Recent ATM Scams in Bangladesh

By Adib Sarwar
Research Associate, Center for Enterprise and Society, ULAB

August 2016 | Current Event Analysis Series

Introduction

With Bangladesh's economic emergence, various business and financial sectors are enjoying steady growth and implementing novel technologies to their business and operational processes. The adoption of new technologies paves the way for opportunity for new businesses. However, with new business have come new opportunities for malpractice. The financial sector of Bangladesh, and the banking sector in particular, is one such segment where corruption has followed closely on the heels of recent innovations. With the advent of Automated Teller Machines (ATMs) in Bangladesh in 2003, most of the fifty-plus banks in the country have already implemented this service, in order to facilitate cash withdrawal, balance enquiry, balance transfer, and other services. Where there are electronic systems however, there are bound to be malfunctions; and when these systems are dealing with money, there usually are malpractices. A global network, ATM Security Association, estimated annual global skimming losses of USD 2 billion as of February 2016; 98% of losses occurred through ATMs.[1] Moreover, now that Europe is EMV-card compliant (Europay, MasterCard and Visa), 87% of frauds have crossed borders.[2]

In Bangladesh, scamming incidents have been increasing since 2012. In 2012, there was a credit-card scam valued at BDT 100 million, involving local bank officials of United Commercial Bank Limited (UCBL). In 2013, another high-profile ATM forgery committed by IT officials and their associates at Mutual Trust Bank (MTB), was valued at BDT 20 million. Both incidents involved locals and were discovered two years later.[3]

From February 2016 onwards, a few significant ATM forgeries have made the headlines. This Current Event Analysis (CEA) piece aggregates a list of recent forgeries, delves into the domestic and foreign involvement in those incidents, provides an overview of "how it occurs", and reviews measures in place and potential ones, with the view towards encouraging more stringent financial stewardship in the banking sector.

ATM Forgery Incidents across the Country

Table 1 summarizes all the incidents of ATM and other transactional device forgeries in 2016. Here, ATMs scams, Point-Of-Sale (POS) terminal frauds and ATM hijackings are also listed. The first 3 rows represent a carefully coordinated attempt by an international gang of flagged fraudsters.[4] The amount stolen by them was only unearthed later on, after investigations were conducted by the Detective Branch (DB) Police and was well beyond originally estimated. Item 4 reflects a scam representing the first time international cards were used to commit electronic theft.[5] All these occurrences happened in a space of few consecutive months and were not observed in this frequency before.

Table 1: Recent ATM Forgeries and Related Incidents

ATM forgeries

S.L.	Cloning of ATM Cards	ATM booth targeted		Date (2016)	Amounts targeted	Other Details
1	Eastern Bank	UCBL	1 ATM	Feb 7 - 12	BDT 2.5 million initially; (Total BDT 10 million withdrawn)	66 transactions
2	The City bank	The City Bank	1 ATM	Feb 6		
3	N/A	EBL	2 ATMs	Feb 8		
4	Foreign origin; non-branded Malaysian financial institution	Premier Bank	4 ATMs	Feb 14 – 28	BDT 4 million	150 transactions; 1st international cards
5	Foreign origin; cloned cards from Riyadh Bank	Prime Bank	3 ATMs	May 18	BDT 575,000 (BDT 66,000 recovered)	20 transactions

ATM robberies

S.L. (cont.)		ATM booth targeted	Date (2016)	Amounts targeted	Other Details
6	N/A	DBBL	Mar 3	BDT 1.2 million	-
7	N/A	DBBL	Apr 20	BDT 900,000 (recovered)	-

ATM Cards seized (from Dhaka Airport)

S.L. (cont.)	Incident	No. of ATM Cards	Date (2016)	Amounts targeted	Other Details
8	Bag left in front of DHL booth, from Hong Kong	1,000	Mar 3	N/A	-
9	City Bank cards illegally imported from Singapore	100,000	Jun 28	BDT 4 million tax evasion	-

Other Forgeries

S.L. (cont.)	Incident	Businesses or Banks targeted	Date (2016)	Amounts targeted	Other Details
10	Through POS Machines	jewelry shops, fashion outlets, merchant houses and hotels	N/A	BDT 500,000 - 700,000 each time (combined with Item 1-3, possibly BDT 50-60 million)	BDT 5.1 million recovered from fashion outlet; comparing frauds and bank transactions deficits may help
11	Turkish hacking group	DBBL, City Bank, Trust Bank	May	N/A	Links to file archives posted on Social Media

Source: CES Research

The largest heist of recent times was perpetrated by an international group of organized European fraudsters in February 2016. Foreign nationals from Germany, Ukraine, Romania, and UK-based Bangladeshi expatriates have been linked with this heist.[6] Police investigation also found connections with local policemen and citizens of significant social status, including bank officers, businessmen and hotel-owners.

