

# Auto Teller Machine (ATM) Fraud – Case Study of a Commercial Bank in Pakistan

Aijaz Ahmed Shaikh<sup>1</sup> & Syed Mir Muhammad Shah<sup>1</sup>

<sup>1</sup> Department of Business Administration, Sukkur Institute of Business Administration, Sukkur, Pakistan

Correspondence: Aijaz Ahmed Shaikh, Department of Business Administration, Sukkur Institute of Business Administration, Airport Road, Sukkur, Pakistan. Tel: 92-333-385-9864. E-mail: aijaz.shaikh@iba-suk.edu.pk

Received: August 5, 2012 Accepted: September 19, 2012 Online Published: October 24, 2012

doi:10.5539/ijbm.v7n22p100

URL: <http://dx.doi.org/10.5539/ijbm.v7n22p100>

## Abstract

ATM occupies an important position in the e-Banking portfolio. It has given the consumers a quality of life allowing them to access cash and other financial information. Its role in promoting, developing and expanding the concept of ‘Anytime Anywhere Anyplace’ banking is undeniable. It offers a real convenience to those who are on the run in their everyday life, but at the same time, it also carries a big element of risk.

In this paper we have investigated and demonstrated a mapping flaw (bug) in the ATM Controller (commonly known as financial middleware), which allows the ATM card holders of various banks to fraudulently withdraw cash from the ATMs of ACB Bank Limited. The flaw remained undetected for nearly 3 months.

Since the breach has been thoroughly investigated, we, therefore, concluded that the banks’ internal control system had failed to detect the implantation of mapping bug which deprived the bank of more than 21 million Pakistani Rupees. In addition, lack of understanding of higher management on the systems & procedures supporting ATM Infrastructure played a significant role in developing the bug.

Considering the nature of the fraud and the degree of losses incurred, this paper has recommended strong internal controls implementation over the payment system applications. A detailed review of fraud screening strategy is also recommended to ensure that the security tools are optimized for their particular product or service. Turnkey ATM solution has also been recommended for the ACB Bank Limited.

**Keywords:** electronic banking, ATM fraud, mapping bug, ATM controller, internal controls, Pakistan

## 1. Introduction

Among the prominent financial touch-points, Automated Teller Machine (ATM) has been considered as one of the important components of electronic banking infrastructure.

ATM is a terminal deployed by bank or other financial institutions, which enables the customers to withdraw cash, to make a balance enquiry, to order a bank statement, to make a money transfer and/or to deposit cash. The ATMs are basically self service banking terminals and are aimed at providing fast and convenient services to customers (Rasiah, 2010).

ATMs provide different services to cardholders without the help of any bank employee or teller. All these services have been segregated as financial and non-financial. A variety of payment cards such as Debit (Expense) Cards, Credit Cards, Prepaid Debit Cards and recently introduced Remittance Cards can be used in Pakistan on ATMs. Prominent services offered through ATMs are listed below in Table-1:

Table 1. Financial and non-financial services usually offered through ATMs

Financial Services	Non-Financial Services
Cash Withdrawal	Balance Enquiry
Utility Bills Payment	Mini Bank Statement
Inter (and Intra)-bank Fund Transfer	PIN Change
Mobile Balance Pop-up	Cheque Book Request

Considering their nature, the frauds perpetuated on ATMs and other E-Banking Channels have been divided among different categories as mentioned in Table 2.

Table 2. Nature and the types of ATM frauds

Cash / Card Frauds	Card Skimming Card/Cash Trapping Transaction Reversal Fraud (TRF)
Operational Fraud	One of the examples of operational fraud is when the ATM cassettes holding cash in various denominations are purposefully filled with currency in the wrong denomination, therefore, giving customers or criminals more money than should be dispensed.
Equipment Fraud	Installing a fake ATM machine in a shopping centre or a fake card reader or skimming devices.
Digital Fraud	Hackers who author viruses or worms intended to exploit ATM operating systems and/or Controllers.

This paper discusses the ATM fraud which was perpetuated on one of the important components of ATM IT Infrastructure i.e. ATM Controller of ACB Bank Limited.

