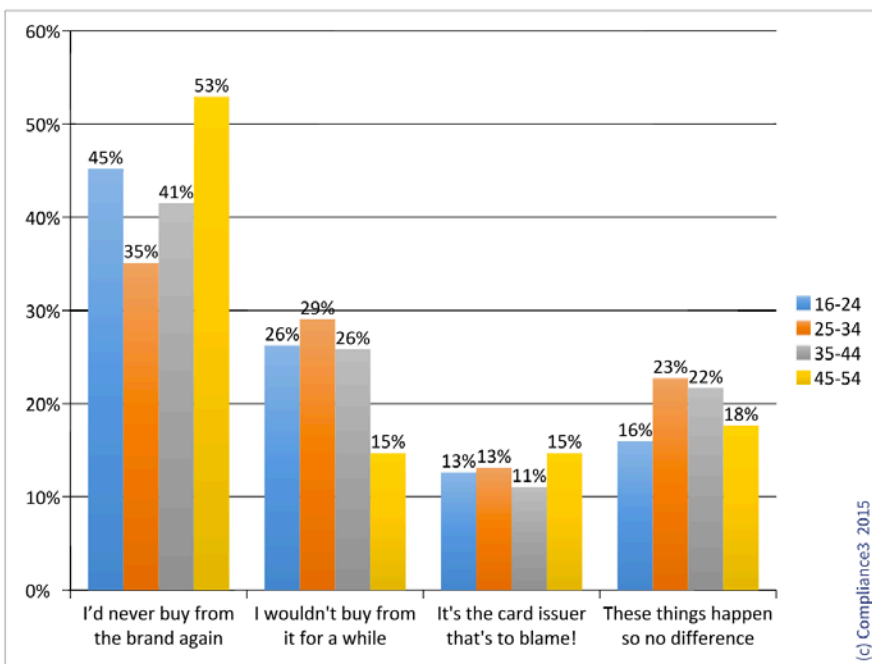


Unequivocally, nearly 70% of consumers state that payment card fraud would seriously impact their future purchasing behaviour, with 4 out of 10 customers saying that they would NEVER buy from that brand again.

A further 27% say they would avoid the brand "for a while", leaving them open to overtures from competitive products and services.

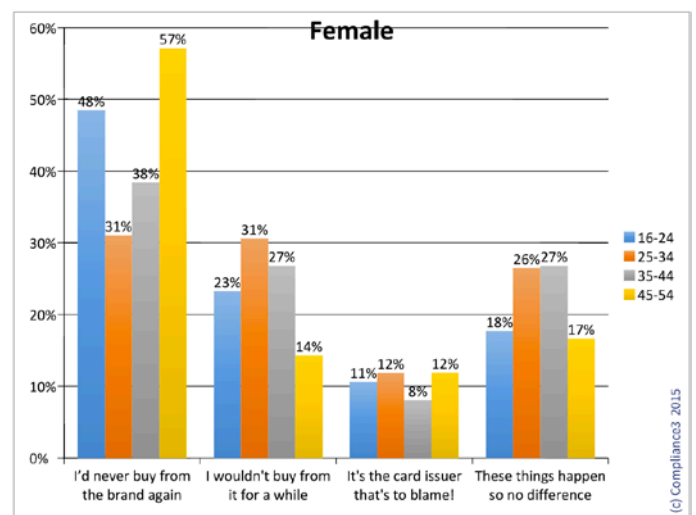
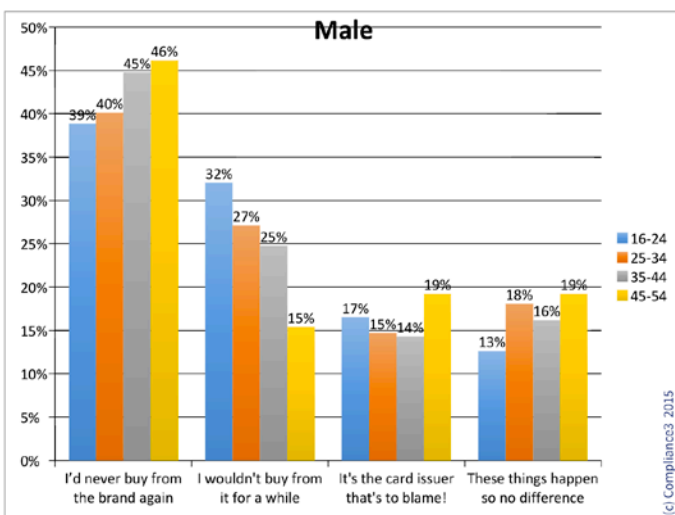
Interestingly, 1 in 5 of consumers appear to believe that this is to be expected nowadays and therefore not to be too much of a concern. A higher percentage of women (22% vs. 17% of men)

