JOURNAL OF INTERNET BANKING AND COMMERCE

Special Issue: E-commerce trends and future of E-commerce
Edited By: Murat Gülmez

SINGH NP
Management Development Institute, Mehrauli Road, Sukhrali, Gurgaon, India, Tel: +919958298615;
Email: knpsingh@mdi.ac.in; netra.singh@gmail.com

Abstract

Standard Bank of South Africa had lost Rand 300 million in an ATM scam. Scam is executed by an international criminal organization in Japan using fake cards of the customers of Standard Bank of South Africa on 15th May 2016. This fraud is unique in many ways such as location of the fraud vis-à-vis location of the affected bank, duration of the fraud (after office hours), number of person involved (unusually large), fraud amount, number of transactions (unusually large in 3 hours), number of machines used, etc. Keeping in view the unique nature of this scam which looks similar to phishing, this research paper presents an analysis the of key facts about the Standard Bank; ATM fraud;
selection of ATM cash counters and country; possible ways of committing crime; status of investigation; possible suggestions for banks; concluding remarks. Secondary data available on Internet is used in research paper for the purpose of drawing conclusions.

Keywords: Standard Bank, Malware, Seven Bank, ATM-Scam, Credit Cards, Japan, South Africa

© Singh NP, 2016

INTRODUCTION

A sum of South African Rand 300 million was stolen by an international criminal organization in Japan from the account of Standard Bank’s customers using fake credit cards of customers of Standard Bank of South Africa on 15th May 2016. Standard Bank had termed it as “sophisticated, coordinated fraud incident”. Standard bank also described it as “transnational organized crime” which is executed in a highly professional manner by the people who are well conversant with the weaknesses of banking technologies. The other unique feature of the event is that criminals may have got data in a variety of ways including by "skimming" cards. Skimming cards did not have unlimited options to withdraw cash. It means they were sure about the technological weaknesses of two Japanese banks and might have used other methods. It also looks certain that members of the group may belong to both the countries and have some connect with internal staff within and branches outside South Africa and Japan.

On 10th May 2016, Master card issued a copy of charge back guide and announced that Japanese bank will move to new card technology by October 1, 2017. It means there is a security issue in the existing technologies of Japanese banks and perpetrators have exploited it to their benefit [1]. Standard Bank had thwarted such attempts by perpetrators last year and before last year but this time they got success by changing the location and processes [2]. It means Standard Bank was on the target of perpetrators for long time¹.

It is true historically that Banks have to live with frauds and losses due to these frauds. The main methods used for cybercrimes in banks Spear are Phising, Whaling, SMiShing, Vishing etc. [3]. The various facets of credit Delamaire et al. [4] classified credit card fraud in to four categories, i.e., (i) Bankruptcy fraud, (ii) theft fraud/counterfeit fraud, (iii) application fraud, and behavioral fraud. They also presented data mining methods to identify frauds. Worthington [5] found that payment card fraud of MasterCard and Visa branded debit cards have a high risk of frauds. Linda et al. [6] reviewed credit card frauds and frauds detection statistical techniques. Mambozda et al. [7] identified many weaknesses of credit card systems in South Korea in the context of Korean Credit Bureau data theft. The major weaknesses were (a) weak policies of media removable, (b) lack of audit for data bases usage logs, (c) easy accessibility of databases, and (d) lack of regular audit trails. Willaims [8] concluded that laws regarding credit cards are not very satisfactory in Trinidad and Tobago. Willaims [8] mentioned that educating users of cards is very essential in preventing credit card frauds and advised bankers to devise effective policies. Sahin et al. [9] applied classification models based on decision trees and support vector machines (SVM) to detect credit card frauds. Ogwueleka [10] used artificial neural networks and self-organizing map neural network for detecting the credit card frauds. Vadoodparast et al. [11] applied a KDA model for detecting credit card frauds. KDA is a combination of three clustering algorithm, K-MEANS, DBSCAN and AGGLOMERATIVE clustering algorithms. Mohiuddin et al. [12] presented in-depth survey of various clustering based anomaly detection technique and compares them from different perspectives.