1.1 ATM Controller

The ATM Controller famously known as Transaction Processing Switching or Financial Middleware is one of the most important components in conducting electronic transactions. The first ATM Controller was introduced in Pakistan by TPS Pvt. Limited in 1996.

The importance of the ATM Controller can be gauged from the fact that in 1990s and most part of 2000, almost all the banks in Pakistan had distributed core banking systems and some banks still continue to operate in the same fashion. These distributed core banking system applications were usually housed in bank branches and once the branches are closed in the evening, the customer data in core banking is not available for any real-time transaction. To overcome this challenge and to provide anytime, anywhere, anyplace banking facilities to consumers, the ATM Controller was introduced.

In the banking environment, the controller sits between the Bank’s Core Banking Application, Bank’s delivery channels i.e. Mobile Banking, Internet Banking, External networks/3<sup>rd</sup> Party Service Providers i.e. 1-Link, VISA, MasterCard, Bill Payment Services, and Financial Touch Points i.e. ATMs, Kiosks, POS as depicted below.

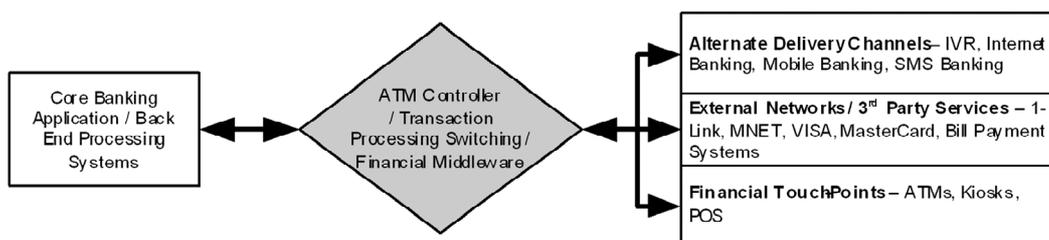


Figure 1. Role of ATM controller as financial middleware

As a middleware, the ATM Controller acquires electronic transactions from the Bank’s ATM and POS network, process these transactions and then forward them to the host or issuer bank for authorization. After receiving authorization, the acquirer bank ATM disburses the cash.

The next section discusses the Statement of Problem (Section-2), Research Methodology (Section-3), Literature Review (Section-4), ATM Infrastructure in Pakistan (Section-5). Findings and Observations have been discussed in Section-6 followed by the Conclusion and Recommendations, which have been discussed under Section-7. Acknowledgement and References have been provided in Section-8 and 9 respectively.

## 2. Statement of Problem

In Pakistan, the ATM transactions are based on predefined and pre-allocated mapping codes ranging from 00 to 99 wherein '00' code has been reserved for 'cash withdrawal' by all the banks. Accordingly, the ATMs and the associated ATM Controllers have been configured on the parameters that does not allow 'cash withdrawal' from ATM if any other code except for the '00' is received from the issuer bank's core banking application.

ATMs are always attached with ATM Controller when conducting inter-bank transactions involving two different banks. Once the card holder of Bank-A (issuer bank) access the ATM of Bank-B (acquirer bank), the ATM of Bank-B sends the card holder credentials to Bank-A for verification and authorization. This communication is conducted through the ATM controller deployed at both Bank-A and Bank-B. After receiving the authorization from issuer bank i.e. Bank-A, the ATM of acquirer bank i.e. Bank-B disburses the cash to cardholder of Bank-A.

In this case study, we have investigated the presence of a mapping bug when the ATMs of ACB Bank Limited started disbursing cash to the card holders of Bank-A having 'zero' or 'insufficient' balance in their bank account. Despite of the fact that the Bank-A sent a rejection "06" code from its ATM controller to ACB Bank ATM Controller, but due to the presence of a mapping bug, the ATM Controller of ACB Bank started reading every code as "00" and disbursed the cash as depicted in the following diagram:

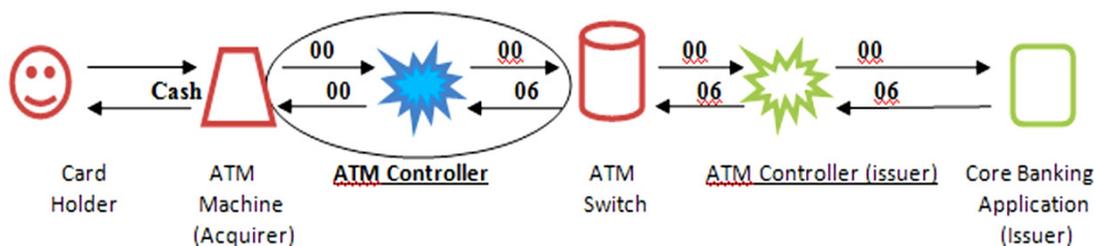


Figure 2. Flow of ATM transactions showing how the "06" was converted into "00" code by the ATM controller of ACB bank limited

## 3. Research Methodology

The data for this paper was collected from different organizations including the ACB Bank Limited, the State Bank of Pakistan (the central bank), technology partners and the ATM Switch operator. Internal bank reports, documents and policy papers, the investigation reports prepared by the State Bank of Pakistan were thoroughly checked and analyzed. The ACB bank premises were visited for conducting few interviews with the staff working in its Information Technology Group.

The Central Bank guidelines, instructions and by-laws on ATMs along with the Payment Systems & Electronic Funds Transfer Act 2007 were also collected and reviewed. The 'Payment Systems Quarterly Review' reports published by the State Bank of Pakistan since Financial Year 2006 were collected, consolidated and analyzed.

In addition, exploratory research based on secondary data obtained through journals and Net was also included in this case study.

## 4. Literature Review

Commercial banking is undergoing rapid change, as the international economy expands and advances towards institutional and market completeness. A major force behind these developments is technology (Liano & Cheung, 2001). As further investigated by Ogbuji, Onuoha & Izego (2012), the converging forces of technology have tremendously altered manual systems of delivering banking services and have subsequently paved way for electronic delivery platforms in recent time. The ATMs is one of existing replacements of the cascading labor-intensive transaction system affected through what is popularly referred to as paper-based payment instruments.

E-Banking in general and ATMs in particular have given the consumers a quality of life allowing them to access cash and other financial information. It offers a real convenience to those who are on the run in their everyday life, but at the same time, it causes a big element of risk. The traditional banking risk, in some instances, are

magnified when banks offer 24/7 transactional websites. As banks move into this new territory, several challenges arise in the context of banking risks (Pennathur, 2001).

Adepoju & Alhassan (2010) while analyzing the cases of ATM usage and fraud occurrences with some banks in Nigeria discussed that consumers have come to depend on and trust the Automatic Teller Machine (ATM) to conveniently meet their banking needs. In recent time there has been a proliferation of ATM frauds in the country even and across the globe. Managing the risk associated with ATM fraud as well as diminishing its impact are important issues that face financial institutions as fraud techniques have become more advanced with increased occurrences. On the other hand, Agoyi and Seral (2010) have shared their concern on the growing number of ATM frauds and have suggested using the SMS encrypted messages to authenticate the users to improve ATM security against frauds and crimes.

ATM hacking is now on the rise with some organized and highly sophisticated attacks. This has now become a real headache because both banks and customers are prone to heavy losses. Criminals are taking the battle a stage further, by directly manipulating the software inside the ATMs to give them money (Bradbury, 2010).

Report on Global ATM Fraud (2007) published by ICMR has reported that the ATM frauds have evolved from the conventional 'trick of shoulder surfing' to steal the PIN of customers at the ATM to more sophisticated methods such as the Lebanese loops, use of electronic gadgets, card jamming, card swapping, diversions, website spoofing, or phishing, ATM Burglary etc.

The first massive and seemingly coordinated fraudulent attack on ATM users was that may best be described as the great phishing scam on 2007, in which fraudsters cloned the inter-switch website and sent wide reaching notices to ATM cardholders to log on to the cloned website and re-register their payment cards by changing their PIN. So daring was this attempt that notices were even pasted on the walls of bank premises. The fraudsters succeeded in accessing the accounts of many cardholders and withdrew their money. This act of fraud was chiefly successful because the magnetic stripe ATM card in use within the country in comparison to the Chip (smart) cards (Chinedu, 2010).

