Fields Associates
Litigation Consultants

Speak directly to a qualified member of staff
0845 301 5778

The iPhone6 and NFC Payments: A Secure System?

It's official: Apple's latest phone, the iPhone6, has been unveiled and is now available for purchase. As you'd expect, the Californian computing group's latest effort possesses a number of new features: a larger screen, faster processor and superior battery life to name just a few. It's the phone's ability to serve as a wireless payment device that's caught our attention, however.

Now, contactless payment is nothing new – a number of banks have been providing debit and credit cards with the facility for over five years now - but, just like video calling and mobile internet browsing, features that are adopted by Apple tend to be embraced by a significantly larger number of people than they were previously. As a result, it seems pertinent to evaluate the potential risks of someone's iPhone doubling up as a debit/credit card.

The most obvious risk would appear to be someone simply commandeering someone's iPhone and going on a spending spree. Such concerns can be allayed by a number of sensible features, though. People will not be able to use their phones for purchases that exceed £10, will be required to verify themselves before the payment is made and Apple have also included a feature that allows a user to disable contactless payments remotely (via the Find my iPhone app) in the event of them losing their handset.

Notwithstanding the fact that an individual will be unable to deactivate this feature unless they are near a device that can access the internet, the most significant threat in the scenario described above comes if the person that has procured the victim's iPhone is technically savvy. Under such circumstances, it would be possible for the individual to utilise what are known as man-in-the-middle attacks. Via such an attack, it is possible to intercept and then clone the data that is exchanged between the phone and a vendor when a contactless payment is made. Following this, the individual that intercepted the data could, theoretically, manipulate it in order to make further purchases with little likelihood of them being traced. Such attacks can often be prevented via secure channels that decrypt the data that is being exchanged, though this does not remove the risk entirely.

Another possible risk stems from the prospect of the data that is being exchanged being intercepted and quickly altered. Under these circumstances, an attacker could redirect the funds that would be used to purchase goods to a bank account of their choosing yet leave the vendor thinking that they received the necessary payment.

Of course, no system, no matter how much time has been spent developing it or how robust it may initially seem, is immune to attacks. To consider every possible eventuality is simply not possible and, as the gaps that are present are exploited, they are in turn are addressed and the system becomes more secure.
What is certain is that this feature will, at some point, be abused. The extent to which it is misused and the damage that is caused, however, we will not know for some time.