



As We Move Toward 2015 - Is the Vision of Client-Centric Mobile Banking and Payments Realizable?

By Greg Walter CEO, Qpay

In 2015 it is projected that we will no longer be able to send checks, we will rarely enter physical banks and that most transactions, bill payments, purchases, banking transfers and even funds trading will be carried out over the mobile phone. We will pass through a toll road and the amount will be deducted through our phone, we will send transfers to our relatives and friends both locally and internationally via mobile and we will pay for our parking and other bills, access retail cash cards and even pay our library fines, if libraries still exist that is, via a mobile device. Even in remote or impoverished areas where carrying cash is more risky and banking and internet infrastructure is weak, the broad based adoption of mobile phones will enable cash to be gradually replaced by some kind of a mobile payment system.

Whether this vision becomes a functional reality or is relegated to an awkward patchwork of technology overlays will be largely decided by December of 2013. Why this date? Because by the end of that year we expect that a serious investment will have been made by most every bank, financial institution and most social networks in some kind of mobile payment technology in order to meet growing customer demand. And, once a corporate commitment of resources – personnel, infrastructure and technology etc., has been made, changing that core technology for at least the next five years or so is probably unlikely, even if something much better comes along.

So, patches, post-implementation security layering or last minute updates notwithstanding, it's absolutely essential that the mobile transaction technology that is chosen in the next two years is the most effective one to deliver what users want.

The mobile banking market is competitive but only delivering the best technology will enable the current market players to hold market share and grow their customer base.

What are consumers looking for? In short, safety and convenience. They want to know that their funds are safe, that their client information cannot be stolen or intercepted and that protecting this information will not cause multiple layers of passwords, security screens or hoop jumping to get the transaction done. Further, as numerous transaction options become available via mobile device, interoperability will become increasingly important to customers. They will expect to be able to customize their own mobile transaction platform to suit their own needs and not just the needs of the provider. I.e. The system must allow them to access multiple cash and credit accounts at different banks and credit institutions and allow a variety of different types of worldwide transactions.

The mobile banking market is competitive but only delivering the best technology will enable the current market players to hold market share and grow their customer base.¹

US financial giant, Fiserv calls this “a more holistic, enterprise-wide mobile financial services strategy” and noted in 2009 that considerable return on investment would be available to those financial institutions that could make the shift from simply enabling basic transactions through cell phones to implementing a comprehensive mobile financial services solution.

So what will a consumer-orientated integrated mobile banking and payment platform look like? What security features are available to protect mobile banking customers and what might constitute interoperability.

¹ The Business Case for an Enterprise-Wide Mobile Financial Services Strategy- Fiserv, 2010

Here at Qpay, our development efforts since the firm's inception in 2006 have been based on the concept of providing the highest level of information privacy and protection through multifactor security and out-of-band authentication as well as ease of operability.

Ease of use is not a function to be underestimated—consider how complicated passwords are eventually discarded or replaced with more simple and memorable logins, even at the risk of undermining the entire system's security.

Many industry experts speak of user complexity and high level security as if these two concepts must go hand in hand. This is simply not the case. We have developed an authentication system that provides Tier 1 security, (the highest level of security aspired to by banks) that is native to the mobile platform, that also facilitates all of the items introduced in the 2015 wish list at the beginning of this article.

Here's how it works. A client can establish an account either on line or over the phone. This account information is stored separately from the internet on three partitioned and encrypted platforms. This set up ensures that the client's private information, their privacy profile, cannot ever be accessed at the same time, in line with NIST privacy protection requirements.²

Once this account is set up a customer can carry out all the typical functions of a mobile banking site—account balances, payments and transfers between in-house accounts etc. without entering any further private information. But in addition to these typical functions they can then add a new bank, a new vendor or a new P2P transfer recipient and conduct their entire suite of daily transactions seamlessly. Account set up takes only about ninety seconds the first time and just a few seconds as subsequent recipient details are added.

Then as each transaction is conducted it is verified using out-of-band technology. The client is contacted through their mobile phone's SMS service and asked to do one of three things – verify and accept the transaction, reject it or report it as fraudulent.

This verification can also be done through biometrics if required. A voice print is made when that account is set up and when transaction verification is required the customer is asked to say a random word to authenticate. The word is compared to a voice print of the client's voice and no particular word or phrase is used more than once so a reproduction of the voice will never be acceptable.

By implementing this thorough structure we have made a system that is safe and secure that we believe will enable the next generation of client-centric banking and payments to be realized.

About Qpay

Qpay is an integrated mobile banking and mobile payments company that offers Tier 1 authentication technology native in the platform. Tier 1 security requires a combination of several security factors in each transaction and is recognized by banks worldwide as the highest and most desirable level of security. Because this "multifactor" user authentication is native to the system, it requires no additional client-facing layers and Qpay is able to deliver a simpler, faster, safer customer payment interface with greater functionality, at considerably less cost.

Qpay security factors include:

- Out-of-band (mobile call or SMS) transaction activation and verification
- Random password that is delivered by SMS or voice
- Response by SMS or voice – as a random word is requested and compared to a unique voice print, the biometric cannot be reproduced
- Multi-level partitioning and individual encryption layers separating all confidential information from the user interface

Qpay's technology functions in all digital environs, with all mobile phone types as well as with traditional hand set systems. Account set up takes less than 90 seconds; funds are available immediately and the system supports multiple languages, multiple currencies and multiple funds sources. A client can use the same system to securely make any payments, carry out all banking functions on any of their banking accounts, and transfer funds globally or locally, as well as many other uses. Once the initial account is established, new user options can be added by the consumer within seconds.

² http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf