Compliance3

Compliance3 **Insights**

What consumers really think

Round1: Making payments via the contact centre

Introduction

Welcome to Compliance3's first consumer insights bulletin!

In this first 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.

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.

The first pulse asked 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).**

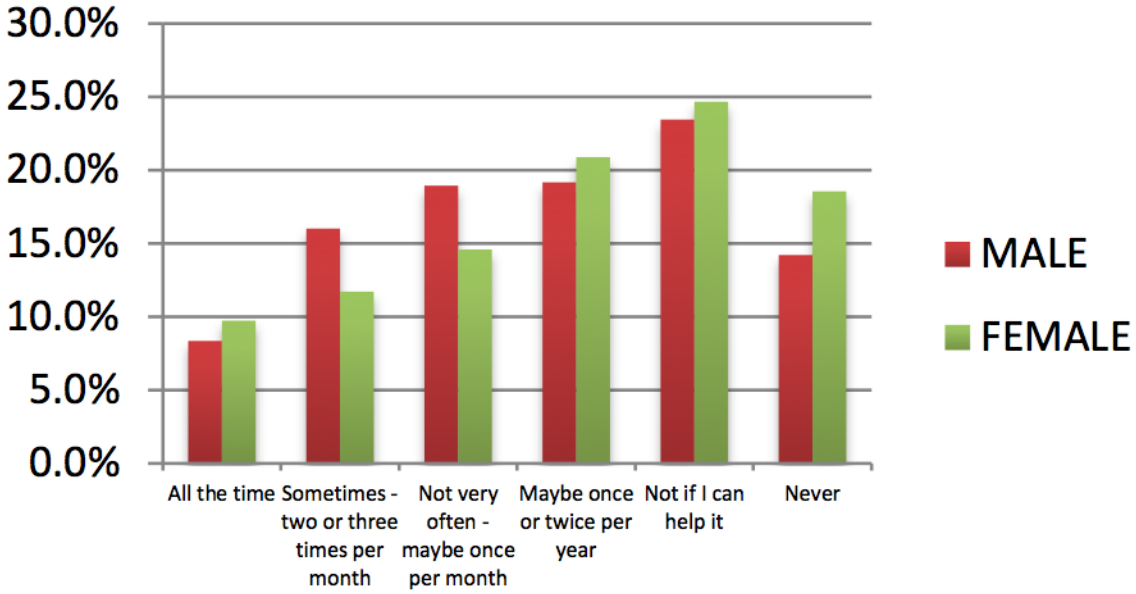
Research findings

The responses provide interesting insights into consumer views on the issue of making payments via the contact centre. Here follows a breakdown of the findings:

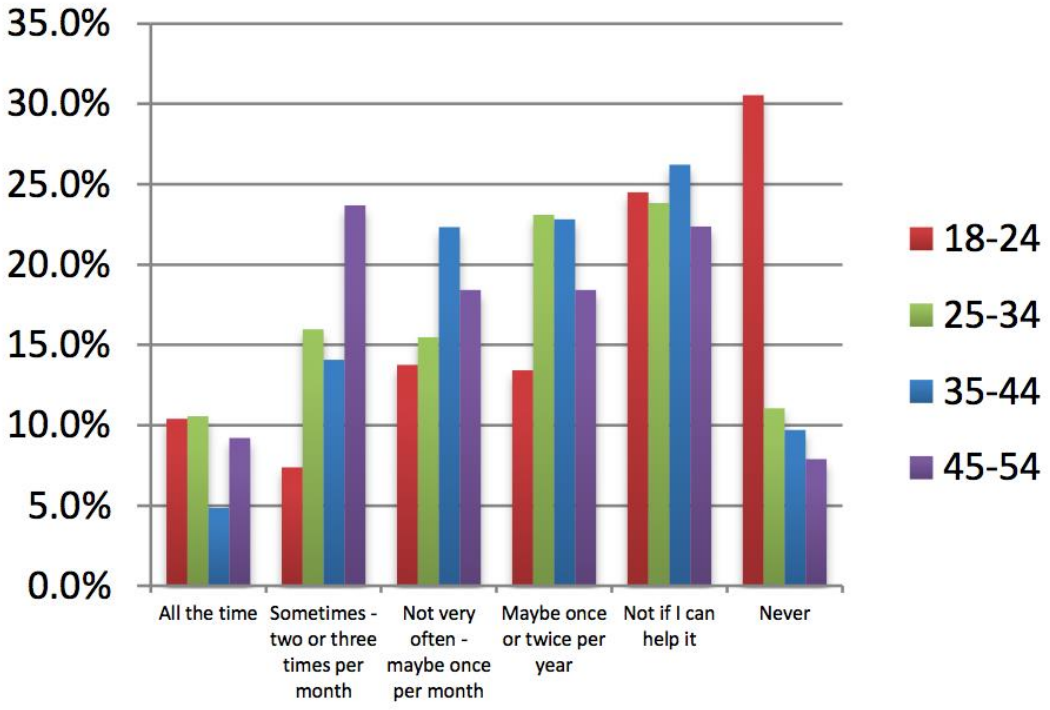
Q1: How often do you buy products or services by giving your payment card details over the phone?

