Abstract

Regulatory Authorities in Albania need to start paying more attention to consumer-related issues and define some standards to which partners (Banks, MNOs/Mobile Network Operators, etc) need to adhere so as to ensure higher consumer satisfaction and protect financial stability. Consumers are not sure who to approach if and when they have complaints related to mobile money, especially when they involve in an issue. This happened to countries focusing on attracting investment and providing an open ground for innovation without thinking allover. Potential areas of action include: partners (Banks, MNOs, etc) providing mobile money services should define some quality metrics that can be tracked over time to ensure improvements. Performance across these metrics should be periodically disseminated to the public for reasons of transparency and accountability. Use of mobile money creates lots of data and a trail that can be followed. This can be used for both good and bad objectives. It is therefore important to specify who can have access to this information.

Keywords: Banks, Customers, Mobile Money, Regulatory Authorities

JEL classification: G21; G28; E4; O3

1 Introduction

“Mobile Money” is electronic money that can be accessed and used for “Mobile Payments” which are payments via mobile phone. Today, mobile subscribers in markets are beginning to use mobile money for transactions and services, including domestic and international remittances, bill payment, payroll deposit, loan
receipt and repayment, and purchases of goods and services ranging from prepaid airtime to groceries to bus tickets to micro insurance. There is no limit to the range of transactions and services for which mobile money could eventually be used. As a result, mobile money has significant implications for economic activity across the board.

Mobile money, facilitates the flow of money from one party to another using a communications infrastructure that already connects billions of customers around the world – far more customers than currently have bank accounts. In an increasing number of developing countries, millions of poor people are using basic mobile phones to transfer money; pay for goods; and access sophisticated financial services, such as credit, insurance, and savings accounts\(^4\). As “mobile money” becomes commonplace, research is shifting from studying design and adoption to assessing impact\(^5\). Although impact assessment remains nascent, that which does exist has been criticized for lacking rigorous conceptual or theoretical approaches, and instead, relying heavily on practitioner surveys, rather than academic research\(^6\).

---

\(^4\) Donovan, 2012  
\(^5\) Donner & Tellez, 2008  
\(^6\) Duncombe & Boateng, 2009
2 Some definitions of “Mobile Money”

Falls within definition of electronic banking; …includes provision of retail and small value banking products and services through electronic banking channels as well as large value electronic payments and other wholesale banking services”\(^{47}\); “Mobile money” consists of financial transactions that are conducted using a mobile phone, where value is stored virtually (e-money) in an account associated with a SIM card. Individuals can deposit cash onto a mobile account, make transactions between accounts, and withdraw funds as cash; “Mobile payments” provision of payment services through the use of mobile phones…

As the cost of mobile phone technology have fallen, and as the technology has been adapted to support financial services, mobile banking innovations have begun to spread across and within poor countries. The low cost, and the unmet demand for financial services, as captured by low rates of bank physical access, means that mobile banking has the potential to reach geographic, spectrum. These advantages are particularly pronounced in developing countries.

Types of Mobile payments recently introduced are still at an early stage of development and deployment, the use of mobile technology for payments may result in additional security exposures attributable to:

1. The fact that the current generation of mobile devices and their operating systems were generally not designed with the security of payments in mind;
2. The reliance on radio technology (i.e. wireless small range technologies such as Bluetooth and Near Field Communication (NFC) or the over-the-air (OTA) data channels provided by the mobile network operator) for transmission of sensitive payment data and personal data;
3. The involvement of additional actors, such as mobile network operators (MNOs) and trusted service managers (TSMs), compared with traditional payments; and
4. The general reduced security awareness of mobile device users or unsafe customer behaviour.

Indeed, the network power of mobile money as a whole—interoperable between many providers—would actually increase, potentially challenging cash’s dominance. Already, some are advocating an “anti-cash movement”\(^{48}\), and major development organizations and private sector entities have formed the Better than Cash Alliance to support electronic payments, presenting cash as an anachronism: expensive to manage, easy to lose, and prone to illicit usages. Although

\(^{47}\) BIS Risk Management

\(^{48}\) Sridharan, 2012
it is generally unwise to take a teleological approach to technology\textsuperscript{49}, and it is unlikely that mobile money will wholly displace cash any time soon\textsuperscript{50}.

