A competitive market for interoperable mobile wallets

An SPA Position Paper

March 2015

1. Introduction

Mobile Wallets constitute a good example of the way innovation is becoming a focal point for payment system development and enhanced competition. Providing banks and other institutions with a broad range of strategic options for gaining market share, Mobile Wallets make it possible for organizations to join forces and issue cobranded wallets. These options include: a proprietary wallet connected to a proprietary platform developed using an organization's own research and development; joint ventures; venture capital investment; and alliances to develop a proprietary or public ISO standard.

Each strategic option carries its own costs and benefits. However, as technology vendors, the SPA membership is concerned that a "wallet war" may result in excessive market fragmentation. We've already seen the lines of engagement being draw. Currently the market is populated by Google Wallet, SOFTCARD, MCX, Visa's V.me Wallet, MasterCard's MasterPass Wallet Services, Apple Passbook, PayPal and American Express' Serve. The battlefield expanded last year with the 2014 launch of Apple Pay, and more recently through Samsung's February 2015 acquisition of LoopPay.

This diverse set of wallet technology offerings will continue to co-exist until users decide which business model will dominate the market. However, the already high level of fragmentation raises the question as to whether an industry-led standard that contains a security framework and is flexible enough to accommodate different business models could boost adoption of the Mobile Wallet.

This paper discusses the nature and expected functionalities of the ideal Mobile Wallet. With respect to terminology, digital wallet' is sometimes used to refer to a wallet stored in the Cloud; this paper does not differentiate between Mobile Wallets and Digital Wallets. The object of this paper is not to discuss access methods to the Wallet ie. NFC, HCE.

2. The Mobile Wallet is more than a new payment financial service

There is still no consensual understanding of what comprises a Mobile Wallet, but the payments industry is progressing in this respect. For instance, the new ISO 12812-2 Mobile Financial Standard that is currently in development offers the first standard definition for wallets.

To fill this gap the SPA proposes the following definition: "A logical repository securely stored in a mobile device that enables the customer to manage different mobile payment instruments as well as personal credentials, resident either in the mobile device or in a remote server". Mobile Wallets are designed to take advantage of the social acceptance and the enhanced interconnection capabilities of a new generation of mobile devices.

Ultimately, the "raison d'être" for the Mobile Wallet lies in its ability to link a mobile device to a wide variety of cards and, potentially, other payment instruments. Mobile Wallet services typically include user authentication alongside other additional functions such as transit, vending, ATM and loyalty services. The combination of these functionalities constitute the bricks and mortar for offering a cluster of mobile financial services extensive enough to cover the day-to-day needs of a customer. Using a Mobile Wallet, holders can make online and offline payments, use e-banking services, add e-money to a local wallet or e-purse, redeem e-money, check payment account balances, view transaction histories and use location-based features.

The Mobile Wallet may be designed as a repository for a single application and personal credentials to manage a payment instrument (for example, mobile electronic money). Or it may support multiple payment instruments - offering sophisticated management options that are directly controlled by the cardholder –all of which require different access conditions (like a proportionate level of user authentication).

In developing countries a Mobile Wallet might be designed with a social objective in mind; for example, facilitating a mobile payment instrument for the unbanked population. To a lesser extent this is also true for developed countries, where a significant percentage of the population remains financially underserved.

The Mobile Wallet also represents a real enabler for mobile financial services by facilitating customer selection and access to applications. The Mobile Wallet is not a technology revolution "per-se", but potentially offers an elegant way to shop online by enabling the Wallet issuer to capture customer shopping data. In itself this offers grounds for a robust business case.

The specific nature of the financial services offer is dependent on the business model of the Mobile Wallet issuer. Differentiation that will create the field for competition will arise in the (1) financial services offered, (2) value-added features, (3) convenience and (4) perceived security.

However, this service integration ability has some significant consequences for both offer and demand sides:

1. Mobile Wallets have the potential to change the customer daily experience, establishing their preferences for particular payment instruments and making it possible to manage finances on the go; and
2. New Payment Service Providers (for example, Retailers) might take over the primary relationships with consumers and merchants if they are able to issue and operate attractive Mobile Wallets.

