THE CONTACT CENTRE TIME-BOMB

Consumer research findings

October 2015

Compliance3

PCI COMPLIANT CONTACT CENTRES. DELIVERED.

FOREWORD

To understand the potential for card payment fraud in the UK, it is important to understand the market context.

According to ContactBabel, there are 5,840 contact centres in the UK, with 734,000 agent positions. In fact, 3.98% (1.23M) of the UK's working population are employed in contact centres today. Large contact centres (with over 250 agent positions) employ around half of all contact centre staff, despite only accounting for less than 9% of physical contact centre sites. The retail and distribution sector has most contact centres (16%), although the finance sector has the most agent positions (17%), employing around 125,000 people.

People costs represent the highest percentage of the cost base in Europe and the United States, although agent wages have reduced in real terms over last 20 years. The most recent agent mean average salary is £15,993 per year, or £53.70 per day (net). The Team Leader mean average salary is £18,278 per year, or £59.68 per day (net). Manager salaries are however increasing year on year and 2013 /14 saw an increase of 5.4%.

All this combines to make this industry - that employs large numbers of relatively underpaid individuals – a soft underbelly for organised crime.

"We know of organised crime groups who are placing people within the call centres so that they can steal customers' data and carry out fraud and money-laundering. We also know of employees leaving the call centres and being approached and coerced, whether physically, violently or by being encouraged to make some extra money. And, of course, you also have the disgruntled employee who may turn their hand to fraud just to benefit themselves".

Detective Chief Inspector Derek Robertson, Strathclyde Police

This context - underpaid, potentially disgruntled employees with access to personal and card payment data working for organisations which, very often, do not have PCI DSS compliance at the top of the agenda – inspired us to help organisations understand the ***true*** cost of falling foul of PCI DSS compliance regulations.

And our research proves that the fines are just the tip of the iceberg…

EXECUTIVE SUMMARY

PCI DSS regulations are in place to protect consumers from fraud. The implications of non-compliance are well publicised and there have been several reported cases of breaches that have resulted in hefty fines and high profile exposure - for all the wrong reasons. Despite this, many UK companies are not taking the necessary steps to secure consumer payment data because it's considered too expensive, too difficult or even more alarmingly, because the risk doesn't warrant the resource and financial investment. Or so they think.

Compliance3's four phase research programme, conducted from January to June 2015, reveals startling insights into what consumers really think about payment card security and fraud in contact centres – and how they will behave in the event of a breach.

First of all, although a majority of consumers pay over the phone they don't like doing so. And although they feel relatively confident that brands are doing a good job to protect their data, they believe that responsibility for card payment data protection is an issue for key senior personnel and the Main Board.

The degree to which consumers indicated increased comfort about their payment card data not being heard or accessed was significant. However, a surprising number of respondents didn't know or weren't sure about how to keep their credit cards secure from fraud.

If the worst happens and a breach does occur, over 40% of respondents put the blame squarely at the door of the brand. Worryingly, consumers will not only name and shame the brand, nearly three quarters will seriously modify their purchasing behaviour. And it doesn't stop there: 85% of people will tell people – from closest relatives and friends to everybody they know on social media – what happened and what they think.

The potential for reputational damage and revenue losses are therefore substantial. 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.

To conclude, our research clearly demonstrates that the risk of non-compliance far outweighs the resource and financial investment required to comply. In short, brands need to ensure that consumer payment card data is secure and also that they are well prepared if the worst is to happen.

As well as complete openness and transparency, consumers expect proactive communication both if a breach occurs and any corrective action taken – and it would appear that "sorry" is not enough. In addition to an apology (which is expected), consumers expect compensation.

On a positive note, if contact centres are to remain a viable payment option into the future, explicit/publicised data security can become a lever for differentiation and subsequent competitive advantage. Clearly, this benefit should be considered above and beyond the expected benefits of reduced risk of fraud, consequential revenue loss and reputational damage in the event of a breach.

THE RESEARCH

The research, designed to probe consumer views on card payment security and fraud in contact centres, was conducted in four phases between January and July 2015. 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.

PHASE 1

Phase 1 – Objectives

In this first phase, we set out to understand how often consumers make payments via a contact centre and to reveal what they think about doing that. The research also 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.

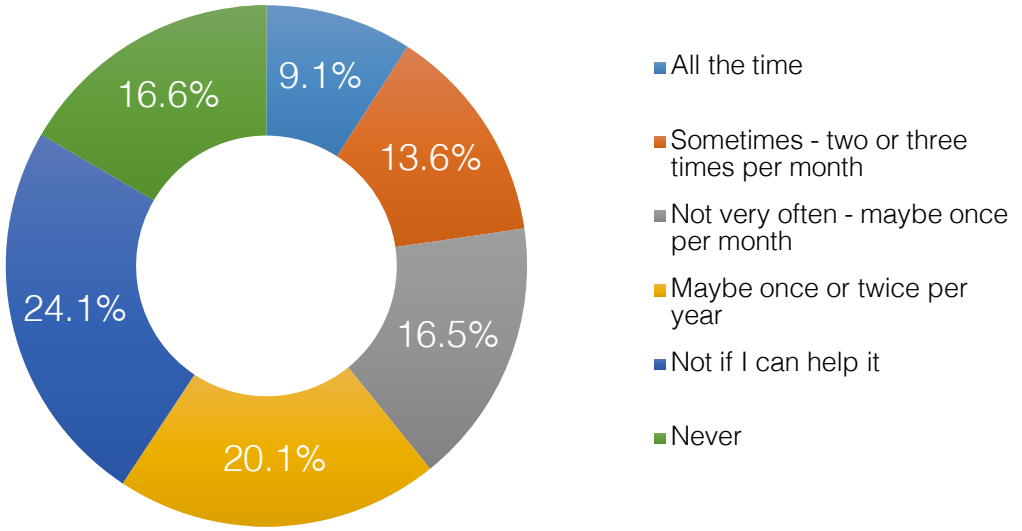
The first phase asked the following 3 questions:

