There May be Trouble Ahead for Mobile Commerce

(Original creator: bolarotibi)

By Clive Howard, Principal Analyst, Creative Intellect Consulting

With the Christmas holidays just ahead of us there will undoubtedly be new figures showing that e-commerce has once again generated more revenue and accounted for more of the holiday spending than ever before. The same figures will also probably show a rise in the amount that was spent via mobile. M-commerce (mobile e-commerce) has been steadily rising for a number of years and most predictions are that it will continue to do so. However recent data points to a tapering off of growth in M-commerce over the next few years. This could be significant with growth rates barely rising at all by 2017 and stagnating at around 30+% of total e-commerce spend. The key questions for many organisations should be however, why and how can they potentially buck this trend? A number of recent surveys by eMarketer show that there are two key reasons why people are growing reluctant to buy online using mobile devices. The first is **security** and the second is the **user experience** of mobile transactions.

Consumers don't have faith in the phone…

The security issue is a significant one and is only becoming more so. With recent high profile breaches such as that of iCloud (although not Apple's fault) and Target stores in the US, consumers are becoming increasingly aware and concerned about security online. This is accentuated when it comes to smartphones. They are right to express concerns as the last year has seen 167% increase in mobile malware with McAfee estimating 200 threats per minute. The Android operating system which is installed on 80% of all smartphones shipped has been especially susceptible to such attacks. Some figures put "rooted" Android devices at 20% of the total. A rooted device gives rogue agents potential access to data stores on the device with the ability of data being entered into device or being passed to and from the device. Google is addressing these issues and Android is not the only mobile operating system to suffer from security challenges. For example, Apple's much touted fingerprint recognition sensor was cracked shortly after launch. Technology has responded to try and address these concerns. For example, mobile wallets (such as ApplePay, Google Wallet and PayPal) try to avoid the need to input and store payment data on the device. Apple's latest ApplePay mobile wallet does not store credit card data either on the phone or in the cloud. Instead an alternate version of the credit card information is stored in a secure element on the phone. If there is a breach, such as a lost device, then the payment information can be cancelled without cancelling the credit card itself. Mobile wallets which also work in conjunction with physical payment mechanism such as Near Field Communication (NFC) where you only need to put your mobile device in close proximity of the payment terminal are widely seen as the future of mobile payment.

When they don't even trust the technology leaders in mobile payment…who do they trust?

The challenge is that data shows people do not trust most of the mobile wallet providers. Apple, Google and even PayPal are only trusted by approximately 20+% of consumers according to eMarketer. So while the technology addresses the security challenges the consumer is less likely to put their faith in it. Surprisingly this issue cannot be put down to age. People in the 25-35 bracket are more likely to try a mobile wallet than those in the 16-24 age group. Some of this might be down to available income but younger generations often show greater awareness of security issues and therefore more likely to take precautions such as not using them. When asked who they would trust with regards to mobile wallets almost 80% of consumers answer banks or credit card companies. These organisations are now starting to enter into this market. Therefore development teams should start looking into mobile wallets, particularly those provided by banks, as a method for taking payment on mobile devices.

Mobile payments are simply too hard

After security the next significant issue that is deterring users is the experience of paying via mobile. This is especially relevant to smartphones. In a recent survey IBM found that while consumers use smartphones to research purchases far more than tablets, the reverse is true when it comes to actually making a purchase. A clear reason for this is the difference in the form factors, in other words tablets are larger devices than smartphones. I'm sure that we have all tried entering data using a smartphone and have probably found it difficult. The small screen size often combined with touch keyboards make entering any significant data awkward. When it comes to making payments in the traditional way, using a credit card, the amount of data that needs entering is a lot. There is not just the card information which includes the long number but also address information. In total this process often involves a combination of character entry and drop down list selections. With websites this can be particularly problematic where they do not correctly fit within the confines of a small screen. Surprisingly even some websites optimised for mobile do not fit all screens. Then there can be the issue of the underlying code, especially the use of JavaScript which can sometimes not work as expected within mobile browsers. In a Jumio survey, 23% of people reported having a transaction fail to go through on mobile. This represents some kind of technical problems affecting mobile. This is not surprising as there are a large number of different devices available running a number of different versions of operating systems. In many cases these operating systems have been customised by handset manufacturers of telco networks. In addition there are new devices and updates to operating systems becoming available very regularly. The result is a very large number of potential environments. Testing all of these is near impossible and many organisations only test on the most popular according market statistics. Such problems with the experience of making a payment leads customers to lose trust, which in turns raises even greater concerns over security.