Briefing Note.
Consumer response to payment card data breach.
Phases 1 to 3 research summary.

Over the last 4 months Compliance3 conducted 3 phases of research securing answers from a cross section of 1,000 UK based individuals (providing a margin of error of c. +/- 2.7%).

The first phase of the research programme looked into *who* consumers 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 second round of research was focused on understanding whether consumers felt brands were doing enough to combat payment card fraud, their confidence levels about how data is being kept secure, and what they felt should happen to businesses that do not do enough to keep card payment data secure. Last but not least, 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 findings

Interestingly, 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. However, approximately 60% of respondents do 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.

The majority also felt that responsibility for card security should be all-pervasive throughout the organisation and a Board level concern. Over half of the respondents (54.71%) believe that key senior personnel and the Main Board are responsible for keeping their card payment details safe.

> 54.71% believe that key senior personnel and the Main Board are responsible for keeping their payment card details safe.

The degree to which consumers indicated increased comfort about their payment card data not being heard or accessed was significant, with 69.14% stating that they would be more comfortable of much more comfortable if they knew their payment card details could not be accessed by the call centre agent.

> 69.14% stated that they would be 'more comfortable' or 'much more comfortable' if they knew their payment card details could not be accessed by the call centre agent.

Results were very similar between age groups and gender, with the only difference being that the youngest age group seemed to be more aware of potential risk which results in lower trust in companies. Overall, a significant majority believe that companies are good at keeping their data secure which means that *if* they're subsequently proved wrong, then consumers will be tough on companies that have data breaches with 80% saying they should be publicly named and shamed.

> 80% of people think organisations that do not keep card payment data safe should be publicly named and shamed.

The research also revealed that from a consumer viewpoint, culpability for a data breach is attributed beyond the contact centre - even if the contact centre is the root cause – with the majority of consumers (41%) seeing the brand as a whole being at fault. A third of respondents, however, saw it being the responsibility of the payment card company.

Furthermore, the potential reputational damage and revenue losses are commercially significant, 41% would never buy from that brand again and in this world of connectivity, 55% would tell everybody that they knew about their loss.

> 41% would never buy from that brand again and 55% would tell everybody that they knew about their loss.

Far reaching implications

If we model 1st and 2nd generation connectedness and making some realistic assumptions on consumer behaviour, we estimate 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. Equally significant is that the findings of this research are consistent across all age groups and genders, which means big implications for all businesses.

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. Our research suggests there is a very real opportunity to increase credit/debit card payment activity by being overt about the levels of card security and fraud prevention in place by making people aware that the organisation operates PCI compliant contact centre operations.

Companies that let their customers know how seriously they take card payment data security and educate their customers about what being PCI compliant means 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.

For more details about our research or to find out about how we can support your existing data breach response plans, please get in touch.

www.compliance3.com