seem to accept that card payment fraud could be relatively common place.

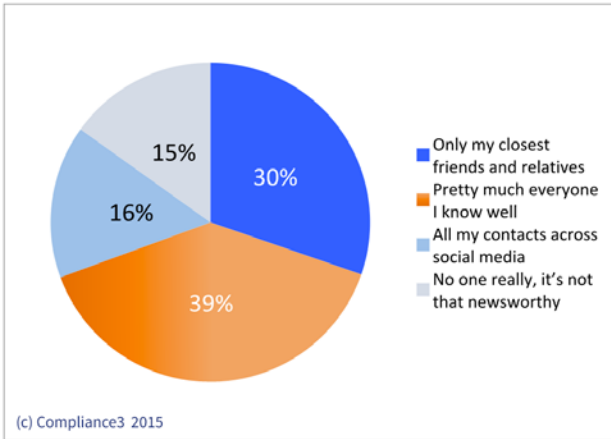


This chart shows that younger and older segments appear to be less tolerant of brands and also more likely to take direct action, whereas nearly a quarter of 25-44 year olds seem to accept that this will happen.

These views are exacerbated when broken down by gender, with more than 25% of female 25-44 year olds saying it wouldn't affect their behaviour and nearly half of older (35-54) men again being harder on the brands.



## Question 3: Who would you tell if you were the victim of payment card fraud?

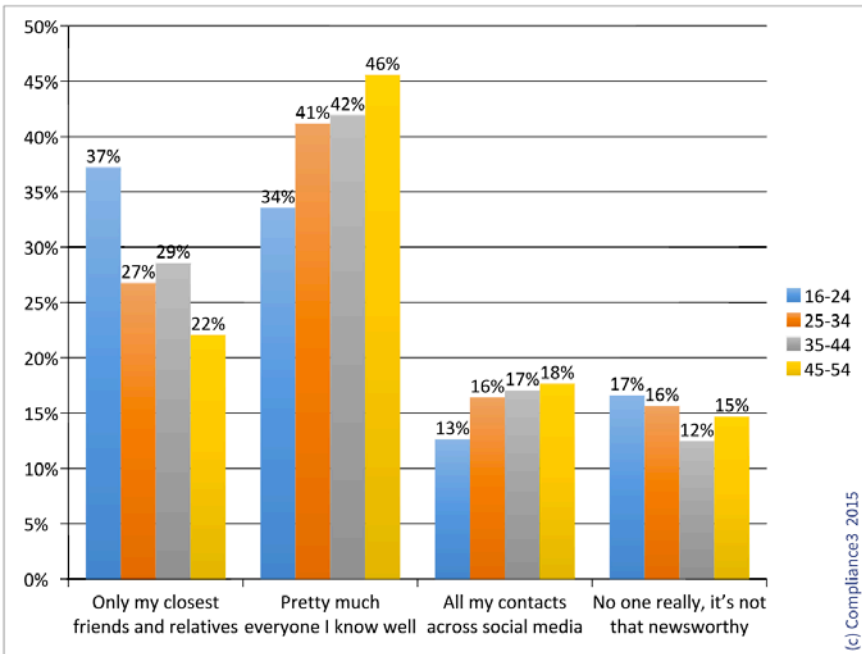


These responses are interesting as it is widely reported that humans have evolved to notice, prioritise and share 'bad news', as the aphorism 'Bad news travels fast' will support.

So the fact that a payment card has been compromised is seen as bad news that people need to know about. **85% of people would tell people they know about what has happened and what they intend to do as a result of a breach.**

Some of those would only tell closest relatives (30%) but nearly 4 in 10 would tell everyone they knew well and a further 16% would broadcast to the world on social media.

