Payment Systems Review

1st Qtr. (July — Sept.) FY13 **Date: 01 January 2013**

Points of Interest:

PCI DSS Security Standards—A brief introduction

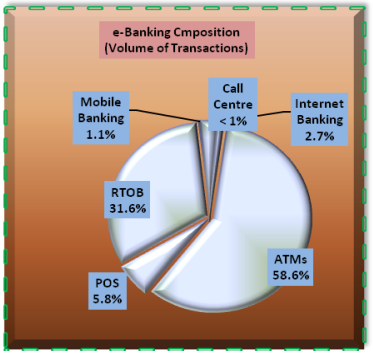
Auto Deposit ATMs-Kiosk Machine—Introduction and development

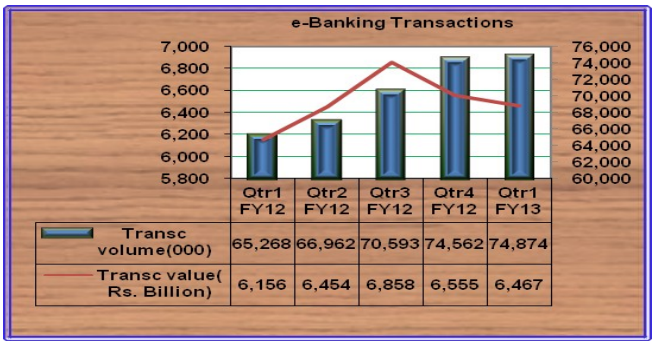
Inside this issue:

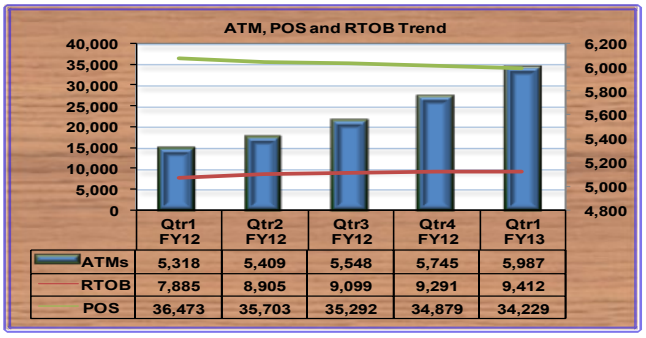
During the first quarter of FY13, the infrastructure of Payment Systems in the country maintained an increasing growth trend. A total of 242 more ATMs were installed by various banks bringing the total number of ATMs to 5,987 in the country. Altogether, 121 more bank branches were added to the network of Real-Time Online Branches (RTOB) which makes a total of 9,412 branches who can now offers RTOB services out of 10,111 bank branches across country.

The number of plastic cards in the country also increased by 9.55 percent compared to the numbers recorded in the preceding quarter. By the end of quarter under review, there were 19.67 million plastic cards issued in the country.

The volume of overall e-banking transactions during this quarter depicted a growth of 15 percent to 74.87 million and the value of transactions increased by 5 percent to Rs. 6.5 trillion as compared to the figures reported in the same quarter of previous fiscal year. The volume and value of RTOB transactions also increased by 21 percent and 4 percent respectively as compared to transactions reported in the first quarter of previous fiscal year.







In terms of volume of overall e-banking transactions Automated Teller Machine (ATM) has a major share of 58.6 percent and an average value per transaction stands at Rs. 9,810. In comparison with transactions reported in the first quarter of previous fiscal year, the overall volume of ATM transactions increased by 13 percent and the value increased by 22 percent. The share of ATMs in the total e-banking transactions' in terms of value is 6.7 percent.

The volume and value of transactions through POS terminals stood at 4.3 million and Rs. 20.8 billion showed a growth of 5 and 15 percent respectively as compared to the figures reported in the first quarter of previous fiscal year.