- How often do you buy products or services by giving your payment card details over the phone?
- Who in the company should have overall responsibility for keeping payment card details safe from fraudulent usage?
- If you knew that your payment card details could not be heard or accessed by the call centre agent, would you feel (choice of: much more comfortable, more comfortable, about the same, less comfortable, much less comfortable).

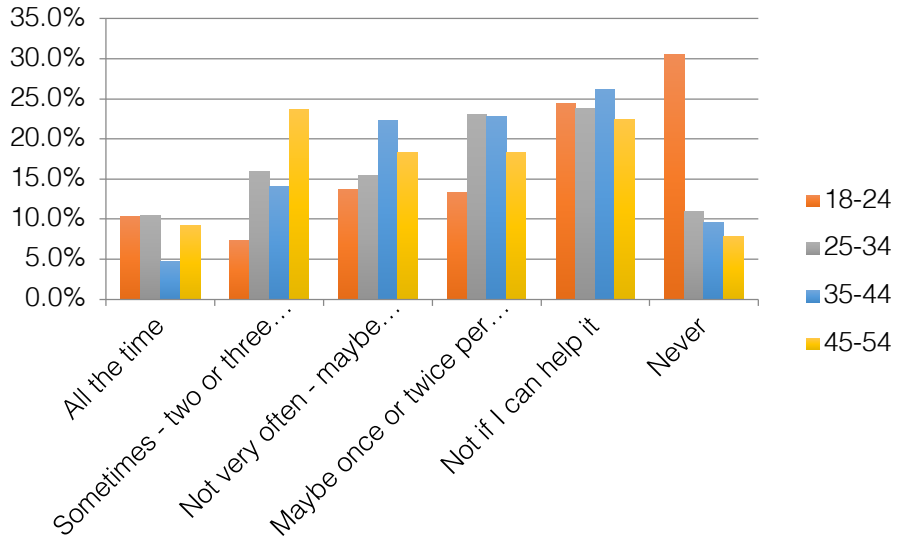
Phase 1 - Findings

The responses provide interesting insights into consumer views on the issue of making payments via the contact centre.

Q1: How often do you buy products or services by giving your payment card details over the phone?



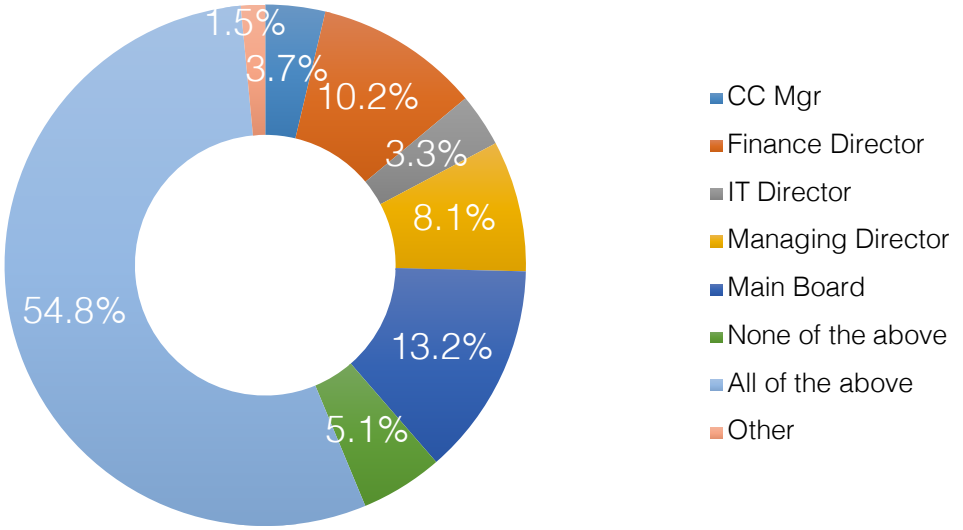
Approximately 60% of respondents make payments via the contact centre, showing that this is a widely used method of payment. However, the responses indicate that a sizeable percentage of consumers would prefer not to pay this way (24.1%) and nearly 17% stating that they never make payments via the contact centre.



Although the variance between age groups for 'not if I can help it' is very small, the breakdown by age in the 'Never' category is hugely significant with just over a third of the 18-24 age group saying that they would never make a credit card payment via the phone.

There could be several explanations for this; perhaps this is indicative of a degree of mistrust amongst younger generations towards contact centres in general and/or that they do not consider credit/debit cards to be a preferred method of payment.