Chip cards based on EMV technology has been considered as one of the most effective solutions to card Skimming fraud until the same was successfully broken by a team of University of Cambridge students. Murdoch, Drimer, Anderson & Bond (2010), in their paper has demonstrated a protocol flaw in Europay, MasterCard and VISA (EMV) protocol. Because the authors have found and validated a practical attack against the core functionality of EMV, they concluded that the protocol is broken.

Realizing the severity and the frequency of the ATM frauds, Diebold in their one of the white papers titled 'ATM Fraud and Security-2012' has reported that the ATM fraud is not confined to a particular region of the world. As further reported, the card skimming was the most prevalent crime affecting ATMs in Europe. Card skimming at ATMs resulted in losses of nearly 111 million Euros across Europe during the first half of 2011. Card Skimmers are devices used by perpetrators to capture cardholder data from the magnetic stripe on the back of an ATM card.

The commercial banks therefore need to deploy sufficient preventive controls to minimize the chances of frauds and maintain the consumer trust on e-banking products and services.

Greene (2009) has defined the key areas of payment fraud. He segregated the fraud into two categories. There is first-party fraud, which is the abuse of the account privileges by the account holders themselves, or the acquisition or expansion of those privileges by deceitful means. There is also third-party fraud, which is often identity fraud, or the abuse of one person's account by another. Third-party fraud is what we usually think when we consider fraud.

While investigating the risk management, security and controls in the context of ATMs, Rasiyah (2010) has described that the crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount important when considering vulnerabilities and causation in civil litigation and banks must meet certain standards in order to ensure a safe and secure banking environment for their customers.

Based on a survey of bank corporate clients in Singapore, Rexha, Kingshott & Aw (2003) concluded that trust was the key factor influencing the adoption of electronic banking. The trust, therefore, remained to the key factor influencing the adoption of various e-banking channels and products offered by the banking industry. In addition, ATM Security has been considered as one of the major concerns for regulators, financial institutions and service providers.

## 5. ATM Infrastructure in Pakistan

The ATM service was first introduced in Pakistan by Habib Bank Limited in 1987. The ATM infrastructure in Pakistan is developed, managed and supported by Commercial Banks, Microfinance Institutions, and by 3<sup>rd</sup> party commonly known as Services Providers. ATMs are owned, operated, deployed and managed by Commercial Banks established under the Banking Companies Ordinance 1962 and licensed by the State Bank of Pakistan (the Central Bank).

In order to provide an easy and quick access to card holders, ATMs have been placed at convenient locations called on-site locations (near or inside the bank branch premises) and off-site locations (shopping malls, universities, colleges, gas stations etc).

In ATM transactions, the role of Issuer and Acquirer bank occupies an important position. For example a banking company in Pakistan can become an acquirer or issuer or both for offering e-banking products and services to consumers. Banks issuing payment card such as Debit, Credit, Prepaid Debit or Remittance Cards are called issuing banks and they are not required to deploy ATMs or POS terminals. Payment cards issued by issuer bank can easily be used on any ATM or POS terminals owned and managed by another bank in Pakistan called acquirer bank. Most of the banks in Pakistan are both issuer as well as acquirer as the case with ACB Bank Limited.

Commercial Banks in Pakistan have deployed different e-banking applications and financial transaction processing middleware from different vendors or non-financial institutions. The prominent vendors include TPS Pakistan (Pvt.) Limited and Avanza Solutions.

Two ATM Switches namely 1-Link (Guarantee) Limited and MNET Services Pvt. Limited are providing real-time inter-bank ATM connectivity platform to their respective member banks in Pakistan. In order to facilitate the inter-bank fund transfer and other e-transactions, in 2002, the Central Bank mandated commercial banks to join any of the ATM switch in Pakistan. Again in 2004, the two ATM switches were interconnected with each other thereby enabling the card holders of any bank to use ATM of another bank anywhere anytime in the country. The interconnectivity of the ATM Switches played a key role for the phenomenal growth of e-banking in Pakistan.