On February 12, sirens went off when 21 suspicious card transactions (subsequently, many more) were detected by EBL from a UCBL ATM. EBL ATMs were also compromised. Initial estimates lost were BDT 2.5 million using over 200 cloned cards using card-skimming technology, at 6 ATMs of 26 banks. The series of incidents, which took place from February 6 to 12, forced banks to immediately shut down card facilities. The police, aided by the Bangladesh Bank Financial Intelligence Unit, found that the German national apprehended was linked to the other foreign nationals, including the mastermind, the UK-based Bangladeshi, all of whom visited Bangladesh in 2014. Since then, multiple trips to the country enabled them to expand their network through local criminal participants, persuading and incentivizing corrupt business entities, e.g. a hotel, to manipulate POS machines. Similarly, corrupt bank officials aided them to make false business transactions with the machines, BDT 500,000 to 600,000 at a

time.[7] As indicated in the Table, the total amount lost in the forgery may stand at BDT 50-60 million, the greater part of it lost through POS machine forgery.

In May 2016, further ATM frauds were recorded. Reportedly having committed 20 card skimming acts at a single Prime Bank ATM, a Chinese man was detained withdrawing BDT 66,000 using three fake cards over five attempts. The Chinese perpetrator belonged to a larger ring. Two of the three in the ring operating in Dhaka, fled the country before Immigration Department was notified, while the total withdrawn amount stood at BDT 575,000 from 3 ATMs around the city. These ATM cards were cloned from Riyadh Bank.

Hackers have also received temporary spotlight as a Turkish group claimed to have gained access to 3 local banks and posted client information on social media. Upon investigation, however, the banks found no noticeable matches with client information.[8]

"How It Occurs"

Fraudsters start with attaining knowledge of the local banking sector, acquiring informed technical accomplices and get-rich-quick-motivated locals, and procuring hi-tech equipment. Using fake IDs, the perpetrators then enter ATMs as banking technicians and install skimming devices in the form of magnetic stripes around the card slot; this copies card information onto the device. The PIN is swindled off using illegally installed cameras in the ATM fascia, pointing at the PIN-pad. Sometimes a PIN-overlay copies the PIN. The miscreant then leaves the ATM, only for their gang-member to return later to extract the device, containing information of all the cards utilized in that slot in-between. They use the information to clone other ATM cards obtained through other means (e.g. theft, imported cards bypassing customs, etc.). The cloned cards are used to withdraw money in a client's name.

Meanwhile, the POS machines are manipulated similarly duplicate (often international) card information. Subsequently, the forged cards are used to make false business transactions which transfer money into the shop-owners' accounts, to be withdrawn. The business gets a percentage from the crime-ring after handing over the amount to them.[9]

Financial Impact of Scams

The scams at ATM booths can have a severely negative effect on personal financial transactions. Bangladesh Bank (BB) statistics show that in the month of February, up until February 15, transactions valued at BDT 2.53 billion were recorded. However, until February 13, the value stood at BDT 2.38 billion. With a usual daily average of BDT 181 million, withdrawals on February 14 saw only BDT 46 million, taking a few days to increase to the average figure.[10] Nervous customers are not to blame. It is incumbent of businesses, banking or otherwise, to ensure consumer confidence, particularly in relation to new technologies.

Existing and Potential Measures for ATM Security

In light of the scams, the Bangladesh Bank (BB) has issued strict guidance to all banks to remain vigilant and implement more contemporary security measures. Usually, in the event of forgery, a bank suspends all debit card transactions, notifying clients. The bank's Fraud Control division then files a police complaint, possibly providing CCTV footage to distribute images to land and air ports. Police and DB then conduct shadow investigations to compare frauds linked with any past cases.