The recorded volume of large-value payments through RTGS in this quarter was 110,255 and the value was Rs.38.49 trillion. This showed 27 percent increase in the volume and 53.3 percent in value as compared to the figures reported in the first quarter of previous fiscal year. The significant increase in value of RTGS transactions is due to settlement against securities transactions which increased by 73.4 percent in the current quarter that has a major portion in RTGS transactions followed by Interbank Funds Transfers and settlement of retail cheques through multilateral clearing; contributing 63.8, 28.4 and 7.8 percent respectively.

E-Banking Growth Trend— *Yearly Comparison*

Yearly E-Banking Trend						
E-Banking Transactions						
	Qtr1 FY12		Qtr1 FY13		Yearly Growth	
	Volume (000)	Value (Rs. Billion)	Volume (000)	Value (Rs. Billion)	Volume	Value
RTOB	19,598.66	5,694.49	23,679.53	5,899.75	21%	4%
ATM	38,805.23	353.51	43,876.79	430.42	13%	22%
POS	4,137.25	18.01	4,328.83	20.77	5%	15%
Call Center	169.82	1.79	166.06	2.09	-2%	17%
Internet Banking	1,646.70	84.85	2,018.78	109.95	23%	30%
Mobile Banking through internet*	909.96	2.94	804.17	4.18	-12%	42%
E-Banking	65,267.63	6,155.57	74,874.16	6,467.16	15%	5%

E-Banking Infrastructure			
	As of September 30,2011	As of September 30,2012	Yearly Growth
ATMs	5,318	5,987	13%
RTOB	7,885	9,412	19%
POS	36,473	34,229	-6%
Credit Cards(000)	1,363	1,274	-7%
Debit Cards(000)	12,553	17,588	40%
ATM Only Cards(000)	613	806	32%

**Branchless Banking data is not included*
In the retail payment systems, Microfinance Banks data are not included.
Discrepancy may occur due to rounding of data.

Auto Deposit ATMs—Kiosk Machine

The Auto Deposit ATMs has the ability for customers to perform transactions that may normally require a bank teller and may be more complex and longer to perform than desired at an ATM.

At the end of 2001, there were 670,000 automated deposit terminals installed around the world. This represents an increase of 45 percent compared with two years earlier showing impressive growth especially when that non-deposit ATMs grew by just 14 percent over the same period.

RBR found that ADTs are becoming a standard feature in many markets, and that despite economic pressures, financial institutions are continuing to invest in the technology. In fact, ADTs now outnumber envelop-deposit ATMs two to one. China, and a little surprisingly, Russia, accounted for more than half of the new ADT installations between 2009 and 2011. However, China is the major growth market for retail banking and ATMs.

In their study, banks cited various reasons for wishing to divert routine transactions away from the teller; not just to reduce queues, but also to facilitate staff redeployment and cost cutting. In some cases ADTs enable banks to implement a cashless or tellerless branch format. RBR forecasts that the number of ADTs worldwide will double by 2017, to about 1.3 million. This represents an annual growth rate of 12 percent, triple that of non-deposit ATMs.

A study conducted by: Retail Banking Research (RRB) Ltd. Wincor Nixdorf International—A London based strategic research and consulting firm.

Payment Systems Developments at SBP

During the period under review:
Circular Letter No. 02 dated July 18, 2012 on "**Settlement Timings During Ramazan-ul-Mubarak**" - Cut-off timings for settlement & transaction charges of Interbank Funds Transfers and Customer Transfers for different time windows in PRISM System during Ramazan-ul-Mubarack. All RTGS participants are advised to ensure the execution of their transactions in PRISM System within the above mentioned time limits. Further, after the holy month of Ramazan-ul-Mubarak, the above timings will automatically be reverted to pre Ramazan-ul-Mubarach timings (http://www.sbp.org.pk/psd/2012/CL1.htm)

News & Updates...