In 2006, Inter-Bank Fund Transfer (IBFT) was introduced. IBFT allows the consumers to electronically transfer funds via ATM, Internet, Mobile, Call Centre and IVR between participating banks without the hassle of writing any paper instrument such as Cheque and making Demand Draft and Pay Order etc.

Considering the severity of electronic frauds in respect of damaging the bank's reputation and consumer interest, in 2008, the **Central Bank** mandated SMS alert facility. Consequently, the commercial banks in Pakistan started offering SMS alerts on all the electronic transactions conducted on POS terminals and ATMs. In addition, the project of Primary Account Number (PAN) masking on transaction slips generated on POS terminals was also initiated and completed in 2008. Few banks have also activated the PAN masking on ATMs transactions in Pakistan. PAN masking helps in minimizing the e-commerce/internet frauds.

According to Payment Systems Quarterly Review published by the State Bank of Pakistan (the Central Bank), as of June 30, 2011, thirty banks are providing ATM related e-banking services to consumers in Pakistan. The volume of ATM transactions during Financial Year 2010-11 was 137,659 thousand valuing 1,204,465 million Pakistan rupees; recording a hefty growth of 19 percentage in terms of number and 33 percentage in value over the Financial Year 2009-10. Similarly, the quantity of ATM has also been showing a continuous growth and reached 5,200 machines during Financial Year 2010-11 (Table-3).

Table 3. Volume and value of ATM transactions in Pakistan

Transactions	FY 2008	FY 2009	FY 2010	FY 2011
Vol. (000)	67,912	91,126	115,677	137,659
Ant (Rs. Mil)	452,972	668,531	905,306	1,196,000
ATM Qty	3,121	3,999	4,465	5,200

Similarly, the total volume of ATM transactions in the e-banking infrastructure occupies a significant position. Among the prominent e-banking channels, the total volume of ATM transactions stood at 86% percentage of the total e-banking transactions in the country during financial year 2011 (Table-4).

Table 4. E-banking trends (financial year 2009-2011)

Transactions (000)	FY 2009	%age	FY 2010	%age	FY 2011	%age
ATM	91,126.00	81%	115,677.00	85.11%	137,659.00	85.76%
POS	18,280.00	16%	15,673.00	11.53%	14,287.00	8.90%
Internet Banking	2,095.00	2%	2,962.00	2.18%	4,436.00	2.76%
Mobile Banking	71.00	-	600.00	.44%	3,363.00	2%
Call Centre	932.00	1%	1,003.00	.74%	778.00	.49%
Total	112,504.00	100%	135,915.00	100%	160,523.00	100%

## 6. Findings and Observations

- A fraudulent activity was took place in December 2007 on the ATM network of ACB Bank Limited. About 21 million Pakistan rupees were fraudulently withdrawn from ACB Bank's ATM Network by conducting 2,430 fraudulent transactions using 228 ATM/Debit cards.
- ACB Bank has been using *Beeta* ATM Controller for its ATM transactions since the start of its ATM Operations in 2003. The Software was managed, updated and upgraded by Omega Pakistan Limited (OPL). ACB Bank is one of the member banks of Alpha ATM Switch.
- The presence of a *mapping bug* in the Beeta and lousy internal controls over payment applications at ACB Bank were observed to be the main reasons which allowed unauthorized and fraudulent withdrawal from the Bank's ATMs for consecutive 89 days until when a criminal was caught by the Bank's staff posted at one of their branches located in a small town near Multan City while withdrawn a huge quantity of cash from their ATM.
- The problem started when OPL upgraded ACB Bank's ATM Controller in December 2007. Soon after the up-gradation, Beeta started malfunctioning in certain error conditions in which the cash was not suppose to be disbursed
- Beeta started interpreting all those transactions in which Alpha ATM Switch was giving message '*BAD TRANS CODE (RC-11)*' as 'OK' transaction with message '*Transaction Approved*'. Hence all ATMs owned and managed by ACB Bank started disbursing the cash based on the false advices received from Beeta. It was, however, noted that prior to the up-gradation of Beeta, all similar transactions were correctly interpreting the message as '*INVALID CARD DATA (RC-07)*' by Beeta and rejected.
- Mentioned below are the two scenarios based on true transactions and showing a complete path of transactions. Scenario # 1 is trail of an "OK" transaction (pre-upgrade period) whereas scenario # 2 is showing a fraudulent transaction (post-upgrade period). For the clarity of the transactions, extra columns found present in the response reports extracted from the system logs of ACB Bank were deleted.