As evident from the above mentioned research work that credit card fraud is being analyzed by large number of researchers and its prevention methods are developed by software vendors and financial institutions. It is also true that most of the studies lack adequate data to reach the right conclusions about the utilities of their newly devised models for real time checking of frauds. From the data available in relation to present ATM fraud, the method of fraud is not yet known to the investigation agencies. Whatever, technique is employed by perpetrators, this ATM scam /fraud is unique in many ways and very important to banks and specifically for Standard Bank of South Africa which is already
mired with fines on many accounts in the recent past.

Keeping in view the importance this ATM scam, this research paper presents analysis of different dimensions of this scam in the subsequent sections. This analysis is based on secondary data collected from different sources on Internet in relation to this scam. The data collected is analyzed in the form of content analysis and then presented in different section. This study can be termed as exploratory in nature. Section 2.0 contains the brief of recent three bank scams in three countries. A brief about Standard Bank is given in Section 3.0. It is followed by facts about scam in section 4.0. Why Japan and Seven Bank is chosen by perpetrators is detailed in section 5.0. Possible ways of committing crime are listed in section 6.0. Investigation status is detailed in section 7.0. It is followed by most important actions to be taken by bank in section 8.0 which is followed by concluding remarks in section 9.0. A small paragraph about methodology is included in the section of introduction.

**RECENT BANK FRAUDS**

In the recent years, Global banking system is suffering due to weaknesses of its computer technology based systems. Recently, banks in three countries, i.e., Ecuador, Bangladesh and Vietnam were targeted by cyber criminals. These scams are briefly described in the following.

**Ecuador**

Banco del Austro ([https://www.bancodelaustro.com](https://www.bancodelaustro.com)) was attacked in January 2015 as per the lawsuit filed by the bank in a New York federal court. Perpetrators transferred $12 million to many accounts in Hong Kong (US$ 9 million to 23 banks), Dubai, New York and Los Angeles (US$ 3 million) (Riley (2016)). In this case it was reported by the bank that thieves had used “malware to circumvent bank's local security systems”. As per bank they “gained access to the SWIFT messaging network and fraudulent messages were sent via SWIFT to initiate cash transfers from accounts at larger banks” [13]. In all there were 12 transfers during the period of 10 days. Bank could get back US$ 2.8 million back and initiated legal action in Hong Kong to get remaining money back [14].
Bangladesh
The criminal group was able to steal a sum of about $81 Million from the Federal Reserve’s Bangladesh account in New York through a series of fraudulent transactions. The money was transferred to accounts in Sri Lanka and the Philippines. However, a typo in some transaction prevented a further $850 Million Heist. It is also reported that a malware was installed on Bangladesh Central Bank Systems few weeks before the event which is not yet identified [15,16]. This malware could be a potential Remote Access Trojan (RAT) or a similar form of spyware that gave attackers the ability to gain remote control of the bank's computer. Bangladesh police and expert in the industry blamed SWIFT for the error but these allegations are rejected by SWIFT [17,18].

Vietnam
Tien Phong Bank (TP Bank) reported that it had prevented a cyber-fraud attempt of US$ 1.3 million towards the end of 2015. It had also reported that a third-party service it used to connect with the SWIFT global money transfers system may have been attacked by hackers. TP Bank had discontinued the service of that third party now [17,18]. In this case also a malware was used. It is further reported by the bank that the bank’s risk warning and oversight systems are very strong. Secondly, bank had implemented a tight internal control process. These two factors played key role in stopping the scam. These two components were missing in other two cases.

In these three bank frauds, malware was the key technology components. In one case latest anti malware tool may be in place and in remaining two old versions may be running or may be put on periodic detection mode to maintain the speed of the systems as done by many banks. Barrett et al. [14] reported similarities in three cases. Perpetrators accessed the bank’s system to log on to the Swift network through customer sites, and doing so after the banking hours. It means they have exploited weaknesses of SWIFT network as well.