Clearly, Mobile Wallets have the potential to initiate payment disintermediation. The processing of payment transactions initiated from the wallet takes place outside of traditional card payment systems, using the systems operated by non-financial institutions that may, in some instances, fall outside of regulation. Thus, Mobile Wallets may house payment instruments issued by both regulated and unregulated institutions (this is more likely for online payments), which creates an interesting case for competition between banks and non-banks in the retail payments market.

3. Profiling the ideal Mobile Wallet

A Mobile Wallet with the following features would maximize the likelihood of widespread user adoption:

- Ease of use and convenience

Overall convenience is likely to encourage consumer adoption of Mobile Wallets for payments. In respect of design, this will mean providing a user interface that enables the easy selection of payment instruments. It also the Mobile Wallet will need to feature other relevant 'convenience' characteristics such as speed, payer control, perceived and real security as well as general acceptance by merchants.

- Deliver evident user advantages for payers

These advantages relate primarily to the payment applications accessible from the wallet, which should support the ability to:

- manage or control spending by providing payment account consultancy services
- receive only targeted advertising and promotions
- enable users to select the most rewarded payment service
- keep track of user-authorized transactions
- allow users to place card payment credentials of their choice into the wallet, as long as these comply with the security policy of the wallet issuer.

A further use case includes allowing consumers to obtain credit at no cost or at a marginal cost. Such a service could represent a key market differentiator, but the conditions for granting a credit line may be subject to strict regional regulatory provisions.

- Support "Universal" acceptance

From a user perspective, "universal acceptance" will mean:

- users may pay for any good and service
- in a physical store or remotely
- in a merchant acceptance context or for person-to-person payments.

From a technical point of view "universal acceptance" will mean interoperable solutions based on international standards.

- Strong authentication capabilities

Strong authentication for both Internet and mobile payments is required by European regulators for obvious customer protection reasons. Not surprisingly the European Banking Authority guidelines, published in December 2014 (R9), mandate strong customer authentication to log-in to wallet payment services.

The SPA position is clear: storing the Mobile Wallet in a hardware tamper resistant device such as the Secure Element is the best guarantee for the integrity of resident payment applications, as well as keeping the mobile wallet under the exclusive control of the legitimate customer.

- Transferability

Functionality must be in place to ensure that Mobile Wallet services and associated information are not lost when customers decide to change his/her mobile device or move to a new mobile network provider.

- Benefits (rewards) linked to the use of Mobile Wallet

If the Mobile Wallet is issued (owned) by the MNO, it will be easy to offer usage rewards. When a Mobile Wallet is issued with m-commerce payments in mind, the extra-revenue generated by an increase in sales thanks to the fact that paying with a Mobile Wallet is easy, could be partially paid back to the consumer.

- A high level of consumers and merchants protection

News stories relating to the collection of personal data by national security organizations is likely to trigger consumer interest for anonymous electronic payment means. Indeed, there is a perceived risk of impersonation by users of remote online payments that could make anonymity appealing for certain types of payments. On the other hand, especially if implemented in a Secure Element, the mobile wallet may feature electronic signature services to prevent the repudiation of legitimate authorized payments, minimizing merchant's financial chargeback losses.

- Offer a cost advantage for merchants

No fees or additional fees related to traditional card payments should discourage the adoption of Mobile Wallet payments by the merchants. Depending on how payment services are implemented, merchants may no longer need to store sensitive customer payment data that reduces the perimeter for PCI-DSS certification. Finally, an attractive liability regime on fraudulent transactions should be contractually proposed to merchants to incentivize the acceptance of Mobile Wallet-based payments.

At present no Mobile Wallet on the market features all the above functionalities, but designing the "ideal wallet" will probably not be enough to gain a dominant position in a highly competitive payment market where new products and solutions are constantly being announced. Ultimately, only a few will successfully generate the volume of transactions required to become profitable and survive.

Payment system transformation has become an urgent need for many financial institutions at a time when it may be difficult to adapt their long-standing systems to the growing demand for anywhere, anytime banking and payments. As a result, other major financial and non-financial players (Telcos, IT vendors and Retailer Associations) are competing strongly for a position in the mobile wallet value chain.

This raises three questions that are addressed in the following sections:

1. Which marketing strategies are likely to stimulate Mobile Wallet adoption?
2. How does the Secure Element solve many of the functional and security issues?
3. Would a new standard boost the Wallet market?