### Scenario-1: Transaction flow of an 'OK' transaction during pre-upgrade period

Step-1: Response generated by Bank-A ATM Controller

DATE	TC	ST	PAN	RQ AMT	DSP AMT	RC	NC	AC
071115	CASH	CMPLT	421**	2000.00	2000.00	00	00	00

Response Code (RC- 00) i.e. 'Authorized' used for internal messaging has been mapped to Bank-A ATM Controller code list.

Step-2: ATM Switch Log provided to ACB Bank.

TYPE	TRAN	CARD NO.	AMNT	TR DT	TR TME	STATUS
020	WITH D	421**	2000	11/15	18:47:07	Ok

Step-3: ACB-Beeta transaction Log

HS TRTY	HS ACTN	HS RSPC	HSN TID	HS CRD	HS TDAT
04	A	00	187	421**	071115

**Scenario-2: Transaction flow of an 'OK' transaction during post-upgrade period**

*Step-1:* Response generated by Bank-A ATM Controller

DATE	TC	ST	PAN	RQ AMT	DSP AMT	RC	NC	AC
080307	CASH	CMPLT	421**	1000.00	0.00	06	57	00

Response Code (RC- 06) i.e. 'not allowed' used for internal messaging has been mapped to Bank-A ATM Controller code list.

*Step-2:* ATM Switch Log provided to ACB Bank

TYPE	TRAN	CARD NO.	AMNT	TR DT	TR TME	STATUS
020	WITHD	421**	2000	11/15	18:47:07	BAD TRAN CODE

The message 'BAD TRAN CODE' refers to RC-11 in Alpha ATM Switch code table.

*Step-3:* ACB-Beeta transaction Log

HS	HS	HS	HS	HS	HS	HS	HS
TRTY	ACTN	RSPC	NTID	CRD	TDAT	TTIM	DBCR
04	A	00	187	421**	1,071,115	183,307	D

RC-06 was converted into '00' at Beeta and transaction became 'OK' because of mapping bug developed after its up-gradation.

- Furthermore, the daily cash withdraw limit of Pakistan Rupees 25,000 was also not invoked due to an 'input error' and the fraudsters were able to conduct a number of transactions and withdrew unlimited amount till the machines went 'out of cash'.
- It may also be noted that aforementioned 'mapping bug' had no effect for its own customers using ACB Bank's ATMs because internally no mapping was needed in such case.
- Printer Journal Log of any ATM is considered as single most authentic record of ATM. More precisely it is called the 'Black Box' of ATMs. The printer journal usually uses thermal jet printer over glossy paper roll. As with the nature of the glossary paper, the print on it usually vanishes within 2 months. It is, therefore, imperative for banks to hold printer journal record in the form of electronic achieves.

As observed, the ACB Bank's ATM Controllers did not have e-journaling to record ATM wise events including transactions. Most of the paper record of fraudulent transactions was not legible due to above limitations of thermal jet printing.

- According to the State Bank of Pakistan Guidelines for Standardization of ATM Operations issued in 2006, all the branches of commercial banks having ATM network in Pakistan were required to carry out ATM cash balancing and reconciliation every working day at a time fixed by their head offices. This time, however, should not be during peak hours and should not cause disruption of ATM services for extended hours.

As observed, the interbank ATM reconciliation mechanism, though existed in the Main Branch of ACB Bank, was inadequate in terms of efficiency and effectiveness. Only few employees were posted in ATM reconciliation unit without any automated reconciliation system. The manual reconciliation of approximately 5000 transactions every day was practically impossible, which in fact resulted into the non-identification of fraud at its earlier stage. The fraudulent transactions continued for 89 consecutive days.

- As explained by Shaikh (2011), the significance of evidences collected and processed during post-fraud scenario occupies a very importance position. In e-banking environment, the evidences have been categorized as Primary and Secondary. In Primary evidence, the ATM or system-based reports are generated and checked for verification, authenticity and for the satisfaction of the complainant. Most of the complaints are resolved based on the information collected and analyzed from primary evidences. Secondary evidences such as collected through built-in event-snap cameras and CCTV footage are used in most sophisticated crimes perpetuated on ATMs such as Skimming, Card/Cash trapping and Transaction Reversal Frauds (TRFs) to name a few.

In view of the importance and necessity of primary and secondary evidences, the State Bank of Pakistan in its Operational Guidelines on ATMS issued in 2007 had mandated all the commercial banks in Pakistan to install CCTV Surveillance cameras to monitor and record all the activity in the ATM vicinity. As investigated, ACB Bank's ATMs were not fitted with CCTV cameras. Few of its ATMs were also not fitted with built-in event capture cameras, which resulted into the non-availability of secondary evidence which can otherwise help ACB

Bank in identifying the fraudsters. Based on the evidences provided by the systems generated reports, the card users were, however, identified and the respective issuing banks were contacted for the recovery of the stolen money.

- Job logs, which serves as an effective internal control, logs every event, changes in any system object and sign-in / sign-off of every user along with date and time so that any unauthorized changes, if made, could easily and timely be identified. By loosing job logs, evidence of changes in the system by authorized users would also be lost.
- Higher management at ACB bank seemed less concerned about the overall security and safety of e-banking channels especially the ATMs, which otherwise would have avoided this fraud.
- Few weeks after the incident, instructions on the 'internal controls over ATM Support' were issued by the senior management to at ACB Bank, which implies that the internal control system was ineffective at ACB Bank.

## 7. Conclusion and Recommendations

The ATM transactions in Pakistan have recorded a continuous growth over the period of time, which shows the customer preferences in selecting and using this E-Banking Channels for conducting both financial and non-financial transactions. The ATM Fraud at the same time has opened up new chapters in the IT security portfolio demanding a reasonable attention from the higher management in thwarting ATM fraud at its early stages. In addition, to better detect and prevent e-frauds, multiple tools may be used with proper fraud management practices and systems in place.

Effective internal controls provide a reasonable assurance to the management on fraud prevention and timely detection. The guidelines and the instructions issued by the central bank need proper attention. Their compliance will help the banks in minimizing e-banking risks, detecting e-frauds, prevention and safeguarding the e-Banking assets including ATMs.

Considering the nature of the fraud and after thoroughly investigating the ACB Bank's internal control mechanisms and lack of higher management involvement and understands of ATM operations, a turnkey ATM solution has been recommended for ACB Bank. Under this solution, a 3<sup>rd</sup> party or an Independent Selling Organization (ISO) may be contacted to deploy and look after the ATMs, provide monitoring and diagnostic services and also ensure the safety and security of the ATMs. The cash replenishment shall rests with the ACB Bank Limited.

In order to keep the identity of the respondent, software developer and ATM Switch Operator anonymous, imaginary names were used in this case study i.e. ACB Bank Limited, Beeta ATM Controller, Omega Pakistan Limited and Alpha ATM Switch respectively.

## Acknowledgement

Staff members working in the Information technology of ACB Bank Limited and Beeta ATM Switch. I also acknowledge the support and access to documents provided by the staff members working at the State Bank of Pakistan.