STANDARD BANK (http://www.standardbank.co.za)

With a heritage of over 150 years, Standard Bank has on-the-ground presence in 20
countries in sub-Saharan Africa. Bank has a strategic partnership with the Industrial and Commercial Bank of China (ICBC). Its headline earnings are R 22,002 million during 2015 which is increased by 27% in comparison to 2014. Its other statistics are (i) headline earning per share (1359 cents up by 27% from 2014), (ii) dividend per ordinary share (674 cents up by 13% from 2014), (iii) net asset value per share (9395 cents up by 9% from 2014), (iv) group return on equity (ROE) (15.3% compared to 12.9% in 2014), (v) cost to income ratio - banking activities (56.7% compared to 55.0% in 2014), (vi) credit loss ratio - banking activities (0.87% compared to 1.0% in 2014). Its employee strength was 54,361 during 2015. Standard Bank has been fined for more than R776.6 million over the past two years. It includes penalties in the UK and South Africa for not having adequate anti-money laundering policies in place. It has agreed to R 573.2 million in settlement after its Tanzanian employees were identified bribing government officials. Standard Bank is still enjoying good reputation in South Africa.

THE STANDARD BANK FRAUD

Key facts about this ATM scam/ fraud are listed in the following

(i) Date of the Scam: The scam happened on 15th May 2016 [19].
(ii) Number of Person and ATM involved in Scam: As per Japanese police, 100+ persons involved across Japan [19]. More than 1000 ATMs are used for withdrawal of money [20].
(iii) Maximum Amount per transaction: The maximum amount of 100,000 yen ($913; £629; R14 300) was withdrawn in each of 14,000 transactions [19]. Since these transactions are below a floor limit and can be processed without bank authorization as per the policies of Standard Bank [21].
(iv) Total Amount of the Scam: Cash worth 1.4 billion yen (US$13 million; £8.8 million) was taken from cash machines or ATMs in Japan using fake credit cards [19].
(v) Credit Cards Used: The credit cards were created with data stolen from a South African bank. The small numbers of fake credit cards were used [19]. As per another source of information 1,600 fake credit cards were used in the ATM scam [22].
(vi) Duration of the Fraud: The money was withdrawn in less than three hours. It was
between 5AM to 8AM. It is also mentioned that total duration was 2 hours.

(vii) Number of Convenience Stores: The money was withdrawn from 1,400 convenience stores (7-Eleven) cash machines (ATM) in Tokyo and 16 prefectures (administrative districts) across Japan’s main island Honshu and neighboring Kyushu [19], the Kyodo news agency. In addition Seven Bank ATMs, located in 7-Eleven convenience stores, were also targeted. These ATM belongs to 2 banks in Japan that allow withdrawals with foreign-issued credit and debit cards [21]. As per another source thieves used ATM run by Seven Bank Japan (http://www.sevenbank.co.jp) which operates 21,000 ATMs in Japan that are located within the 7-Eleven stores across Japan for 24 hours a day [23].

(viii) Tangible Losses: Tangible losses to Standard Bank are estimated by bank at US$ 19.25 million [19] or R 200 Million [22]. It could be R300 Million [21]. Final figure will depend on recovery from perpetrators.

(ix) Losses to the Customers: No loss to the customers as per assurance given by the bank [22]. South Africa’s Central bank also confirmed that Standard Bank would shoulder the losses [24].

(x) Possible perpetrators: It is work of international criminal organization [25]. They might have moved to safer locations outside Japan and South Africa. As per Standard Bank sources, it is done by Japanese fraud syndicate [26].

(xi) What is not known? It is not known that which security measures were compromised internally or externally. The security breach was isolated to Japan or it may happen to other geographies or already happened in other geographies. There is also no information about perpetrators.

WHY 7-ELEVEN CASH MACHINES AND JAPAN?

The perpetrators have done an in-depth analysis of technological weaknesses and other security related issues of Japanese banks as well as Standard Bank of South Africa. Few possible reasons for selecting 7-Eleven and Japan are mentioned in the following.

