Call centres

The vulnerability:

Customers giving card details over the phone. This includes credit cards and debit cards, possibly bank account details for direct debit purposes:

By giving the details to a live but anonymous person, the customer has at that point lost control of their card details.

It's a trust based transaction. And trust is very hard to create and very easy to lose.

Even if the client trusts the brand, they don't know the individual telephone operative.

Some of these call centres are offshore, further complicating the situation, Compliance, law enforcement, and so forth. The call centre employees are perhaps on $200 per month in some instances, and recruitment practices may not be as thorough as one would hope. In the UK, call centre employees are paid an average of less than £16,000 per annum and can be on zero hour contracts. The temptations are huge, and according to Strathclyde Police "approximately 10% of Glasgow call centres have been infiltrated by organised crime".

Even if the call centre is trusted, and the individual operatives are all trusted and honest, hacking into the actual phone lines, or the database of call recordings 'for security and training purposes' would give a hacker absolute access to the card data. There's always a weak point. It's about accepting that, and strengthening each point in the chain.

Whist the message is usually that the customer is not the victim, it's the card company that loses money, this is only theoretical and not always accurate:

The credit card companies are responsible for reimbursement, but not if it's a debit card, and certainly not if it goes unnoticed by the customer for more than 3 months. Would you notice an extra £11.34 going from your account each month? Unlikely.

In addition, the complete card details can be sold on, and can even be used to purchase illegal items from the dark web, further exposing the legitimate holder to a completely new area of risk.

The risk to the brand:

A single incident would damage the public's relationship with the brand. Even a single instance can go viral on social media, it's out of the control of the brand what happens once the incident is media engaged.

If multiple instances occur, it easily can be picked up by mainstream media, gathering detractive attention in a snowball effect in a very short period of time. If the brand doesn't have a pre determined response strategy for this eventuality they will be reactive in their response, and damage limitation is unlikely to be effective.

If a systematic and professional criminal abuse has occurred, things can get really tricky. An example could be a rogue telephone operative concealing a microphone on their person to record every conversation they had for a month. Or a hacker 'harvesting' a database containing card data.

This would almost certainly result in high profile investigations by law enforcement agencies, possibly cross boarders, multiple regulators, multiple lawsuits, merchant claw back, and literally years of customer service repair work, litigation, and reputational repair. Investigation and remediation costs can run into millions – Talk Talk admitted to costs of £35m - plus consequential loss of reduction in new sales, loss of market value – Talk Talk's share price has recovered to 'only' 16% off its pre-data breach price - and loss of senior management expertise if heads are required to roll.

But TalkTalk is the tip of the iceberg. The Home Secretary recently said that "90% of large organisations suffered an information security breach last year" and, according to the UK Government's Department for Business Innovation and Skills "14% of respondents took more than a month to detect their worst breach of the year" the important words in that are 'more than a month' and 'worst breach of the year'.

Over to Compliance3:

Recent consumer research conducted by Compliance3 has found that, in the event of their data being compromised, nearly 40% of people would tell everybody they knew, with a further 16% adding that they'd spread the bad news on social media. And 41% of people surveyed said that they'd never buy from a compromised brand again.

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.

Compliance3 helps the call centre industry to deliver compliant customer contact take card data out of temptation's way. By deploying solutions where customers 'key' their card data into their phone so the agent never hears the card details (not even the keypad tones), we can then help companies protect customer payment card data. We can also help move any existing call recordings to a secure facility and 'cleanse' card data from recordings if they need to be accessed – for regulatory purposes, for example. For one client, we moved over 13 million call recordings off-site, and no card data now enters their environment. Find out more at www.compliance3.com, or email John@compliance3.com to request our new research paper: "The contact centre time bomb".