

P E R S P E C T I V E

Making Mobile Transactions
Safe for All



YOUR INNOVATION PARTNER

Mobile Banking Evolution

Improving customer convenience and reducing channel costs are two of the most important drivers of banking innovation. The ATM was introduced in order to divert routine transactions from the branch; however, when competitive and cost pressures mounted, as did the load on expensive ATM infrastructure, the industry yearned for a more effective alternative. This came in the form of the short message service (SMS) which enabled a reasonably mobile-savvy customer base to initially make routine enquiries and progress to more complex operations, such as funds transfer and bill payments, using their mobile phone keypads. No doubt, SMS banking reduced ATM footfalls, yet, had its glitches which made it less than 100% reliable or safe.

Security became the bugbear of mobile banking. In time, mobile transactions progressed to WAP and browser-based banking, which improved the security and user experience on sophisticated handsets to some extent, but excluded the basic devices altogether. The arrival of downloadable mobile applications circumvented many of the earlier issues - since apps could be used on most handsets, they made mobile banking more inclusive. They also enabled the best possible experience within the limitations of each device.

These developments marked the evolution of the mobile phone into a transaction instrument. A global analyst firm estimated the growth of worldwide mobile payments in 2009 at 70%. They also predicted that nearly 200 million people, or 3% of mobile users, will use m-payments by 2012. Expectedly, Asia and Japan will lead this growth to achieve nearly 4% penetration; whereas that figure will touch 2.5% in markets of Western Europe, historically, laggards in this space.

U.K Developments

In the U.K., mobile transactions are making a second entry. Some months ago, Barclays took mobile financial transactions up a notch, pioneering a third party payment service as well as tying up with the Oyster transport ticketing card to enable their customers charge payments made at Oyster terminals using an NFC-enabled mobile phone, directly to their Barclays debit or credit card. The success of this tie-up prompted the U.K transport authority to think about how, in future, mobile contact-less payments could be made the preferred mode of transaction authorisation, replacing RFID

technology. Wonga, a U.K-based online credit start-up launched an instant short-term loan facility allowing customers to apply for small-ticket loans of up to 1000 over the mobile phone, without going through an elaborate application and authorization process. They claim that the money is paid out within 15 minutes. Last year, wireless telecom provider, O2 entered the mobile banking space with the launch of prepaid cards.

Mobile Security Measures

Expectedly, the growth of the mobile delivery channel sparked security concerns. Basically, service providers had three security priorities:

Authenticating the identity of users. Towards this end, they asked customers to present information that only they would be privy to, for example, a Personal Identification Number.

Ensuring that the mobile device was not replicable. As GSM phones and SIM cards were particularly vulnerable to spoofing, every mobile device was assigned a unique PIN number to provide a second-level authentication.

Securing data transmitted over SMS networks. Since data was transmitted in unencrypted format over SMS networks, hackers could easily tap into it using a simple transmitter-receiver device. WAP or browser-based banking improved the security of data by encrypting it, and also enhanced user experience; however, as mentioned earlier, it could not run on older handsets.

Mobile applications took security forward, allowing large volumes of encrypted data to be exchanged safely. However, one question still remained – how could the data on a phone be protected in case the device was misplaced? The response of financial institutions was to encrypt that data as well and store only ‘nicknames’ or pointers and non-critical information on the phones.

But, while security was important, banks and other service providers realized that it could not come at the cost of user experience. A cumbersome 2-factor authentication or the need for an RXX token to trade SMS would only drive customers away. As of now, banks are still trying to resolve this conundrum and by trading further security enhancements for better experience, they may be exposing mobile transactions to somewhat higher risk.

Mobile Payment Security Concerns

The issue is complicated by the evolution of the mobile phone from just a banking device to a payment instrument. Mobile payments - built up in the U.K by the likes of Citibank, Visa, Mastercard, Barclays and Oyster - are the next generation, adding a business dimension to the security paradigm on top of the technological one in the case of mobile banking. For instance, proximity payments, in which the paying and receiving devices are physically near each other, present different concerns from non-proximity payments, where the mobile acts as a communication and authorization device to facilitate remote transactions. While both are gaining importance in the U.K, non-proximity payments may jump manifold if the intent of CEPA and GSMA Europe to enable cross-border mobile payments within the continent becomes a reality- which makes it doubly important to address its risks.

One of the key risks associated with the loss of a mobile payment instrument is that any sensitive information stored on it could be subsequently misused to steal money or even identity. Hence, data security is a paramount concern. So is proper identification of the source and destination in a money transfer, more so when money is laundered or terror financed by way of innocuous looking small-ticket payments.

Other Security Approaches

Banks are addressing these issues through the use of firmware-based security elements. The first of these is a smart card-like SIM with an in-built security application to store customer data. However, it is clearly not feasible to replace the SIM cards of all mobile phone users. Also, NFC or proximity payments require handsets to have the inherent capability to communicate with receiving devices. Therefore, the use of a secure element SIM card in a proximity transaction is handset-dependent and could adversely affect user experience. A secure SD or memory card is an alternative to the SIM card-based secure element. It provides similar protection as well as the added benefit of universal applicability - existing handsets can be SD-enabled by simply attaching a peripheral device. An innovation in the form of an inbuilt NFC antenna provides security for proximity transactions.

Banks are also resorting to the traditional method of personal verification for certain customer segments. While rural or low income customers

have started using SMS-based payments, their transactions are usually facilitated by a bank representative. In such cases, the representative can provide an additional layer of security by verifying the source and destination of funds. This is not a novel idea - credit card companies advise merchants to demand photographic proof of identity from dubious customers. That being said, this method of labor-intensive verification is probably more appropriate to the developing world than the U.K.

Besides adopting various practices such as encryption, limited on-device data storage, 2-factor authentication etc., financial institutions are collaborating with regulators, payment authorities and telecom firms to ensure KYC compliance in order to prevent unlawful activities such as money laundering and terror financing. They are also moving towards greater regulation of the P2P lending space with the goal of making it more secure in future.

Conclusion

Till now, banks have taken several measures to secure mobile banking and payment transactions. The diversity of mobile handsets - from the very basic SMS-only phones to a huge number of intermediate phones to the sophisticated iPhone and BlackBerry, which support encryption and safe storage/transmission - makes it impossible to adopt a single universal security solution. Hence, banks have no choice but to take a multi-pronged approach, relying on technology, regulation and infrastructure as needed, to ensure that transactions on every type of mobile device are made more secure.

They will need to collaborate with a number of other parties in this endeavor - technology vendors for platforms capable of working with all types of devices and telecom firms and payment authorities for KYC compliance at the mobile-subscription stage. Improved transaction security will go far in making mobile banking and payments ubiquitous and universally preferred.

Author

Kiran K. S. R.

Product Consultant – Finacle
Infosys Technologies Limited



YOUR INNOVATION PARTNER

PERSPECTIVE

Universal Banking Solution | System Integration | Consulting | Business Process Outsourcing

Infosys Technologies Limited

Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100. India
Tel.: + 91 80 28520261, Fax: + 91 80 28521747, e-mail: finacleweb@infosys.com
www.infosys.com/finacle

Join us on Twitter, LinkedIn and Finacle Whiteboard at www.infosys.com/finacle/networking.asp

"COPYRIGHT NOTICE: Copyright ©2009 Infosys Technologies Limited, Bangalore, India. ALL RIGHTS RESERVED."
Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.