Response option	% response
All the time	9.1%
Sometimes – two or three times per month	13.6%
Not very often – maybe once per month	16.5%
Maybe once or twice per year	20.1%
Not if I can help it	24.1%
Never	16.6%

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.



Little difference but women are more likely to never make payments via the contact centre.



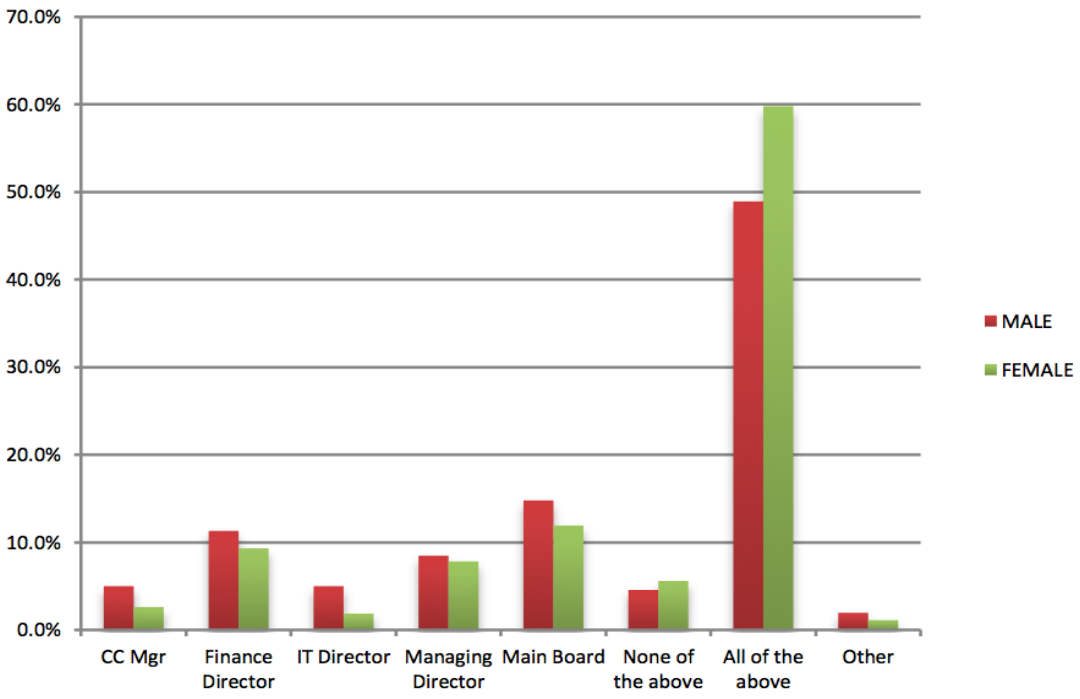
Although the variance between age groups for ‘not if I can help it’ is very small, there is more variance when we look at how often payments are made via the contact centre, with the 18-24 group making less payments overall, and scoring extremely highly on ‘Never’. There could be

several explanations for this; perhaps, the fact that a third of this age category would never give their card details to a contact centre is indicative of a degree of mistrust amongst younger generations and/or that they do not consider credit/debit cards to be a preferred method of payment.

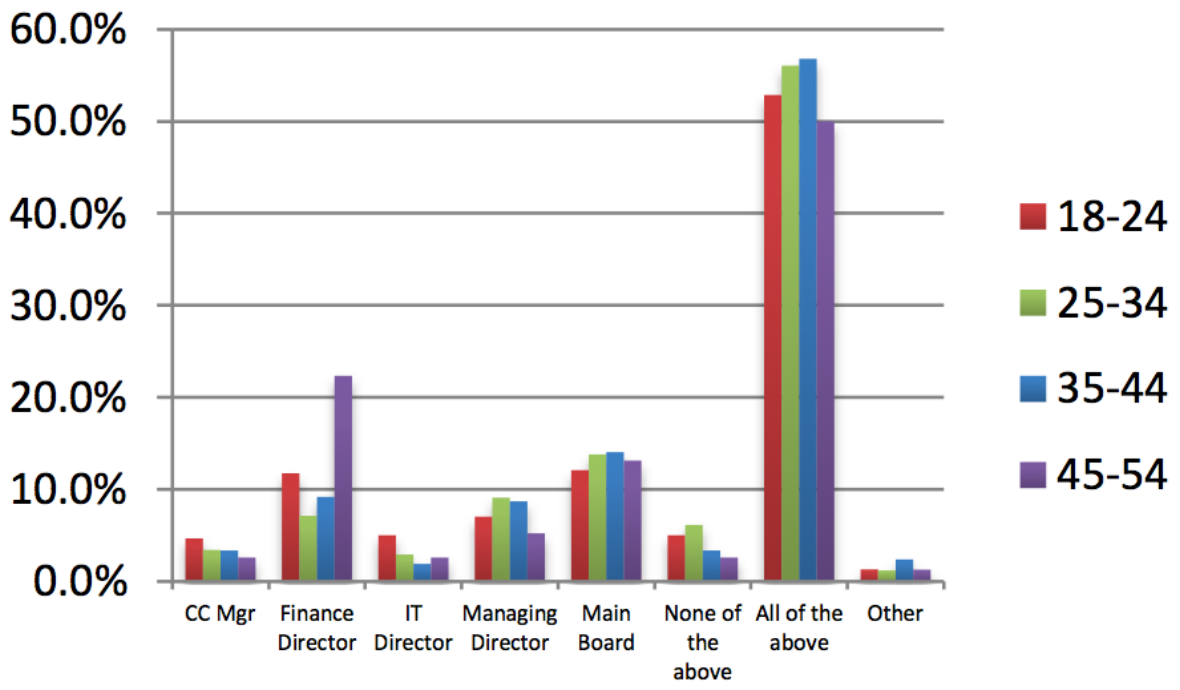
Q2: Who in the company should have overall responsibility for keeping payment card details safe from fraudulent usage?

Response option	% response
Main Board of the company	13.23%
Managing Director	8.12%
Call Centre Manager	3.71%
IT Director	3.41%
Finance Director	10.22%
All of the above	54.71%
None of the above	5.11%
Other (please specify)	1.5%

Over half of the respondents believe that key senior personnel and the Main Board are responsible for keeping their card payment details safe. This just goes to show 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.



The breakdown by gender reveals remarkably similar results, with the exception of 'All of the above' which shows that females outweigh males by 11% with their view that there should be shared, senior responsibility with regards to the safe-keeping of card payment data.