4. Marketing strategies to boost Mobile Wallet adoption

Mobile Wallet market growth is well below forecast, with early Mobile Wallet implementations and adoption proving disappointing. It has been argued that too many technology choices confuse customers, despite the fact that most Mobile Wallets on the market today offer incentives with merchant deals and loyalty programs.

As discussed in the previous section, convenience, perceived security and zero cost are key features for consumers. However, while the design of the "ideal" Mobile Wallet encompasses all the features needed to stimulate mass user take-up, the fact remains that recent market surveys in developed countries (R8) confirm the conservative behaviors of payers. Today's consumers already have a number of electronic ways to pay and any new payment method and/or payment instrument must demonstrate clear advantages.

The dynamism of the Mobile Wallet market offer side can be interpreted in a variety of ways. The technology is perceived as having the potential to ignite NFC mobile payments, representing a kind of "killer use case" if you like. On the other hand, Mobile Wallets have been around since 2010 and no one wallet solution appears dominant today. It's a scenario that's incentivizing new entrants to try out new business models, backed by aggressive marketing campaigns, in a bid to capture and dominate the market.

Apple and Samsung, the most recent entrants in the battle for the Mobile Wallet market, are intending to succeed where Google, PayPal, Square, SOFTCARD and others haven't. Although recent announcements that the Google Wallet app will come pre-installed on Android phones offered by major US carriers AT&T Mobility, T-Mobile USA and Verizon Wireless will certainly strengthen the Mountain View company' s position.

That said, the IT technology revolution has shown that business models emerge fast but evolve slowly, coexisting with former ones; all the current incumbents hold a platform with other developers writing and provisioning applications.

So, why are Mobile Wallets so appealing from a business perspective? In essence, Mobile Wallets present multiple opportunities for revenue stream creation – revenues which depend on high customer numbers and an average volume of transactions being undertaken by individual customers.

That said, Mobile Wallets offer the potential to create a large core of loyal users thanks to their potential ability to integrate wallet services into customers' everyday tasks and lifestyle preferences.

Today it's proving easier to create a new innovation than it is to ensure its profitability – and market entrants need to consider this hazard and seriously assess options for sharing risk with other partners.

1. Mobile Wallet issuers are in a position to collect a lot of information on the consumption and payment habits of users – an asset that represents high economic value for both financial and non-financial entities and which is incentivizing business collaborations in joint ventures. Joining forces opens the way to higher numbers of potential customers adopting the Mobile Wallet technology to pay.
2. The successful issuance and operation of a Mobile Wallet requires hardware and software computing components, governance rules, a sustainable business model, a payment infrastructure with big databases, and a security certification program. The diversity of complex skills required to run a wallet represents a significant investment – and the need to share costs is a therefore a major incentive to cooperate.
3. Governance rules backing the business model must clearly set out the rights and responsibilities of different members of the wallet program. An important issue to resolve is whether the Mobile Wallet issuer is given some access to data stored in the wallet by a financial service provider, or whether it reserves the right to keep track of the customer behaviors.
4. A diversity of alliances between stakeholders has been observed when it comes to creating a wallet offer that's populated with cards. Banks appear slow to promote wallet partnerships, perhaps fearing the loss of customer ownership, competition with merchants and other non-banking institutions – or it may simply be the lack of a clear business case.

5. Mobile Wallet: the case for Secure Element implementation

The recent announcement of software-only Mobile Wallet implementations by major IT players like Google has led to debate on the role of the Secure Element in the protection of mobile financial services.

When issuing a secure Mobile Wallet, a decision needs to be made in relation to its location; if the wallet is resident in the cloud then a safe way to protect data is required to ensure this cannot be accessed by a third party.

Data must be encrypted using keys stored in the wallet, but this is hard to manage and raises a number of issues:

- Which entity stores the decryption key?
- How does the user ensure the key is available - and that he has sole control when it comes to using the decryption key?

Ideally, Mobile Wallet access should be protected by an authentication hardware device under the direct control of the customer; in essence the Secure Element is able to store the key locally and use it to perform complex crypto-calculations.

The SPA has always advocated extending the card security model to other acceptance contexts, contending that a Mobile Wallet is best protected if stored in a Secure Element which emulates the card in the mobile device; in the case of a Wallet it will emulate multi-application contactless cards executing NFC transactions.