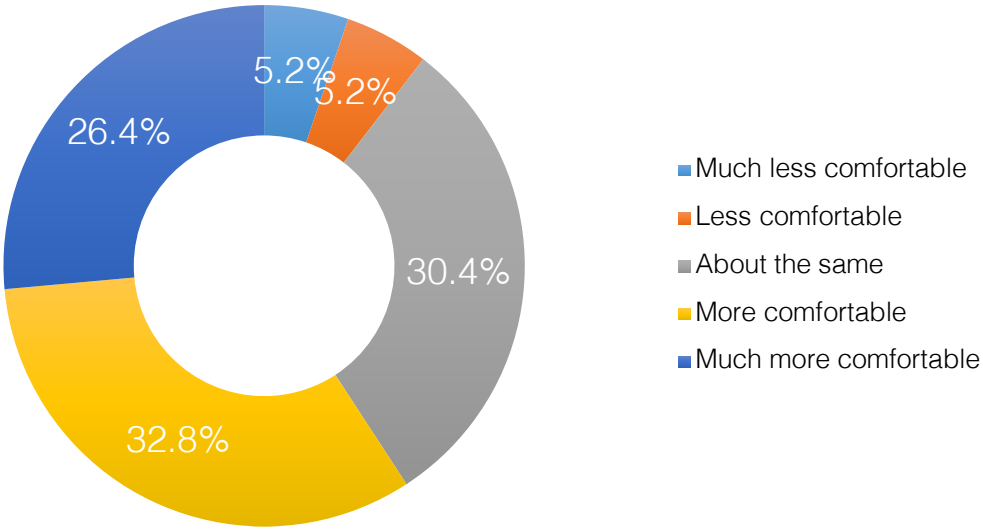
Q2: Who in the company should have overall responsibility for keeping payment card details safe from fraudulent usage?



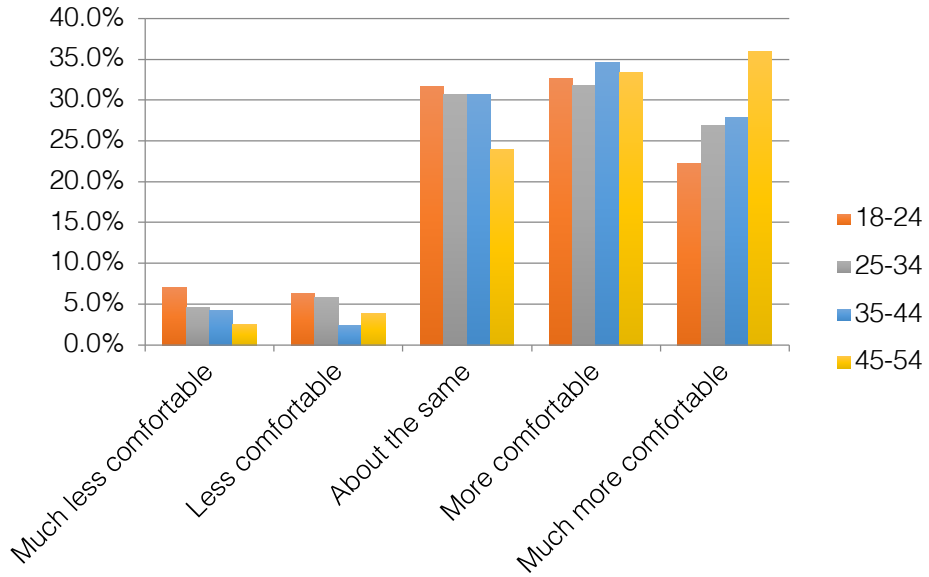
Over half of the respondents believe that key senior personnel and the Main Board are responsible for keeping their card payment details safe which shows how seriously consumers take the safe-keeping of their payment details.

The 'usual suspects' for responsibility within organisations, the Call Centre Manager and the IT Director, scored a staggeringly low 3.71% and 3.41% respectively. Our respondents were pretty unanimous about this and there was no significant variation by gender or age.

Q3: If you knew that your payment card details could not be heard or accessed by the call centre agent, would you feel...



Clearly, understanding that the card payment data cannot be heard or accessed is a key reassuring factor for nearly 60% of the survey sample. There is no significant variance between genders but if we study the breakdown by age, it is clear that communicating the benefits of being PCI DSS compliant will help engage with all customers, but specifically the 45-54 age group, where more than 2/3rds of respondents state that they would be 'more' or 'much more' comfortable about making card payments via the contact centre under these conditions.



Phase 1 – Implications

Essentially we have 3 major takeaways from our first phase:

1. Although payment via the contact centre is a mainstream method of payment for products and services in the UK, a fairly high percentage of consumers prefer not to pay this way.

2. Responsibility for card security should be all-pervasive throughout the organisation and needs to be a Board level concern. The research proves beyond doubt that consumers consider card payment data security not to be the sole responsibility of the Call Centre Manager or the IT Director.

3. Organisations need to reassure customers that their card data is secure if payment via the contact centre is to remain and increase as a viable payment option into the future. The degree to which consumers indicated increased comfort about their payment card data not being heard or accessed was significant.