As a new technology for payments, face the particular challenges that customers’ perception of security is a basic condition for the use of mobile payment services, and that security incidents could (temporarily) damage the image of mobile payment services. A number of regulatory issues and potential policy actions should be discussed. The issues relate to consumer protection, registration and transaction limits, agent networks, interoperability, taxation as well as collaboration between regulators both within and across

3 The Challenges and conclusions that we can meet

Some traditional risks modified; Risks (operational, legal, reputational risk); Structure and function of financial institutions; Privacy concerns Information security concerns; For supervisors: operational risk and reputational risk. (Security, outsourcing and vendor management); Law inevitably lags behind technology and Implications for regulators; Reliance on third party service providers; Balancing act: access v over-regulation; Cross-border (mobile money transfer) less developed; Various trade-offs: in payment system, trade-off between regulating the institution v product, inclusion v integrity.

4 Mobile banking and mobile payments in Albania

Referring to the available data, home banking\textsuperscript{51} is increasingly expanding in the Albanian banking market. Since the introduction of this product in 2005 till in December 2013 the result is that 11 banks provide e-banking. The growing number of these accounts is followed by growing e-banking transactions in terms and value, but recent trends on electronic payments show a positive slow step and paper based (SWIFT) money transfers yet is dominating. The above-mentioned development may factorise an extension of the use of this instrument to a wider range of users. More specifically, while this instrument was initially provided only by one bank and was meant for large companies. Meanwhile, boosted competition in this segment of the market and the subsequent decrease of costs, as well as familiarisation of the public with this alternative payment instrument, led to

\textsuperscript{49} Edgerton, 2007
\textsuperscript{50} Maurer, 2011
\textsuperscript{51} Meaning internet banking, phone banking, mobile banking, etc
its use by other user categories. During recent years is noticed an increase: In the number and the value of transactions made through home banking in Albania and in the number of accounts accessed through internet. However, the utilization of the instrument has shown a negative trend, firstly introduced in Albanian market as product targeting only for private companies.

We must specify that internet banking is the leading service among the home-banking services in the Albanian banking market. But seeing it in a regional perspective, Albania appears to have the lower level in the region in terms of home banking use (Graph 1.). While, the Albanian market has shown increase in the electronic banking channels as ATMs and POSs and in terms of payment cards has shown increase in the number of debit and credit cards.

Graph 1 Home banking transaction per 1 million inhabitants (Authors)

According to Bank of Albania report, the number of credit and debit cards issued by private banks increased by 54% and, the total number of cards in use is estimated to be 870 thousand, one in three Albanian citizens owns a debit or/and credit card (Albania has a population of 2.9 million). But, debit cards which are linked to current accounts are frequently used by Albanians compared to credit cards estimated to be only 78 thousand credit card holders. However, card transactions in Albania are dominated by cash withdrawals (ALL 109 billion of card transactions, where 92% of them were cash withdrawals).

Following the above, we will present some quantitative information, specifically for the mobile payments service generated by analysing the data of 6 banks which actively offer these services in Albania.
Below you will find a list of the most typical transactions performed through the mobile banking service done through authorisations\textsuperscript{52} and check over credentials\textsuperscript{53} in Albania: transfers of funds between the accounts of the same client within the same bank; transfers of funds between different clients within the same bank; transfer of funds in another bank in Albania; payment of bills (utilities; credit cards etc.); etc

Mobile banking activity in Albania is offered only by banks because our Banking Law did not permit non-banking financial institutions to have deposits or repayable funds from the public which would make possible the transfer of funds or other transactions from the client’s account. In such circumstances, even the nonbanking financial institutions which aim to offer this activity, or already can, have to perform monetary transactions only through bank accounts (client’s bank account and nonbanking institution bank account).

The new changes in the Banking Law, made possible the introduction of a new kind of financial activity in Albania, the e-money issuance as well as the establishment of the E-money institutions. The Supervisory Council of Bank of Albania approved on January 17th, 2013 the regulatory framework amendments related to the e-money institutions licensing and supervisory procedures. Such e-money institutions, in difference from the other non-banking financial institutions (NBFI), can collect “deposits” from the public, even though the name “deposit” in this case, does not have the same meaning with that of a bank deposit. The

\textsuperscript{52} A procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data.