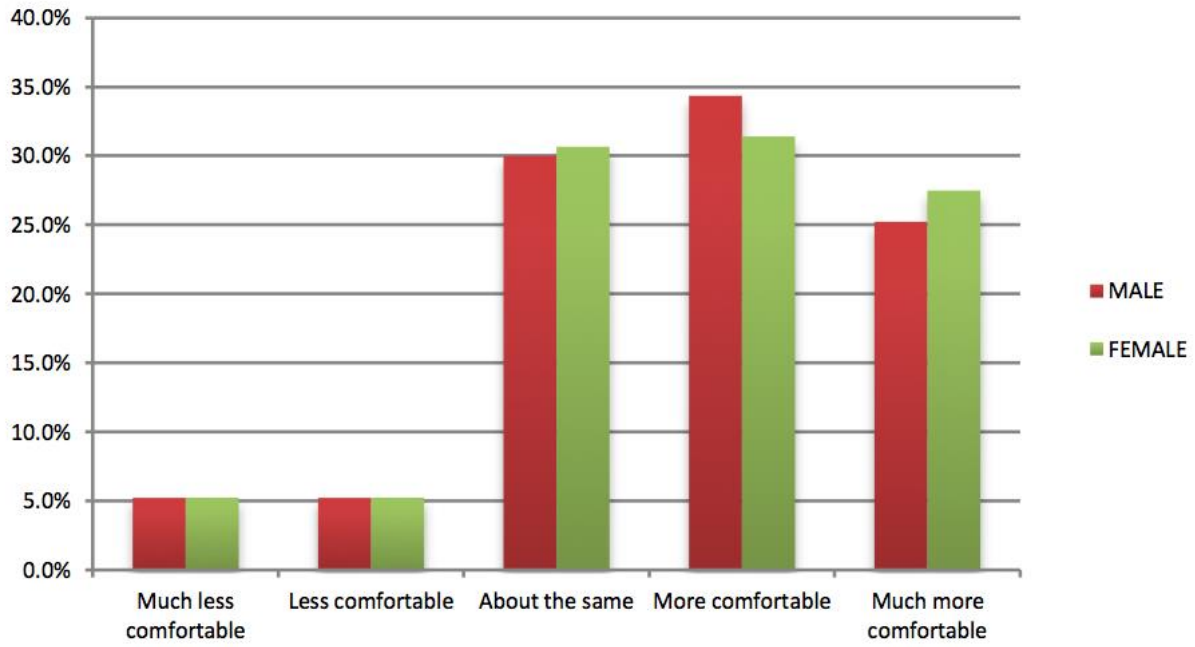


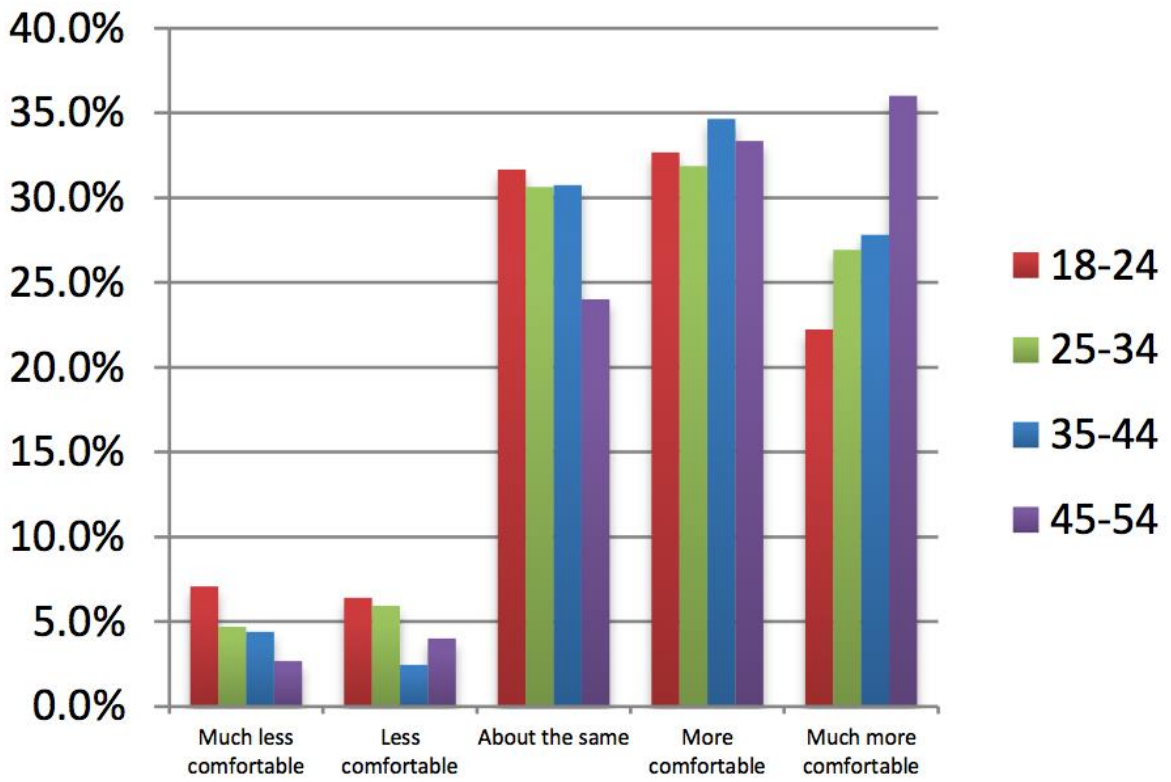
Again, the results per grouping are remarkably similar, with the only statistically robust difference being that considerably more 45-54 year olds believe that the Finance Director should be responsible for keeping card payment data secure than all the other age groups.

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

Response option	% response
Much more comfortable	**26.41%**
More comfortable	**32.73%**
About the same	**30.42%**
Less comfortable	**5.22%**
Much less comfortable	**5.22%**

Clearly, understanding that the card payment data cannot be heard/accessed is a key reassuring factor for nearly 60% of the survey sample. There is no significant variance between genders.





If we study the breakdown by age, it is clear that the communication of the benefits of being PCI compliant is a route by which to engage with all customers, but specifically the 18-34 age group given that almost 75% state that they would be more or much more comfortable about making card payments via the contact centre under these conditions.

So, what can we conclude?

Essentially we have 3 major takeaways from our first Insights research initiative:

- *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 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.*

These 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 compliant contact centre operations. Organisations that let their customers know how seriously they take card payment data security and educate their customers about what being PCI 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 and consequential revenue loss and reputational damage in the event of a breach.

So, what are you waiting for? If you have any questions about your organisation's PCI 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.

We hope you find this first Insights bulletin informative. Contact us if you'd have any burning questions you'd like to know the answers to, and we'll consider them for our regular insights research programme.