PHASE 2

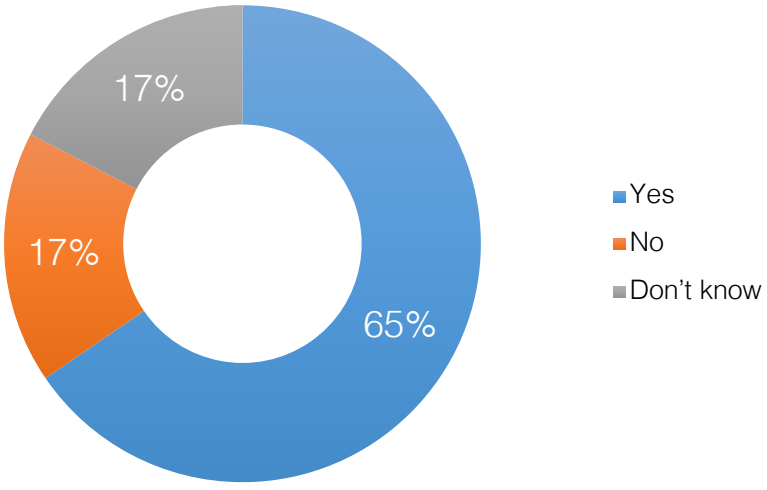
Phase 2 – Objectives

This round of research was focused on understanding consumer awareness levels of payment card fraud, confidence levels about how data is being kept secure and what should happen to businesses that do not do enough to keep card payment data secure. The questions we asked were:

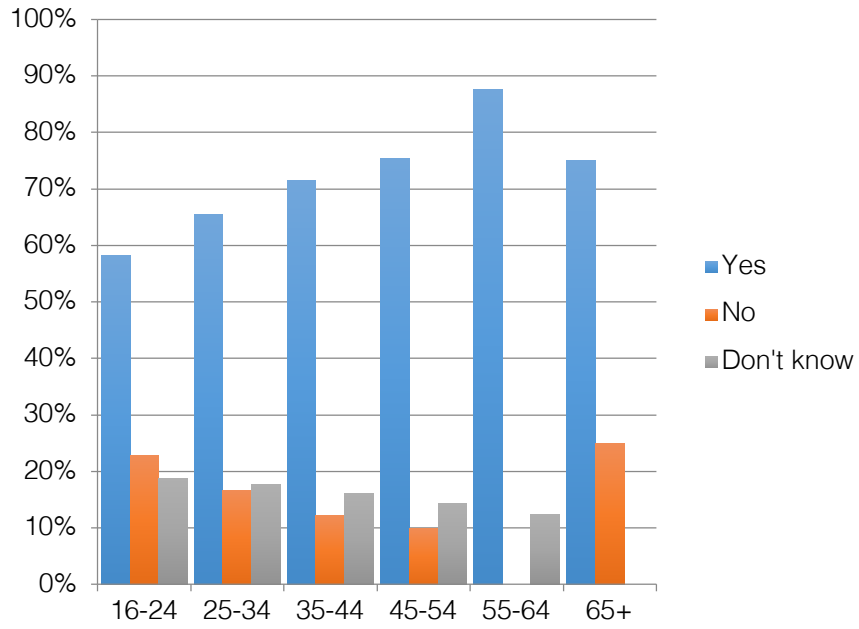
- Are you aware of what you should and shouldn't do to keep your payment cards safe from fraud?
- How confident are you that your card payment data is kept safe and secure by companies that take payments via the contact centre?
- Do you think that businesses that do not do enough to protect payment card data should be named and shamed?

Phase 2 – Findings

Q1: Are you aware of what you should and shouldn't do to keep your payment cards safe from fraud?

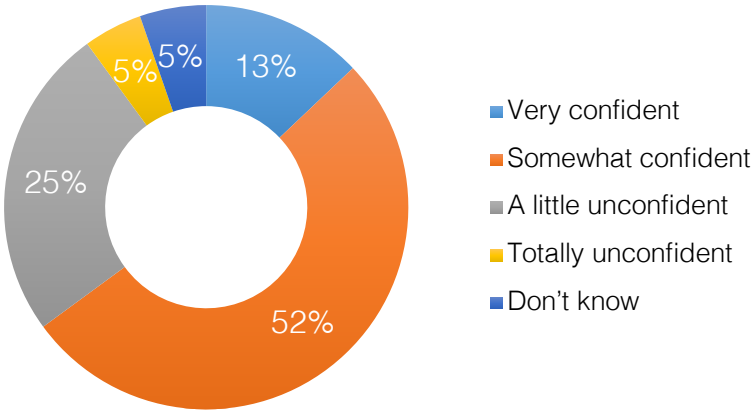


A surprising number of respondents (nearly 35%) didn't know or weren't sure about how to keep their credit cards secure from fraud. Although the younger segment (18-24) appears the least aware - despite being internet savvy - this could be indicative that they are more aware of the risks and therefore more aware of what they don't know (i.e. they know all the possibilities).

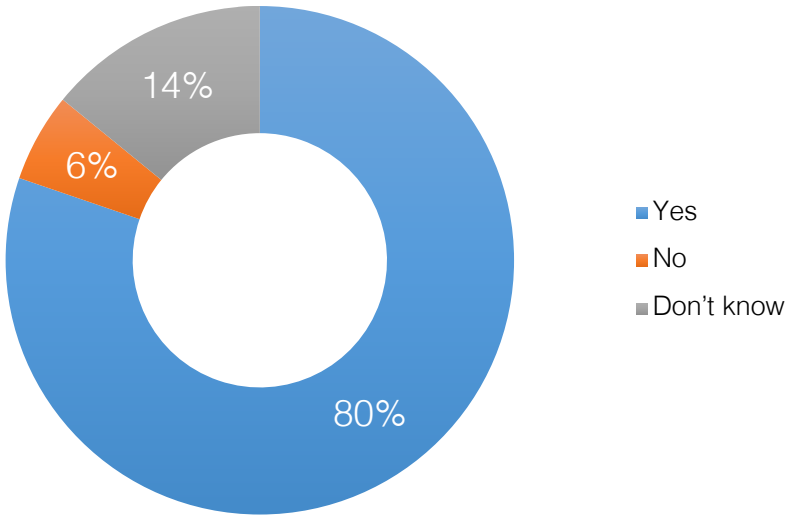


Q2: How confident are you that your card payment data is kept safe and secure by companies that take payments via the contact centre?

