FRAUD IN THE MOBILE PAYMENT INDUSTRY

March 12, 2012 by Nick Brown

The hottest emerging technology to hit the payment industry in years is mobile payments, and yet this year the momentum has stalled. Why is this? Could it be because of the fear of fraud?

Smartphone use in the U.S has been rocketing in the last couple of years, and is now around 50% of all phone users and growing rapidly. There are also several mobile payment initiatives available, with companies like eBay and PayPal showing interest in adopting mobile payment systems. Everything seems to be perfect for a huge push to take advantage of smart phone adoption with mobile payments. Why isn't that happening?

Consumers Skeptical About Smartphone Security

The problem seems to be a fear of fraud. According to a new survey conducted by Radius Global Market Research, "While the number of smartphone users has exploded to nearly 50% of all U.S. consumers, the majority of Americans remain quite skeptical of smartphone generated payment solutions, and in the near-term are not likely to give up traditional forms of payment." The survey also found "Half of all American consumers say potential security and fraud significantly influence their likelihood to use smartphone technology to make purchases in the future. In comparison, only 14% say security and fraud don't influence their future likelihood to make those purchases."[1]

Security is starting to be a problem for smartphones. Malicious code has already been found in many Android apps. Once an app is installed, it can record all calls and texts, and potentially record personal data related to banking and credit cards. Robert Siciliano, a McAfee consultant and identity theft expert, says "The low hanging fruit is still the PC. If you are a criminal hacker, Microsoft's OS is the most hacked software on the planet." However, this is likely to change to include mobile hacking. Steve Santorelli, director of global outreach at the Internet security research group Team Cymru, and a former Scotland Yard police officer says: "If I had money right now, I'd bet on the Russian mafia. Mobile hacking is going to be huge."

Current Mobile Payment Systems

There are currently two main variations of mobile payment systems, both using Near Field Communication (NFC). The first method requires the user to wave their phone at the point of sale (POS) device in the store and their credit card information is sent from their phone to the POS device, and the transaction is performed per usual by the merchant. The second method requires the user to wave their phone at the POS device in the store, the transaction is transmitted from the POS device to the phone, passed to the mobile carrier that has their credit card, and the credit card transaction is performed by the mobile carrier. In both of these variations, the mobile device is an added

[1] Radius Global Market Research: Feb 29, 2012: Study: Consumers Unlikely To Abandon Wallets In Favor of Paying with Smartphones

component to the transaction, adding the potential security problem of the device itself being hacked and manipulated.

Chip Lister, Managing Director of Radius, recognizes the real problem for alleviating the concerns of consumers with regard to mobile payment systems: “While marketers have done a good job at promoting convenience, they will also need to boost messaging efforts to address security concerns in a way that convinces digitally savvy consumers.” However, the source of the marketing matters when is comes to financial fraud.

Financial Institutions Must be Part of the Solution

When credit card fraud was a problem, it was the financial institution that guaranteed transactions taking place on their cards. A similar approach is necessary with mobile payment systems in order to satisfy the concerned public. The financial institution must support and guarantee the payment system to consumers. None of the current mobile payment systems involve financial institutions in the process, and therefore are unlikely to succeed.

With the recent product launch of Chase QuickPay, it appears that the banks are clearly interested in getting involved in mobile banking services. However, in order for a bank to adopt a mobile payment system there are three key areas of concern:

- They have to be be comfortable with any additional risks they are taking on. This means they need to have an element of control over the mobile payment process, and be able to control the risks.
- They have to see some benefit for themselves. Ideally, the mobile payment system should be a revenue generator for them.
- They have to be able to market it as their own. This would require the banks having a direct relationship with the consumer regarding the mobile payment system.

Fraud remains an impediment to adoption by both merchants and their customers until the financial institutions adopt and support a mobile payment system.

Nick Brown has been in the payment industry for over 20 years, and is currently CEO of ClearPurchase, a guaranteed fraud-free online and in-store mobile payment system. Nick can be contacted at nick@ClearPurchase.com.