Vodafone, ICICI Bank to launch M-Pesa Mobile service in India—They have entered in an agreement to launch the mobile money transfer and payment service dubbed M-Pesa in India by the end of 2012.
The service is to be launched through Mobile Commerce Solutions, a Vodafone India subsidiary, and ICICI Bank. It would comprise a mobile money account with ICICI Bank and a Mobile Wallet issued by MCSL.
M-Pesa is set to enable customers to make cash deposits or withdrawals from designated outlets, transfer money to mobile phones or bank accounts in India, make payments at selected shops and have access to mobile payment services including mobile or DTH recharge and utility bills.

Bahrain introduces e-security system—to enable citizens to access electronic services in the public and private sectors.
The newly launched system is part of Bahrain's new vision to prepare the country for the digital future. The e-key system is the first in the region, provides three layers of security, including passcode, smart card and fingerprint for identity verification. Additionally, it allows users to access government services offered via all available channels. In order to activate the service, users will have to create a personal account on the e-government portal.
A national e-government strategy, which will be implemented by 2016, to upgrade Bahrain's position in e-government service internationally, was also rolled out. The initiatives also include service procedures through one-stop shops, the use of social media network to communicate with citizens, creating open data platform to develop new applications and service.

MasterCard, Standard Chartered Bank (Singapore) release security token card—using MasterCard's Display Card technology.
From January 2013, all Standard Chartered online banking or breeze mobile banking users will use the Standard Chartered security token card as a new personal security device for higher-risk transactions such payments or transfers above a certain amount, adding third party payees, or changing personal details.
The MasterCard Display Card includes a built-in display allowing cardholders to generate one-time passwords. Card issuers are able to activate the one time password as a dynamic card verification code (CVC2) or as an on-card activation of MasterCard SecureCode which offers online security service against the unauthorized use of a customer's MasterCard card while shopping online.

ROAM Data launches mobile Point of Sale (POS) card reader—US mobile commerce platform provider ROAM Data, a subsidiary of French-based provider of payment services Ingenico, has launched a mobile POS card reader dubbed G4X.
The G4X mobile reader provides enhanced features including auto device detection enabling plug and play pairing with a handsets and tablets, along with auto power management. The G4X supports both Android and iOS-based smartphones and tablets and is integrated with the ROAMpay product suite providing a mobile POS service or it can be integrated with thirst party mobile POS application using the ROAMpay SDK.

VISA has contradictory position regarding the law on functioning of payment systems—The VISA international payment system's criticism of the law on the functioning of payment systems in Ukraine passed by the Ukrainian parliament is not in line with the behavior of the company on the U.S. market where they observe the tougher and all-embracing requirements of the FRS which were passed in a law on financial stability in 2010. The law on the functioning of payment systems passed on September 18, 2012 by Ukrainian parliament gives the right to the National Bank of Ukraine (NBU) to define the procedure for clearing and making cross payments between payment systems participating in transactions in Ukraine using payment cards issued by Ukraine banks. The director of the Ukrainian Interbank Association of members of payment systems said that there was fierce competition on the global market among payment systems. He said that the position of visa was not in line with the facts stipulated in annual reports of the company to the U.S. Securities and exchange commission; Visa does not participate in routing transactions on the territory of over 50% of countries where the system operates – special purpose companies do this including those belonging to local banks and governments.
Visa has expressed deep disappointment at the adoption of a law on the functioning of payment systems and has asked Ukrainian President Viktor Yanukovych to veto the law. Visa said the adoption of the law would hinder the development of electronic payment industry in Ukraine due to the establishment of monopoly on the Ukrainian payment market. Visa also said that Ukrainian consumers would not be able to use their payment cards in stores and restaurants or get cash from ATMs inside the country. However NBU would continue its dialogue with Visa and MasterCard international payment systems on the prospects for Ukrainian national payment card transactions routing and clearing system.

The advancement in information technology over the years has enabled electronic payment systems to replace traditional modes thus reducing costs and simultaneously improving reliability, security and convenience. However, with these associated benefits the electronic payment systems also pose threats and security concerns for cardholders. The cardholder's data has become vulnerable to variety of threats by hackers, phishers and fraudsters. Five well known electronic payment companies namely American Express, Discover Financial Services, JCB International, Master Card and Visa Inc launched different programs in order to counter the emerging threats being faced by electronic payment methods. The primary goal of each of these programs was to ensure safety and security to the electronic payments methods such as debit, credit, prepaid, e-purse, ATM and POS cards and cardholder information is handled safely from hackers and data hijackers.