Two thirds of consumers believe that their data is relatively secure with the companies they're dealing with, with males being slightly more positive than females in this area. There is however no real significant variance by age or by gender.



Q3: Do you think that businesses that do not do enough to protect payment card data should be named and shamed?



There is an overwhelming call for companies that blatantly play fast and loose with card data security to be "outed", with only 6% of respondents saying that this is a bad idea.

Phase 2 - Implications

1. The youngest age group could be more aware of the risks, which could result in lower levels of trust in paying via a contact centre. Similarly, because they know more about the level of potential risk they could be less comfortable that they know how to protect themselves against it.

2. A significant majority believe that companies are keeping their data secure so if they're subsequently proved wrong then…

3. …consumers will be tough on companies that have data breaches with 80% saying they should be publicly named and shamed.

PHASE 3

Phase 3 - Objectives

The 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.

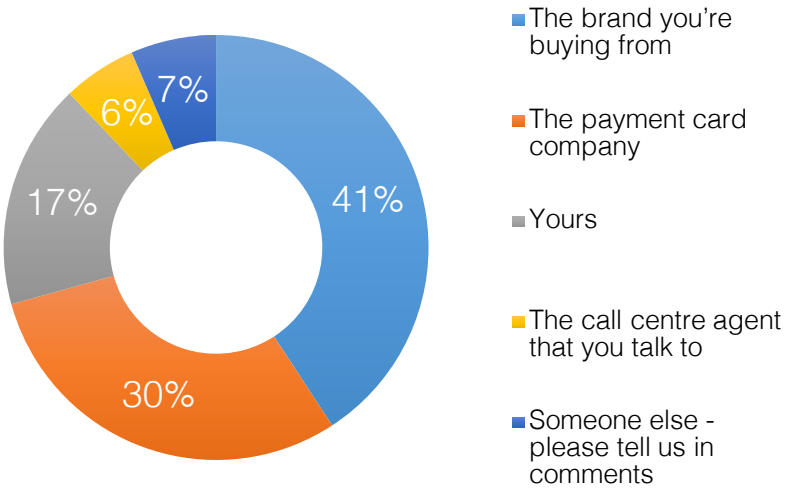
The questions we asked were the following:

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

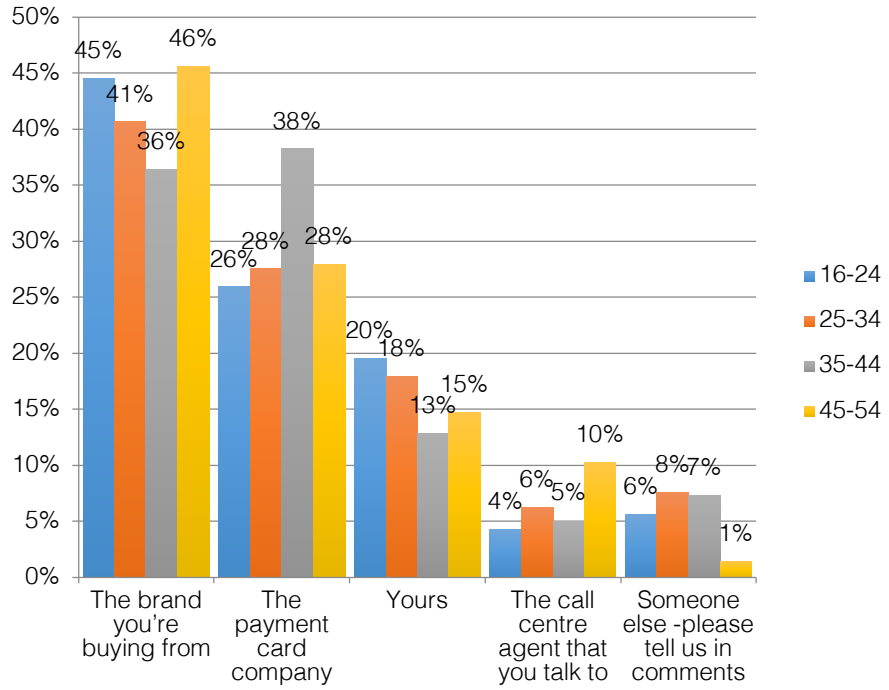
Phase 3 - Findings

Q1: 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".