BBC [19] mentioned that in Japan many bank ATM machines did not accept foreign cards. Operating hours of ATM in Japan are not round the clock but 7-Eleven cash machines
accept foreign cards also ATM of Seven Bank of Japan. ATM of Seven Bank operates 24X7. Secondly, Japanese banks permit the use of vulnerable credit and debit cards with magnetic strips as opposed to the newer and more secure chip and pin technology based credit and debit cards [21]. Thirdly, Japan has long been ignored by international criminal gangs and cybercrime groups because of its relatively isolated location. It means cyber police and investigation agencies may be relaxed in their approach and may lack skills in identifying members of gangs. It will give members of group sufficient time to shift to other safer locations. Last year hackers broke pension data and leaked millions of records in Japan.

Fourth reason could be the reputation of Japan as a low risk country for banking transactions fraud but at the same time it is reported that Japan had badly protected ATM network. If they could have gone to a high risk country detection of large number of transaction could have been identified by Standard Bank Analytical Software or the security systems of acquiring banks [27]. Fifth reason was the weaknesses of analytic software of these two Japanese banks as is evident from the fact that software could not identify spikes of transactions [27]. Sixth reason the overall weakness of the systems of the two banks (Seven Bank and Standard Bank) in catching spikes of unusual activities of account holders [27]. The last but not the least could be distance between two countries. Perpetrators were sure it will take more time for Standard Bank to identify location of the crime.

**POSSIBLE METHOD OF COMMITTING CRIME**

Possible methods of committing this crime depend on internal as well as external security measures implemented by Standard Bank. The perpetrators could have obtained the data from an internal source, merchant or other third party records or by exploiting numeration vulnerabilities of the system.

(i) Banks issue 16-digit credit or debit cards. The first six digits usually for Major Industry Identifier like Visa or MasterCard as well as a Bank Identification Number based on the type of card issued such as gold or platinum. The 15th digit denotes the number of times
that a card has been issued in many cases. The last digit is a check digit. It is a function of the first 15 digits and calculated based on the Luhn algorithm. If one knows these remaining 8 digits or one can guess these remaining 8 digits will be in position to commit crime. In addition, cards have additional information such as expiry date, CVV number. Knowing all may be difficult but not impossible. Perpetrators might have paid for the data in this case or coded the cards [21].

(ii) Perpetrators might have created cards for other banks and might have committed similar crime with other bank at small scale to check their process and then executed it in Japan with the generated data of Standard Bank’s customers.

(iii) Perpetrators might have used networks operated and maintained by third parties as was the case of failed attempt in Vietnam towards the end of 2015.

(iv) Banks (Standard Bank, Banks in Japan) may be using an outdated technology and systems. Perpetrators may be aware of the weaknesses of out dated technologies or may be aware of breaking inbuilt security systems.

(v) Perpetrators may have some connect with internal employees or internal employees may be member of this syndicate. The perpetrator may be helped by third party employees who are responsible for maintenance of the high tech systems.

(vi) Perpetrators might have used some short of phishing techniques with the help of Trojan horse program or any other spyware which could be made effective or active on computer system of the Standard Bank [3].

**STATUS OF INVESTIGATION OF THE SCAM**

Japanese police is examining security camera footage to identify suspects. Japan and South Africa are working with world police body Interpol to investigate how the data was stolen and how the heist was coordinated. No one is arrested so far. The investigation is as sensitive stage [22]. Seven Bank of Japan reported that it is cooperating with police, Japan’s banking regulator, and the Financial Services Authority (FSA) of Japan [27]. In addition, Central Bank of South Africa had advised lenders to be vigilant about credit card frauds [2]. It seems investigation is moving in the right direction as per the investigation agencies involved. However, strange part of the investigation is that a fraud conducted by
more than 100 people (the number could be 150 or 200) with information systems equipped with cameras & other electronic sophisticated equipment’s and investigation agencies are not able to catch even a single member of the Group even after 14 days of the event. Recently, two youths are apprehended by investigation agencies.

What is most important to standard bank?

Most important for Standard bank is to communicate to its employees that bank is a member of global banking information systems. It works with large number of members of its eco-system. Banking information systems are made up of many components which are integrated in to one. Similarly communications networks are operated by more than one technology providers. One component can make your system vulnerable to cyber-attack. It requires very stringent internal control and internal audit systems in place. This is needed due to the fact that individual banks had no control on external components. In an environment of shared control or no control, the perpetrators always target data of customers that are protected by laws from losses. Many bank employees are not aware of these facts specifically sitting on higher position because of their past of manual systems and educational background.