To protect against skimming incidents, banks arguably should have put a few contemporary measures such as PIN-shields, hiding the PIN entry, costing BDT 1000-2000 per ATM. Costlier alternatives, ranging from BDT 25,000 to

80,000 per ATM include anti-skimming devices which protect cards. Thus far, 22 banks have requested for the installation of anti-skimming devices at their ATMs. Although 3,000 ATMs have these devices, recent threats have prioritized installation of these systems in all 7,500 ATMs nationwide.[11]

Banks can also adopt EMV chip cards. These create a unique transaction code upon each transaction, which magnetic stripe cards do not. Banks ought to prioritize the incorporation of this technology after conducting a comprehensive assessment. Even after repeated directives of the BB, thus far, only a handful of banks have introduced EMV chips. Furthermore, the BB has also directed all banks to be certified by Payment Card Industry Data Security Standard (PCIDSS), an information security standard maintained by banks that extend branded credit-card facilities. Only Q-Cash has thus far certified their business.

On a customer level, below are safety tips to minimize the risk of ATM or credit/debit card fraud[12]:

- Covering up PIN entry to prevent hidden camera pickup
- Only inserting cards when the ATM asks
- Checking the card scanner slot with a wiggle for lose, false panels
- Not forcing cards in
- Using familiar ATMs – avoiding doubtful spots or late hours; limiting visits
- Inspecting the ATM card slot for scratches, marks, adhesives or tape residues which indicate tampering
- Checking balance frequently through receipts
- Not accepting external assistance
- Not leaving if ATM Card is stuck; immediately calling the corresponding bank and awaiting instructions, even to cancel card before leaving ATM

Conclusion

As the citizens of Bangladesh embrace the path towards advanced technology in banking, so are their counterparts of high-tech pilferage. Banking scams, counterfeits and frauds have gradually evolved in the dynamic sector that is banking in Bangladesh. With 3,50,000 daily ATM transactions of around BDT 2.5 billion and 35,000 daily POS transactions of nearly BDT 300 million,[13] we require a serious re-look at the existing and potential security safeguards from the financial stewards of the country.

---

1 Ahmed, I., & Rahman, S. (2016, March 18). Plastic money not so safe. *The Daily Star*. Retrieved from http://www.thedailystar.net/frontpage/plastic-money-cards-unsafe-1043614

2 JOSE, S. (2016). ATM Compromises in US Jumped Six-Fold in 2015, FICO Reports | FICO®. Retrieved from http://www.fico.com/en/newsroom/atm-compromises-in-us-jumped-six-fold-in-2015-fico-reports-04-08-2016

3 Rahman, S., & Islam, R. (2013, July 25). ATM forgery unearthed. *The Daily Star*. Retrieved from http://www.thedailystar.net/news/atm-forgery-unearthed

4 Khan, M. J. (2016, February 25). UK-based Bangladeshi masterminded ATM forgery. *Dhaka Tribune*. Retrieved from http://www.dhakatribune.com/bangladesh/2016/feb/25/uk-based-bangladeshi-masterminded-atm-forgery

5 Alo, J. N. (2016, March 2). Premier Bank ATM hit by int'l card scam. *Dhaka Tribune*. Retrieved from http://www.dhakatribune.com/bangladesh/2016/mar/02/premier-bank-atm-hit-intl-card-scam

6 ATM scam probe reveals involvement of many businesses (2016, February 26).*The Daily Star*. Retrieved from http://www.thedailystar.net/city/atm-scam-probe-reveals-involvement-many-businesses-682630

7 Ibid.

8 Hackers steal data from 3 banks: Report. (2016, May 13). *The Daily Star*. Retrieved from http://www.thedailystar.net/frontpage/hackers-steal-data-3-banks-report-1223014

9 Khan, M. J. (2016, February 25). Businessmen let ATM forgers use their point-of-sale terminals *Dhaka Tribune*. Retrieved from http://www.dhakatribune.com/bangladesh/2016/feb/26/businessmen-let-atm-forgers-use-their-point-sale-terminals

10 Islam, S., & Hasan, J.(2016, February 17). *The Financial Express*. Retrieved from http://www.thefinancialexpress-bd.com/2016/02/17/16190

11 Rahman, S. (2016, March 2). Banks move to equip ATMs with anti-skimming devices. *The Daily Star*. Retrieved from http://www.thedailystar.net/business/banks-move-equip-atms-anti-skimming-devices-784951

12 9 tips to avoid ATM fraud. (2016, February 16). *The Daily Star*. Retrieved from http://www.thedailystar.net/city/9-tips-avoid-atm-fraud-511960

13 Ahmed, I., & Rahman, S. (2016, March 18). Plastic money not so safe. *The Daily Star*. Retrieved from http://www.thedailystar.net/frontpage/plastic-money-cards-unsafe-1043614