## References

- Adelowo Solomon A., & Mohammed Enagi A. (2010). Challenges of ATM usage and Fraud Occurrences in Nigeria-A Case Study of Selected Banks in Minna Metropolis. *Journal of Internet Banking and Commerce*, 15(2). Retrieved from [www.arraydev.com/commerce/jibc/2010-08/Solomon.pdf](http://www.arraydev.com/commerce/jibc/2010-08/Solomon.pdf)
- Aijaz Ahmed Shaikh. (2011). Reducing Fraud Risks in E-Banking. *Pakistan and Gulf Economist*, 30, 19.
- Anita K. Pennathur. (2001). Clicks and Bricks: E-Risk Management for Banks in the age of the Internet. *Journal of Banking and Finance*, 2103-2123. [http://dx.doi.org/10.1016/S0378-4266\(01\)00197-2](http://dx.doi.org/10.1016/S0378-4266(01)00197-2)
- Chinedu N. Ogbuji., Chima B. Onuoha., & Emeka E. I. (2012). Analysis of the Negative Effects of the Automated Teller Machine (ATM) as a Channel for Delivering Banking Services in Nigeria. *International Journal of Business and Management*, 7(7), 180-190. Retrieved from <http://ccsenet.org/journal/index.php/ijbm/article/view/16034>
- Danny Bradbury. (2010). A Hole in the Security Wall: ATM Hacking. *Network Security*, 2010(6), 12-15. [http://dx.doi.org/10.1016/S1353-4858\(10\)70082-9](http://dx.doi.org/10.1016/S1353-4858(10)70082-9)

- Devinaga Rasiah. (2010). ATM Risk Management and Controls. *European Journal of Economics, Finance and Administrative Sciences*, 21, 161-171. Retrieved from [www.eurojournals.com/ejefas\\_21\\_13.pdf](http://www.eurojournals.com/ejefas_21_13.pdf)
- Diebold Corporation. (2012). *ATM Fraud and Security (2012)*. Retrieved from [www.diebold.com](http://www.diebold.com)
- ICMR. (2007). *Report on Global ATM Fraud-2007*. Retrieved from [www.icmrindia.org/casestudies/catalogue/Business%20Reports/BREP041.htm](http://www.icmrindia.org/casestudies/catalogue/Business%20Reports/BREP041.htm), July 2007
- Igwe Stanley Chinedu. (2010). Technology Innovations and in the Banking Sector – An Evaluation of the Rate of Diffusion of the Automated Teller Machine. *Academic Leadership, the Online Journal*, 8(4).
- M. Agoyi., & D. Seral. (2010). The use of SMS encrypted message to secure automatic teller machine. *Procedia Computer Science*, 1310-1314.
- Mark N. Greene. (2009). Divided we fall: Fighting payments fraud together. *Federal Reserve Bank of Chicago*, 37-42. Retrieved from [www.chicagofed.org/digital\\_assets/publications/economic\\_perspectives/2009/ep\\_1qtr2009\\_part6\\_greene.pdf](http://www.chicagofed.org/digital_assets/publications/economic_perspectives/2009/ep_1qtr2009_part6_greene.pdf)
- Nexhmi R., Russel Philip John K., & Audrey Shang Shang A. (2003). The Impact of the Relational Plan on Adoption of Electronic banking. *Journal of Services Marketing*, 17(1), 53-67. <http://dx.doi.org/10.1108/08876040310461273>
- SBP. (2002). *Mandatory Connectivity of Two ATM Switches By all Banks*. Retrieved from [www.sbp.org.pk/bpd/2002/c20.htm](http://www.sbp.org.pk/bpd/2002/c20.htm)
- SBP. (2006). *Guidelines for Standardization of ATM Operations*. Retrieved from [www.sbp.org.pk/psd/2010/CL2.htm](http://www.sbp.org.pk/psd/2010/CL2.htm)
- SBP. (2007). *Operational Guidelines on ATMs*. Retrieved from [www.sbp.org.pk/psd/2007/c2-07.htm](http://www.sbp.org.pk/psd/2007/c2-07.htm)
- State Bank of Pakistan-SBP. (2010). *Payment Systems Quarterly Review*. Retrieved from [www.sbp.org.pk/psd/reports/index.htm](http://www.sbp.org.pk/psd/reports/index.htm), July 2012
- Steven J. M., Saar D., Ross A., & Mike B. (2010). Chip and PIN is Broken. *IEEE Computer Society*, 433-445.
- Ziqi L., & Michael Tow C. (2001). Internet-based e-banking and consumer attitudes: An empirical study. *Information & Management*, 39, 283-295.