\textsuperscript{53} The personal and confidential information provided for the purposes of authentication. Credentials can also refer to the physical tool used for obtaining the information (e.g. one-time-password generator, smart card), or to something the user memorises or represents (such as biometric characteristics
Banking law states clearly such difference. That is the new facility BoA offered to the market, in compliance with the EU Directive on E-money institutions. BoA open the possibilities for NBFI (Non-Bank Financial Institutions) to enter in this activity offering to customers the service of making transactions by using cards, mobile phones or internet, to perform low value transactions through e-money institutions.

5 Mobile payments, a new technology for payments

Mobile payments can take several forms, but a generic definition, as defined in the 7th SEPA Progress Report (2010), is “payments for which the payments data and the payment instruction are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device\textsuperscript{54} between the customer and his/her payment service provider in the course of an online communication.

In one typical use case of mobile payments, the initiation of the payment takes place through a wireless communication between the customer’s mobile device and the merchant’s payment terminal (e.g. using NFC capability pre-installed on the mobile device or delivered separately on a SIM or SD card). In another use case, the initiation of the payment may take place through the scanning of a QR (Quick Response) code provided by the merchant (e.g. on display at the cash register, generated by its payment terminal, in a printed publication, or on the e-commerce website) followed by a wireless or over-the-air communication between the customer’s mobile device and the mobile payment solution provider using an MNO’s network or a Wi-Fi connection and the internet. In yet another use case, mobile payments are used for person-to-person (P2P) payments. Further use cases exist and are still being developed. These payments are internet payments.

- Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:

\textsuperscript{54} For the purpose of this document, a mobile device is a handheld machine: (i) connected to other devices or systems via radio technologies or via telecommunication networks based on wireless (“over-the-air”) technology (e.g. GSM/GPRS/UMTS, Wi-Fi, NFC, RFID, Bluetooth); (ii) designed with a multimedia interface for user interaction (e.g. display, keyboard, sound-speaker); (iii) equipped with a storage facility for “user identification data” (for instance a SIM card, other UICC, or a micro-SD card); and (iv) equipped with a mobile operating system.
something only the user knows (e.g. a static password, code or personal identification number);

something only the user possesses (e.g. a token, smart card or mobile device); and

something the user is (e.g. a biometric characteristic, such as a fingerprint). In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s).

At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen. The strong customer\textsuperscript{55} authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data. As an example, where a static password or PIN is used as an element to perform strong customer authentication, as referred to in the Payment Services Directive\textsuperscript{56}.

Types of mobile payments are still at an early stage of development and deployment, the use of mobile technology for payments may result in additional security exposures attributable to:

- the fact that the current generation of mobile devices and their operating systems were generally not designed with the security of payments in mind;
- the reliance on radio technology (i.e. wireless small range technologies such as Bluetooth and Near Field Communication (NFC) or the over-the-air (OTA) data channels provided by the mobile network operator) for transmission of sensitive payment data and personal data;
- the involvement of additional actors, such as mobile network operators (MNOs) and trusted service managers (TSMs), compared with traditional payments; and
- the general reduced security awareness of mobile device users or unsafe customer behaviour.

Mobile payments, as a new technology for payments, face the particular challenges that customers’ perception of security is a basic condition for the use of mobile payment services, and that security incidents could (temporarily) damage the image of mobile payment services.

Customer trust in mobile payments is all the more important, given that the mobile technology can introduce previously “remote” payment instruments and solutions into the “bricks-and-mortar” environment; mobile payments are therefore an alternative for cash, cheques and “card-present” payments. For

\textsuperscript{55} Customers include both consumers and corporate entities to which a payment service is provided

\textsuperscript{56} e the definition of low-value payment instruments in Articles 34(1) and 53(1) of the Payment Services Directive
card-present payments, a high level of security has been reached throughout Europe thanks to the efforts made over recent years migrating cards and payment terminals to the EMV specifications, which allow for robust card authentication (e.g. by using dynamic or combined data authentication) and cardholder verification (PIN), together forming strong customer authentication. For mobile payments at the point of sale, an equivalent level of security should be aimed for. Similarly, for those mobile payments that compete with internet payments, an equivalent level of security should be aimed for as in the Recommendations for the security of internet payments. For both use cases, the specific vulnerabilities and threats, as well as the opportunities, related to the use of mobile technology for payments should be taken into account.