In 2004, these electronic payment companies aligned their individual policies on payment card industry and collectively launched Payment Card Industry Data Security Standard (PCI DSS). In 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard these five electronic payment companies established Payment Card Industry Security Standards Council (PCI SSC). This council is responsible for the development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Council later on formally established a body of security standards known as the PCI Data Security Standards. These standards consist of twelve significant requirements including multiple sub-requirements which contain numerous directives against which organizations may measure their own payment card security policies, procedures and guidelines.

A brief description of these 12 PCI DSS requirements are as follows:

Requirement-01: Install and maintain a firewall configuration to protect cardholder's data.
Requirement-02: Do not use vendor-supplied defaults for system passwords and other security parameters.
Requirement-03: Protect stored cardholder data.
Requirement-04: Encrypt transmission of cardholder data access open, public networks.
Requirement-05: Use and regularly update anti-virus software.
Requirement-06: Develop and maintain secure systems and applications.
Requirement-07: Restrict access to cardholder data by business need-to-know.
Requirement-08: Assign a unique ID to each person with computer access.
Requirement-09: Restrict physical access to cardholder data.
Requirement-10: Track and monitor all access to network resources and cardholder data.
Requirement-11: Regularly test security systems and processes.
Requirement-12: Maintain a policy that addresses information security.

By complying with qualified assessments of these standards, organizations can become accepted by the PCI Standards Council as compliant with the twelve requirements and thus receive a compliance certification from PCI Security Standard Council. Validation of compliance is done annually by an external Qualified Security Assessor (QSA) for organizations handling large volumes of transactions or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

Following sources of ADCs where transactions done through cards are found risky and weak security areas for PCI DSS:

On ATMs including vulnerable payment applications; inadequate perimeter security of firewall; out of date system security patches; vendor default setting and passwords and poorly coded web-facing applications etc.
On CDMs including unreliable network links; remote access to other system; vulnerable payment applications; inadequate premier security; vendor default setting and passwords; poor cryptographic key management use for PIN encryption etc.
On POS, for example, during a card swipe POS collect enough information and, if get hold of hackers, enough to create a replica card. The blame not only goes to the POS acquirer but partly goes to the merchant and the way they configure networks. Some of the merchants are using internet to transmit data instead of dial-up network and some have incorporated wireless access points into their network using WEP (Wired Equivalent Privacy), which is not considered a strong form of encryption.

Although the PCI DSS must be implemented by all organizations that process, store and transmit cardholder data. However, formal validation of PCI DSS compliance is not mandatory. Merchants and service providers need to be more vigilant ensuring PCI DSS for enhanced security, while smaller merchants and service providers are not required to explicitly validate compliance with each of the controls prescribed by the PCI DSS. Nevertheless, these organizations must still implement all controls in order to maintain safe harbor and avoid potential liability in the event of fraud associated with theft of cardholder's data. Issuing banks are not required to go through PCI DSS validation although they should try to secure the sensitive data in a PCI DSS compliant manner. However, acquiring banks should always comply with PCI DSS validated by means of an audit.

Contact:
Payment Systems Department
State Bank of Pakistan
I. I. Chundrigar Road
Karachi

Phone: 021 3245 3448
021 3245 3413

Email:
arshad.khan2@sbp.org.pk
nadeem1@sbp.org.pk

Disclaimer
The information provided articles, submissions and spotlights are those of the contributors and do not necessarily represent the views of State Bank of Pakistan or any other authority. It is the purpose of this piece to share a variety of information on the subject. Although, great care has been taken in ensuring the correctness of the facts/ figures we, however, accept no responsibility whatsoever for the accuracy of the contents reproduced