As the Mobile Wallet is designed to be populated with payment applications, possibly from different brands, it would therefore benefit from the interoperable infrastructure for the remote management of the Secure Element content, using TSM.

Furthermore, the combination of the Secure Element with a TEE provides a secure user interface - another desirable security property for wallet management.

In summary, utilizing a Secure Element implementation ensures that the Mobile Wallet will benefit from (1) the security and management capabilities of the Secure Element, and (2) of the user interface and wireless multi-channel connectivity of the mobile device.

6. Is a standard necessary to boost mobile wallet adoption?

New mobile financial services require infrastructure, products, an aggressive marketing and communication campaign, as well as incentive programs for adoption. That's because customers tend to adopt a new payment instrument and drop former ones, only when it offers significant advantages in terms of convenience, perceived security and other advantages – such as a greater level of acceptance by retailers or an associated reward program.

It follows that some level of standardization should be beneficial: if there are too many different wallets, all using different non-interoperable standards, adoption by the consumer will be hampered.
Creating viable business models for mobile financial services is challenging for everybody and minimizing the investment required for a new wallet solution is a key business requirement. Mobile Wallets should accommodate existing payment infrastructures or be designed to comply with a standard which does not exist at present (ISO 12812 simply describes Mobile Wallets as a technology for mobile financial services; see R7 in bibliography).

The SPA believes that priority should be given to the development of this standard which should cover both the interoperable access and the life cycle management of Mobile Wallets - a point that has already been suggested in the SEPA for cards program.

The standard should establish a minimum set of additional functionalities; propose security and data protection requirements; elaborate on already existing specifications; and support competition by not necessarily addressing implementation details. This should lead to a downward trend in costs and prices for wallet users (both customers and merchants) and more choice and transparency for mobile financial services.

For a comprehensive list of potential items for wallet standardization the SPA suggests consulting the EPC White Paper on Mobile Wallet Payments (R1), referring to documents R3 and R4 for the core GSMA interoperability requirements for NFC-enabled mobile wallets issued by mobile network operators.

7. Conclusions

So far, no wallet issuer seems to have found the right combination of appealing features that enables the mass adoption of Mobile Wallets by customers – which in turn should fuel NFC payments.

However, the business goal remains: one mobile device, one wallet. The Mobile Wallet represents a major challenge for mobile financial service providers, which has led to fierce competition for offering the best product that has resulted in a highly fragmented market.

Thus, in the short term a diverse set of mobile wallet technology offerings will continue to co-exist until customers and retailers decide which business model will dominate the market. Regardless of the specific model, wallets should be interoperable (open and ubiquitous), work on most mobile devices, payment networks, and be accepted by most merchants.

Learning from past unsuccessful initiatives, the SPA has identified some of the key requirements that are needed to enable a successful Mobile Wallet experience. A Mobile Wallet system should (1) provide a friendly customer enrollment process, (2) provide clear calls for the provisioning of applications to boost the number of transactions, (3) guide the user in how to act before and after transactions for key features (payment, money transfers, loyalty programs), (4) ensure fast processing of mobile financial transactions as well as other commerce non-payment applications, (5) be stored in a secure environment accessed through a trusted user interface, and (6) operate in an interoperability context that at the present time is insufficient due to the lack of a global standardization framework.

8. Bibliography

R1: European Payments Council: White Paper: Mobile Wallet Payments, EPC 163-13 (Version 2.0) - January 2014
R2: Mobey Forum: Mobile Wallet: The Hidden Controls, July 2012
R3: GSMA: NFC Mobile Wallet-POS Proposal, Version 1.0, April 2013
R4: GSMA: Official Document NFC 1.0 - NFC Core Wallet Requirements, August 2013
R5: Federal Reserve Bank of Boston: U.S. Mobile Payments Landscape – Two Years Later, May 2013
R6: European Central Bank: Fraud, Investments and liability regimes in payment platforms, October 2011
R7: ISO 12812 Core Banking- Mobile Financial Services – Parts 1 to 5, Currently in draft
R8: Federal Reserve Bank of Boston: The 2011 and 2012 Surveys of Consumer Payment Choice: Technical Approaches, Upgraded version October 2014
R9: European Banking Authority: Final Guidelines on the Security of Internet Payments, December2014