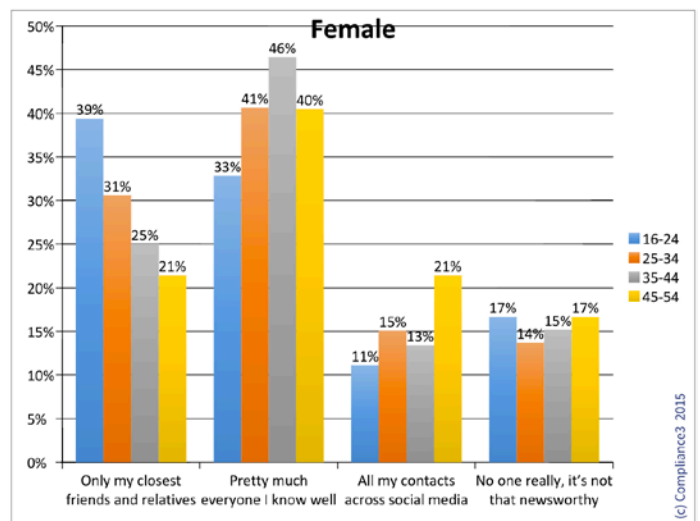
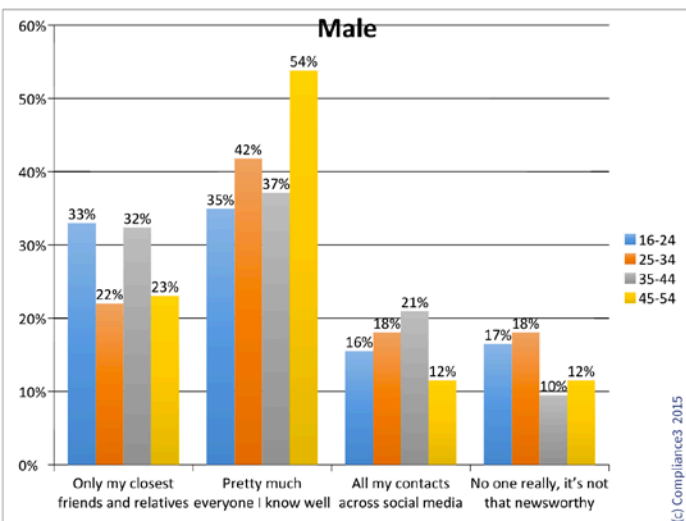
The results are remarkably similar between male and female respondents, with the only difference being that men are more likely to 'tell the world' than women.



Age groupings are quite similar in terms of responses with two surprising exceptions: firstly, the youngest age grouping purports to be less vocal, with a relatively higher percentage of 16-24 year olds saying that they would only tell their friends and relatives and 17% saying they would tell no one.

Secondly, the 45-54 age group are more likely to tell all their contacts across social media.

The difference between the youngest age group is exacerbated by gender, with nearly 40% of women under the age of 24 only telling their closest friends and relatives.



## Conclusions and implications

Clearly, Compliance3's research confirms that keeping card payment data security is of paramount importance. Why?

Firstly, from a consumer viewpoint, culpability for a data breach is attributed beyond the contact centre - even if the contact centre is the root cause.

Secondly, the potential reputational damage and revenue losses are commercially significant. Above and beyond the immediate consumer backlash, the secondary and related impact could be devastating. Modelling only 1st and 2nd generation connectedness and making some realistic assumptions on consumer behaviour, Compliance3 estimates that for every one person that has their data compromised, up to 50 connected people might well change their purchasing behaviour or relationship with a brand as a result of a breach. Multiply this by ARPU (average revenue per user) and potential customer lifetime value, and the true potential impact could be many times more severe than initially estimated.

And last but not least, perhaps the most significant of all, the findings of this research are consistent across all age groups and genders, which implies big implications for all businesses.

Don't risk it. Contact us for more information on how to stay safe.

## Further consumer research

For the results of earlier rounds of consumer research, please visit our website

<http://www.compliance3.com/pci-compliance-news.html#>