6 Recommendations

Consumers are not sure who to approach if and when they have complaints related to mobile money, especially when they involve in an issue. This happened to countries focusing on attracting investment and providing an open ground for innovation without thinking allover. Regulators need to start paying more attention to consumer-related issues and define some standards to which partners (Banks, MNOs, etc) need to adhere so as to ensure higher consumer satisfaction and protect financial stability. Potential areas of action include: partners (Banks, MNOs, etc) providing mobile money services should define some quality metrics that can be tracked over time to ensure improvements. Performance across these metrics should be periodically disseminated to the public for reasons of transparency and accountability. Use of mobile money creates lots of data and a trail that can be followed. This can be used for both good and bad objectives. It is therefore important to specify who can have access to this information.

1. Governance

Mobile Payment Solution Providers (MPSPs) should implement a formal security policy for mobile payment services which is subject to periodic review, monitoring and challenge being compliant with regulatory framework of Governance authorities (of a payment instrument scheme).

57 Mobile network operator

58 The entity accountable for the overall functioning of the scheme that promotes the payment instrument in question and for ensuring that all the actors involved comply with the scheme's rules. It is responsible for ensuring the scheme's compliance with oversight standards. European Central Bank (2009), Harmonised oversight approach and oversight standards for payment instruments.
2. Risk assessment

MPSPs should identify and assess risks on an ongoing basis (supported by a formal policy and strategy) in order to ensure the security of mobile payments and ancillary services, but also prior to establishing the service(s).

3. Security incident monitoring and reporting

MPSPs should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. MPSPs should establish a procedure for reporting such incidents to management and, in the event of major payment security incidents, to competent authorities.

4. Risk control and mitigation

MPSPs should implement proportionate security measures aligned with the risks in order to mitigate identified risks. These measures should incorporate multiple layers of security, whereby the failure of one line of defence is mitigated by the next line of defence (“defence in depth”).

5. Traceability

MPSPs should have processes in place ensuring that all transactions are logged with an appropriate audit trail.

6. Initial customer identification and provision of information

MPSPs should properly identify customers (payers and payees) in line with the European anti-money laundering legislation and should obtain the confirmation of their willingness to make and/or to accept mobile payments using

---

59 The customer identification process is without prejudice to any exemptions provided for in existing anti-money laundering legislation. PSPs (Payment Service Provider, as defined in the Payment Services Directive) do not need to conduct a separate customer identification process for the mobile payment services, provided that such customer identification has already been carried out by them, e.g. for other existing payment-related services or for the opening of an account. For example, a passport, a national identity card or an electronic identification with an adequate electronic signature and certificate.

60 This information complements Article 42 of the Payment Services Directive which specifies the information that the PSP must provide to the payment service user before entering into a contract for the provision of payment services.

the services before being granted access to such services. MPSPs should provide adequate “prior”, “regular” or, where applicable, “ad hoc” information to the customer about the necessary requirements (e.g. equipment features, procedures) for performing and/or accepting secure mobile payment transactions including the inherent risks.

7. Strong customer authentication

MPSPs should ensure that the initiation of mobile payments, as well as access to sensitive payment and personal data, is protected by strong customer authentication. MPSPs should ensure that customer enrolment for and the initial provision of the customer’s authentication tools and/or the delivery of software required to use the mobile payment service is carried out in a secure manner. MPSPs should limit the number of log-in or authentication attempts (e.g. wrong PIN entries), implement time-out controls and set time limits for the validity of authentication.

8. Transaction monitoring

MPSPs should operate transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions; suspicious or high-risk transactions should be subject to a specific screening, filtration and evaluation procedure.

9. Protection of sensitive payment data and personal data

Sensitive payment data and personal data should be protected when stored, processed or transmitted.

10. Customer education and communication

MPSPs should provide assistance and guidance to customers, where needed, with regard to the secure use of mobile payment services. MPSPs should communicate with their customers in a manner that reassures them of the authenticity of the messages received.

a) Through the secure channel, MPSPs should keep customers informed about updates to security procedures regarding mobile payment services.

b) MPSPs should initiate customer education and awareness programmes designed to ensure that customers understand, at a minimum, the need: to protect their passwords, PIN codes, personal details and other confidential data; to manage properly the security of the personal device (e.g. mobile handset), through installing and updating security components (antivirus, security patches);
c) It is desirable that MPSPs offering acquiring services arrange educational programmes for their merchants on fraud prevention.

d) It is desirable that MPSPs and third parties such as the MNOs draft appropriate customer education and communication policies based on a common understanding of risks.

References

2. Data on websites of ABA, BoA and CBA