Innovations in retail: Mobile payments

Alexandre Stervinou
Banque de France
Deputy Head
Non-cash Means of Payment Oversight Division
alexandre.stervinou@banque-france.fr

Regional Payment Systems Workshop - LAC
Port of Spain, Trinidad & Tobago
08 February 2011

Outline

1. What are exactly mobile payments?

2. A promising new payment service

3. What chances of success?

4. Challenges for regulators/overseers
1. What are exactly mobile payments?

Various definitions, evolving over time as mobile services evolve:

- **ECB (2004):** sub-group of e-payments, where mobile phones or other wireless devices are used to access accounts and to use payment services.  
  *Focus on user interface.*
- **Dewan & Chen (2005):** payments made by using mobile devices, including wireless handsets, PDA, RF devices or NFC-based devices. Too large.  
  *N/a for analysis of payment markets.*
- **Mallat (2006):** use of mobile device, commonly a mobile phone, to make a payment transaction, where funds are transferred from payer to payee, either via a bank or directly, without an intermediary. *Functional definition.*
- **Heikkinen (2009):** use of payment services, other than Internet banking, by using a mobile handset, its keyboard and display. *Large definition acknowledging that many mobile payment applications are a variation of existing payment types, but however excludes mobile banking.*
- **EPC (2010):** main focus on mobile contactless card payments, but also considers credit transfers and direct debits. *A technical & functional definition, centred on the underlying instruments, but limited to EPC ones.*

Need to consider both the financial services & technologies involved

<table>
<thead>
<tr>
<th>Mobile payment services</th>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile money transfers P2P</td>
<td>Message mode (SMS order or notification)</td>
</tr>
<tr>
<td>Mobile payments P2B</td>
<td>Emulation of a payment card (contactless payment, NFC)</td>
</tr>
<tr>
<td>· Prepaid (e-wallet)</td>
<td>· SIM centric</td>
</tr>
<tr>
<td>· Postpaid (e-billing)</td>
<td>· secure element</td>
</tr>
<tr>
<td>Mobile banking</td>
<td>Web access protocols (WiFi, 3G…)</td>
</tr>
<tr>
<td>· Different from technical services (e.g. emulation of an EFTPOS)</td>
<td></td>
</tr>
</tbody>
</table>
2. A promising new payment service

- Various experiments in different countries
- Taking advantage of the mobile phone massive distribution all over the world
  - Almost 4 billion mobile phones end 2008 according to UN's agency for information and communication technologies = almost 60% of the planet's 6.7 billion inhabitants
  - Smartphones (iPhone, Google Android) on a growth trend worldwide
- Adequate response to some payment situations:
  - peer to peer
  - prepayment
  - unbanked population
  - migrant financial flows

3. What chances of success?

- Business model still not certain
  - SMS order
  - Prepaid units
  - Emulation of a payment card (contactless payment): requires a delivery process of the payment application in the payer’s handset
  - Still an evolving ground: concepts on e-banking based payments on mobile phone start to appear (also called remote payments, e.g. on the EPC agenda)

- Ecosystem still not certain
  - Repartition of roles between actors: telcos, banks, money remitters, vendors, transporters
  - Chicken & egg dilemma: who is the best in place for ensuring a successful launch of the product?
4. Challenges for regulators/overseers

- Financial stability of the payment institution
  - Protection of funds received against the risk of default vs. need for some light regime
  - The EU Payment Services Directive (2007/64/EC) of 13 Nov. 2007 states that mobile payments are limited to banks OR newly created Payment institutions
  - Waiver for the cases where the Telco is not a financial intermediary, even if the goods or services to purchase can only be used through the Mobile/IT device and the Telco is the seller.

<table>
<thead>
<tr>
<th>Services permitted</th>
<th>Banks (PSP)</th>
<th>ELMIs (PSP)</th>
<th>PIs (PSP)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Taking deposits &amp; granting credits + Providing payment services</td>
<td>Issuing &amp; managing EM + Providing payment services</td>
<td>Providing payment services</td>
</tr>
<tr>
<td>Information to be provided to users of payment services</td>
<td>PSD + Other texts</td>
<td>PSD + Other texts (incl. EMD)</td>
<td>PSD + Other texts</td>
</tr>
<tr>
<td>Rights and obligations of users and service providers</td>
<td>PSD</td>
<td>PSD</td>
<td>PSD</td>
</tr>
</tbody>
</table>

AML/CFT Standards for M-payments

- Cross-border transfers: pay attention to AML-CFT standards.
  - World Bank 2008: « FATF recommendations seem to constitute an adequate preventive framework for cross-border mobile phone financial services and associated risks. For example, special recommendation VII on wire transfers specifies the information that should accompany domestic and cross-border wire transfers. »
  - FATF revised whitepaper issued in 2010 to take into account latest payment innovations