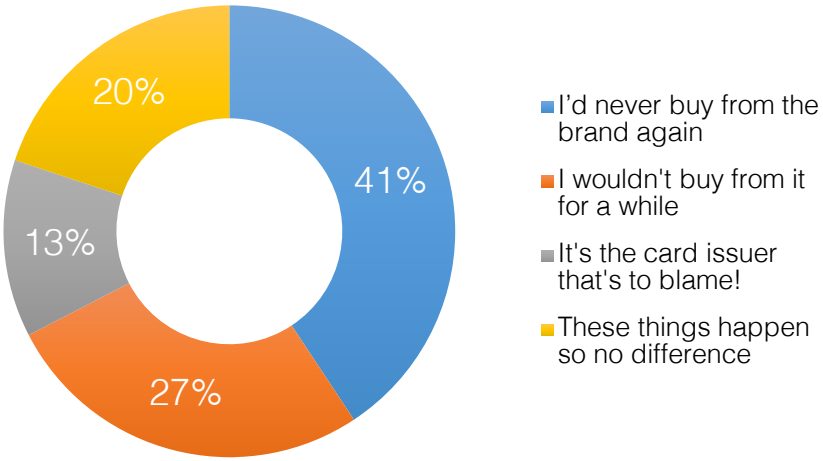
Remarkably similar results were witnessed for male and female respondents. The lion's share of the blame is attributed to the brand the customer buys from, closely followed by the card company. 20% of males and 15% of females believe that they themselves would be to blame, whereas a minority (6% combined)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



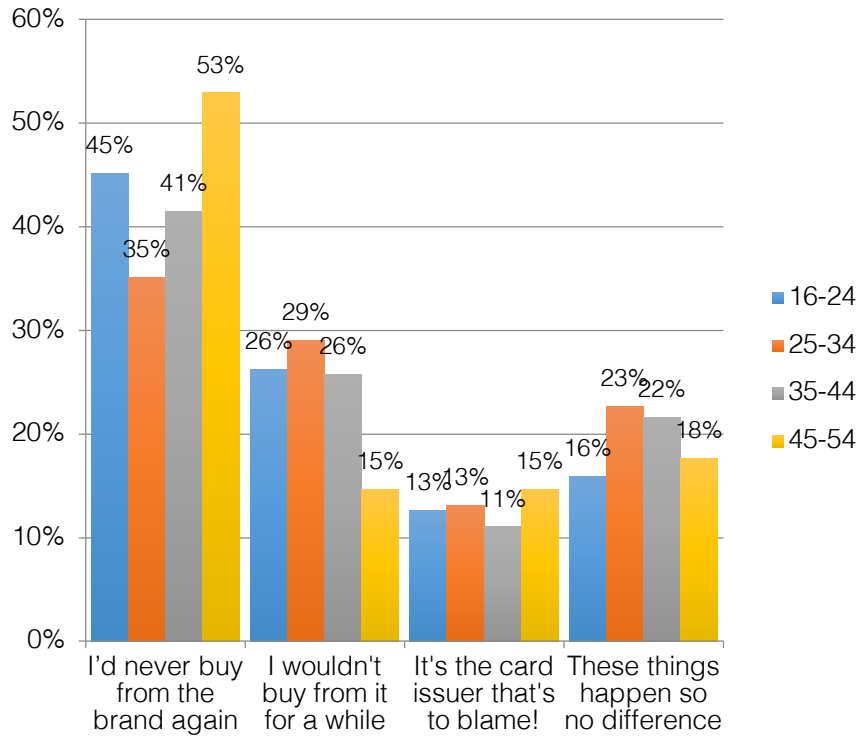
Results don't really differ significantly by age group. However, 35-44 year olds appear to be the only segment that holds the brand and payment company equally responsible, whereas the other age groups are more likely to hold the brand primarily responsible. Overall, all age groups are less likely to hold the call centre agent responsible than either the brand, the payment card company or themselves.

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.

Q2: What impact would payment card fraud have on your perception of the brand?

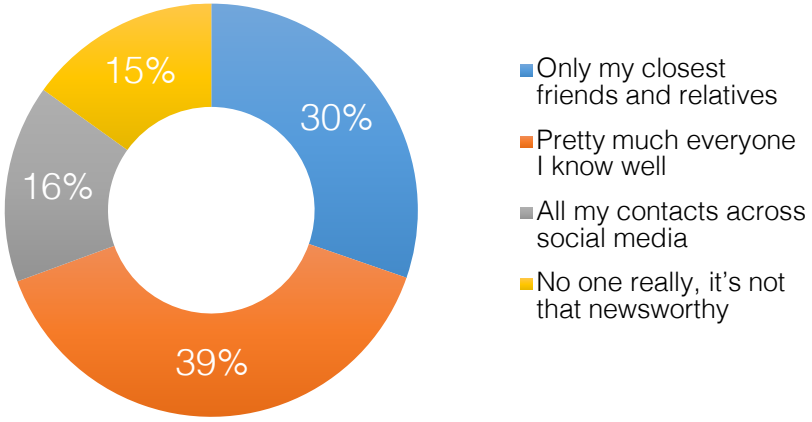


Unequivocally, nearly 70% of consumers state that payment card fraud would seriously impact their future purchasing behaviour, with 4 out of 10 customers saying that they would **NEVER** buy from that brand again. A further 27% say they would avoid the brand "for a while", leaving them open to overtures 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.

