



## ***Will Multi-Factor Security be the Answer to the Next Generation of Mobile Security Threats?*** By Greg Walter (CEO Qpay)

Having experienced the internet and mobile banking world for several years now, the average customer accessing financial services via the internet is well aware of the issues surrounding secure identity. Several recent incidents of fraud at the world's largest banks, identity theft on the Sony Playstation site, illegal access to the RSA platform, hacking issues relating to the US military and hacking scandals in the media keep the issue in the headlines and ensure that security remains front of mind for consumers.

So what are the traditional authentication options and will these be sufficient to meet the future security needs of a consumer that is increasingly embracing mobile transactions?

The first line of defense in the security tool kit is encryption, the process used to transform information into a less accessible algorithm or cipher. Encryption can be used to protect data in storage and data in transit and, while it is generally regarded as an essential part of information security, there have been numerous reports of data in transit being intercepted over the years.

The second phase of information security is authentication. Authentication requires customers to provide valid identification data followed by one or more authentication credential, also known as factors, to prove their identity.

Password and PINs (*something a person knows*) are the most widely used authentication factors.

Additionally a picture or a random word visible only to the user may also be used to authenticate the transaction and move it forward. However, this single factor authentication is also the most vulnerable to online phishing, pharming and malware where customers are tricked into accessing and giving away security information on fake sites, or they use insufficiently complex or easily guessed passwords for the sake of convenience.

To facilitate online transactions banks added a second factor - tokens (*or something a person has*) several years ago. Customers can use a smartcard, a password-generating token or similar device to generate a random password and authenticate their unique identity.

*Mobile banking and social networks are expected to pose new security threats in the payments space in 2011. But security experts say those threats won't displace the Zeus botnet, malware attacks and phishing threats, which for years have plagued banking institutions. Fraud attempts will escalate, not diminish, as new threats and channels blossom in 2011.<sup>1</sup>*

Biometrics, i.e. finger print, voice print or retina scanning etc. are a third factor or unique identifier that is used for authentication. Biometrics provides *something a person is*. These biometric measures have varied in effectiveness over the years mostly constrained by "reproducibility". Reducibility is the ability to use a copy instead of the actual item for example a picture of an eye to get the same result as the actual retina scan or a recording of a word to be used by a fraudster instead of the actual voice of a customer.

<sup>1</sup> [http://www.bankinfosecurity.com/articles.php?art\\_id=3091](http://www.bankinfosecurity.com/articles.php?art_id=3091)

Out-of-band authentication is a way to add further strength to the authentication layers by using a remote device or separate channel to contact the user and verify their identity. For example a person carrying out transactions on line could be called via mobile or sent a text message to authenticate the user identity or to verify the accuracy of a transaction.

*Currently, most financial institutions do not authenticate their web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack.<sup>2</sup>*

The immediacy of out-of-band feedback also offers a considerable benefit in terms of fraud detection and fraud elimination as the two sides of the transaction can be mutually authenticated and a fraudulent transaction can be immediately reported.

As more transactions are carried out on mobile devices and through less secure sites like social networks, authorities expect to see transaction fraud, site phishing and other criminal activities rise exponentially.

Whether or not the mobile device is in itself less secure than its online counterpart or whether fraud opportunities increase if a mobile device is used for web browsing, security concerns remain one of the key issues constraining widespread adoption of mobile transaction platforms.

Certainly, the incidence of man-in-the-browser,(MitB) also known as man-in-the-middle, schemes that target two-factor authentication are expected to rise in lock step with the increase of mobile payment devices. However, out-of-band authentication also offers a countermeasure to this as attackers are less able to intercept both ends of a connection and reroute funds. Similarly, we will probably also see an uptick in the incidence of skimming, given the capacity of mobile devices to easily capture and redirect credit card information.

Whether it is fraud or phishing the one area where regulators and industry experts seem to agree is that a more robust authentication system needs to be achieved to move the mobile payment industry forward. So far the front runner being advocated by regulatory authorities is a system that utilizes a combination of factors from the various layers, multi-factor security and some form of out-of-band security. Moreover, officials suggest that customers are more likely to adopt payment technologies if this integrated security is easy to implement and native within the payment platform.

## 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 the multifactor user authentication is native to the system, this security requires no additional client-facing layers and Qpay is able deliver a simpler, faster, safer customer payment interface with greater functionality, at 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.

<sup>2</sup> *Authentication in an Electronic Banking Environment* (2001 Guidance) Federal Financial Institutions Examination Council