<table>
<thead>
<tr>
<th>Categories of PSPs in PSD</th>
<th>Banks</th>
<th>E-money licenced institutions</th>
<th>Payment institutions</th>
</tr>
</thead>
</table>
Security weaknesses in M-payments

- **Common security features:**
  - Mobile platforms become more evolved with advanced features (e.g. multimedia capabilities) and connectivity (Bluetooth, WiFi, 3G, Wimax, etc.)
    - Security vulnerabilities seen in PC world spread to mobile devices (viruses, trojan, backdoors, keyloggers): enable MITM attacks and identity theft
  - Authentication, confidentiality and integrity not often built in by design in standards

- **SMS channel**
  - Insecurity of the GSM protocol
    - Legacy encryption & authentication algorithms in use have been cracked
    - Ability to forge & intercept SMS messages
  - Rogue base stations enabling MITM attacks

- **Contactless M-payments (and cards)**
  - No mutual authentication in the RF transport layer used (electronic pickpocketing, relay attacks)
  - Countermeasures exist, with some limitations
    - Device or card activation mechanism (user experience, smoothness of the process)
    - Roundtrip monitoring at the terminal level (still under design)

Main issues for the Central bank oversight of mobile payments

- Internet channel on mobile devices: risk of
  - Fraudulent access
  - Phishing attempts

- Message mode (SMS, exchange of prepaid units): risk of
  - Injection (forged SMS)
  - Takeover
  - Theft

- Emulation of cards (contactless NFC):
  - Protection of the payment application (need to isolate applications, risks of capture of secrets stored)
  - Risk of capture of data: eavesdropping
  - Risk of electronic pickpocketing: fraudulent capture of information or initiation of a payment without the user’s consent
An example: Eurosystem oversight frameworks (I)
Approach and methodology

- Risk analysis and modelling
  - Identification of all functions
  - Identification of assets and threats

- Establishment of security objectives / standards
  - Classification (cf. CPSS Core Principles)
  - Oversight framework

- Oversight tools
  - Assessment criteria (questionnaire)
  - Assessment guide for overseers
  - Scoring methodology

An example: Eurosystem oversight frameworks (II)
Common oversight standards

- The 5 standards retained are common ground for all payment instruments. The specifics of each instrument are then taken into account in « key issues » defined per standard.
  - **Standard 1**: The scheme should have a sound legal basis under all relevant jurisdictions
  - **Standard 2**: The scheme should ensure that comprehensive information, including appropriate information on financial risks, is available for all actors
  - **Standard 3**: The scheme should ensure an adequate degree of security, operational reliability and business continuity
  - **Standard 4**: The scheme should implement effective, accountable and transparent governance arrangements
  - **Standard 5**: The scheme should manage and contain financial risks in relation to the clearing and settlement process
An example: Eurosystem oversight frameworks (III)
Overview of the main oversight tools

<table>
<thead>
<tr>
<th>Oversight Framework (public – overseen entity)</th>
<th>Assessment Questionnaire (overseen entity)</th>
<th>Assessment Guide with CheckPoints (Overseer**)</th>
<th>Eval. (Overseer)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards (5)</td>
<td>Assessment Question (1)</td>
<td>CK (1)</td>
<td>OK/NOK (1)*</td>
</tr>
<tr>
<td>Key Issue [1..n]</td>
<td>AQ (2)</td>
<td>CK (p)</td>
<td>OK/NOK (p)*</td>
</tr>
<tr>
<td>Explanatory Memorandum [1]</td>
<td>AQ (3)</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>STD9: Sub-domain [1..6]</td>
<td>AQ (m)</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Key Issue [1..n]</td>
<td></td>
<td>Eval.</td>
<td></td>
</tr>
</tbody>
</table>

** + overseen entity: currently debated  
* + justifying documentation

Conclusion: what stance for Central banks?

- Not hamper innovation: mobile payment services useful for unbanked people, migrants, as well as for peer-to-peer payments

- Pay attention to regulatory frameworks, possibly in cooperation with banking supervisors
  - In EU, creation of the European security forum on retail payments

- As overseers, pay attention to technical security: need for technological watch and for expertise (internal or external)
  - Ability to have approaches which encompass most recent innovations
Research papers and studies

- ECB, The Eurosystem card payment scheme oversight framework, 2008 (credit transfer & direct debit, 2010)
- Heikkinen P., A framework for evaluating mobile payments, Bank of Finland, 2 March 2009
- Chatain P-L et allii, Integrity in mobile phone financial services, World Bank working paper 146, 2008
- Karnouskos S, Mobile payment: a journey through existing procedures and standardization initiatives. IEEE Communications Surveys, Fourth quarter 2004, Volume 6, No.4
- Mallat N., Consumer and merchant adoption of mobile payments, Helsinki School of Economics A-285, HSE 2006

Thank you for you attention

Questions?

alexandre.stervinou@banque-france.fr

www.banque-france.fr