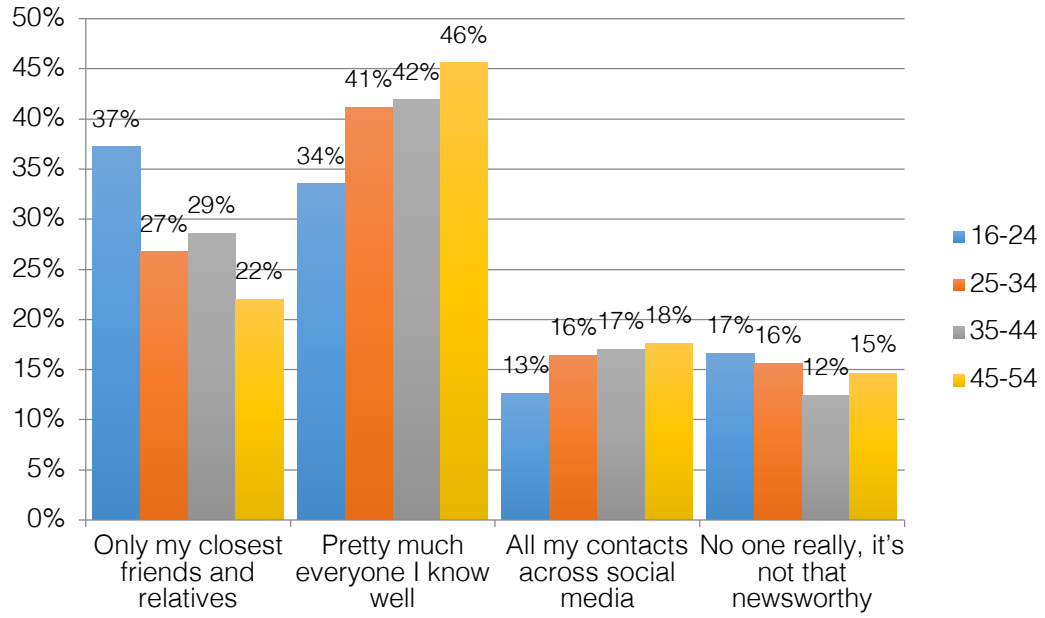


This chart shows that younger and older segments appear to be less tolerant of brands and also more likely to take direct action, whereas nearly a quarter of 25-44 year olds seem to accept that this will happen. These views are exacerbated when broken down by gender, with more than 25% of female 25-44 year olds saying it wouldn't affect their behaviour and nearly half of older (35-54) men again being harder on the brands.

Q3: Who would you tell if you were the victim of payment card fraud?



85% of people would tell somebody 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 slight 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.

Phase 3 – Implications

This phase 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 and the potential for long term brand damage is substantial.

The responses are also interesting as it is known that we 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 – and share.

The impact of these findings is to recognise that it is not only your direct customers that will change their behaviour as a response to a breach but also their immediate connections and those connections' connections leading to a ripple effect that will have significant long term commercial impact.

PHASE 4

Phase 4 – Objectives

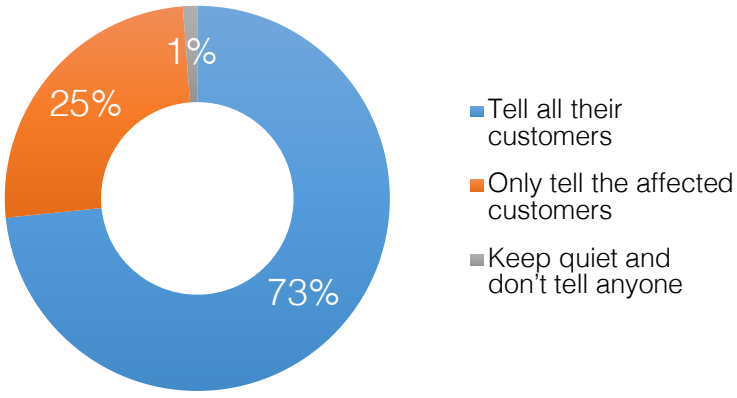
This final phase was designed to understand how brands should behave in the event of a card payment data breach.

The questions we asked were the following:

- If a brand you purchase from experiences card payment data theft, how do you think they should behave (response options as per the graphs)?
- How should the brand communicate the fact that they have experienced card data theft?
- How should the brand behave towards customers in the event of card data theft?

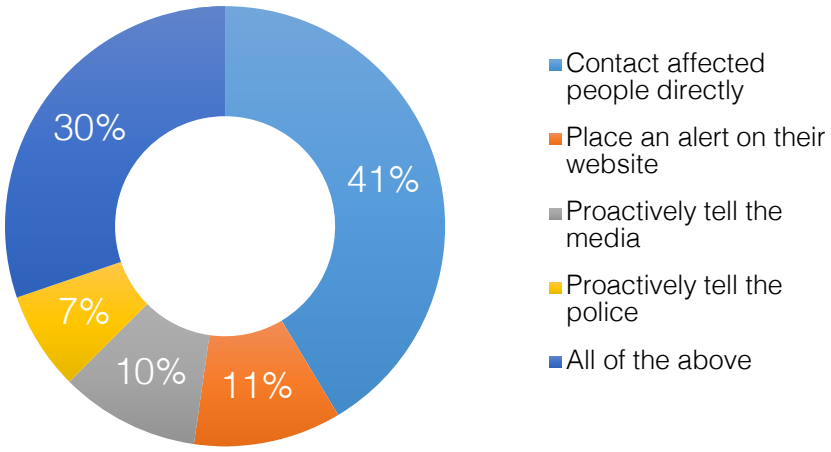
Phase 4 – Findings

Q1: If a brand you purchase from experiences card payment data theft, how do you think they should behave (response options as per the graphs)?



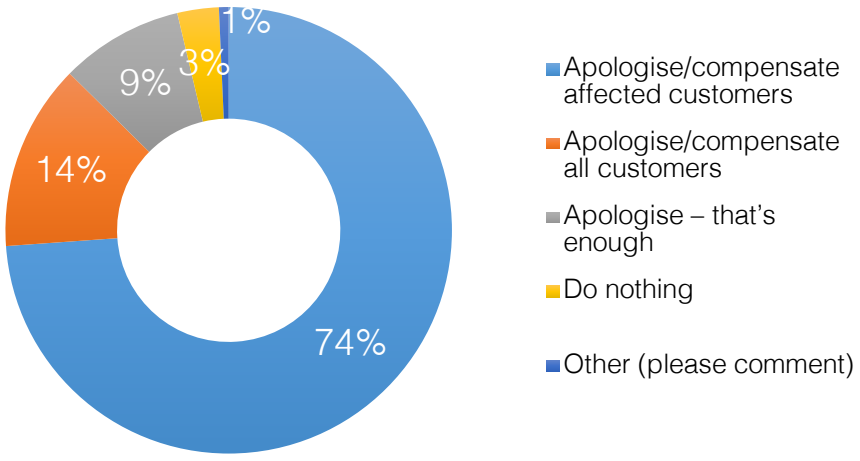
Only 1% of consumers thought that brands should keep quiet, meaning that a resounding 99% should either tell all their customers (73%) or affected customers (25%). Male & female responses were exactly the same and there was little variance between age groups.

Q2: How should the brand communicate the fact that they have experienced card data theft?



41% felt that brands should contact all affected people directly, 11% that brands should place an alert on the website, 10% that they should proactively tell the media, 7% that they should proactively tell the police and 30% felt that brands should do all these things. Slightly more women than men (43% vs 39%) felt that brands should contact affected people directly whereas more men than women thought that the media should be informed (13% vs 8%).

Q3: How should the brand behave towards customers in the event of card data theft?



74% of respondents felt that brands should apologise to and compensate all affected customers, whereas 14% felt that all customers should receive an apology and compensation. 9% felt that an apology was enough and only 3% felt that brands should do nothing.

The only differences in response by gender were that more males than females felt that all customers should receive an apology and compensation (16% vs 11%) whereas more females than males (76% vs 71%) felt that only affected customers should receive an apology and compensation.

Phase 4 – Implications

This phase of research proves beyond doubt that consumers expect transparency openness in the event of a breach. They also expect compensation.

This means that:

- Brands must communicate proactively that they have suffered a breach which implies that they should have a robust data breach response plan in place.
- Sometimes “sorry” is not enough. In the event of card payment fraud, in addition to an apology (which is expected), consumers expect compensation – at the very least for all affected customers.
- It is imperative that brands need to evaluate their policy with regard to compensation and make the necessary budget provisions.

CONCLUSIONS

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.

Thirdly, explicit/publicised data security can become a lever for differentiation and subsequent competitive advantage. It is also essential if contact centres are to remain a viable payment option into the future. The research findings indicate a very real opportunity to increase credit/debit card payment activity by being overt about the levels of card security and fraud prevention by making people aware that the organisation operates PCI DSS compliant contact centre operations. Organisations that let their customers know how seriously they take card payment data security and educate them about what being PCI DSS compliant means and that card payment cannot be heard or accessed by the contact centre agent will benefit commercially from customers being more likely to use their credit/debit card to pay for products and services. Clearly, this benefit should be considered above and beyond the expected benefits of reduced risk of fraud, consequential revenue loss and reputational damage in the event of a breach.

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

ABOUT THE AUTHOR

Glenn has over 25 years' experience in Asia Pacific, the US and Europe in various businesses management roles in the contact centre industry within start-ups, high growth companies and at senior and Board level in billion dollar turnover businesses. This, and his wide industry experience – from childcare to fibre-optics to global contact centres - means that he now holds executive roles for new and emerging companies.

Glenn is passionate about emerging consumer trends and loves traveling and discovering great wines from lesser known vineyards of Languedoc Roussillon in France.

ABOUT COMPLIANCE3

Compliance3 helps contact centres cost-effectively achieve and maintain customer contact compliance – including PCI DSS. In doing so, we help protect our clients' revenues and margins and significantly reduce the risk of reputational damage and consequential revenue loss – as well as the costs associated with compliance.

Achieving customer contact compliance isn't just about technology. It requires a robust understanding of risks, personal data and financial services regulations and legislation, as well as best-in-breed technology solutions. It also requires a firm grasp of contact centre operations and how to deliver exceptional customer experiences - not to mention finely honed cost and project management skills.

At Compliance3, we combine all this to make customer contact compliance easy. We blend people, process and technology, engaging with only the very best experts and solution providers available in the marketplace. As far as PCI DSS compliance is concerned, we accompany our clients from their unique starting point to a compliant state as quickly and cost-effectively as possible. But when we have delivered PCI compliance, we don't just walk away; we work with clients over the longer term to protect card and personal data, implement strong access control measures, regularly monitor and test to eradicate vulnerability, and maintain a robust card and personal data security policy. In addition to card scheme data security requirements, we are conversant with all relevant personal data and financial services regulations and legislation.

Thanks to our deep and extensive experience within contact centres, we are fully aware that customer contact compliance must not be to the detriment of the customer experience. That's why the solutions we deliver build trust with customers and are designed to be easy.

Don't risk it. If you have any questions about your organisation's PCI DSS compliance status, talk to Compliance3. We'll help you understand where you are on the journey and what's required to achieve and maintain compliance cost-effectively.