Secondly, bank must go for system’s audit with the help of external information system auditors to identify security risks in near future. It will not only bring out the names and numbers of inside and outside persons involved in helping the perpetrators but also additional weaknesses of the information systems. This information will be very valuable to the Standard Bank. Standard Bank may consider in identifying the technological weaknesses of network providers including SWIFT and fix it. In case of TPBank in Vietnam fraud could have been avoided by identifying weak links with efficient and sophisticated risk warning systems and tight internal control systems. On the other hand Bangladesh central bank could not avoid the fraud last year due to weaknesses of information systems. Bank must devise non-traditional, innovative matrices of security audits which are unique and secretive to Standard Bank in many ways. This information should not be shared even with technology vendors. To mention, statistics with respect to card frauds are available
with central bank of South Africa. These statistics are reported in the public domain with some time lag [28]. What is needed in this case? Standard bank must have weekly analysis and reporting system of card and other frauds and make comparison with past data of central bank with respect to frauds. Standard bank may create its own benchmarks and targets of controlling cards and other related frauds by making all employees accountability for its domain of duties.

It is now known to the bank that its application software could not detect spikes in transactions from given number of owners from a given country which is far off and may not have Standard Bank card holders. Risk and control algorithms are not adequate and need replacement or bank may think of additional layer of security. Banks continue to allow its customer to use cards without changing security data for large number of years. Standard Bank may like to limit the usage of same security data for six months or less.

There are advisory by security agencies that card holders should not enter their credit card details on any third party web application unless they intend to pay for something but in many cases such as registration in scientific conferences, hotel booking etc., credit card number are asked for. There is an urgent need to stop this practice by making new laws for global banking systems.

Standard Bank is getting criticism from investors for a series of fines and fraud losses. It is improving its internal controls. It is enhancing strength of compliance officers to 400. It has already hired about 300 employees to the division over the past year. Standard Bank has also trained staff in spotting “red flags” related to bribery and also employed an external expert [29]. What is needed to train these staff with more use cases to identify weaknesses of the information systems?

Standard Bank should also devise a policy of award and punishment to avoid criticism as in case of Tanzania. Some of the investors criticized of firing of only Tanzania staff and they suggested improvement in the governance processes of banks. In addition, there is a need to full and complete implementation of the Europay, MasterCard and Visa (EMV) standards is required through the processing chain as reported by Kitten [30] and
suggested by Wald, the global director of security solutions at ATM manufacturer NCR.

CONCLUDING REMARKS

Japan has low risk of online bank frauds and in South Africa credit card frauds are historically very low as reported [31]. These strengths of two country’s banking system became strength of perpetrators. Agencies responsible for monitoring and auditing the security of the systems may be at ease since system is working as per their expectation. Perpetrator took advantage of it. More than 100 persons were involved. These people will be moving in and out of premises of ATM and cash machine areas equipped with sophisticated cameras and even after 14 days police could not catch hold of even a single person in two countries. They may be aware of working conditions of cameras and cyber police. Based on the data presented in this article following is suggested to banks or financial institutions.

(i) Create an environment for technology personnel to stay with the institutions for longer duration by rewarding them financially and equipping with the knowledge of changes and complexities of new technologies.

(ii) In addition to training, every week a mail is to be sent to all employees of the banks about the events of security breach happened across the globe and asking the employees to assess the impact of these events. The employees who are responsible for the security of the information system must prepare a report with respect to risk levels of various components of their systems and also the risk level of third party systems used for electronic transactions within and outside the home country.

(iii) Risk of fraudulent transactions must be shared among issuing bank, acquirer bank, technology vendors, network service providers and other organizations of ecosystems. Investigations should not be limited to issuing bank since three additional cases reported in section 2 are pointing towards weaknesses of SWIFT systems.

(iv) If scam is related to skimmers installed on ATM machines, customers must also share the risk. But banks must show a virtual image of ATM as ATM’s first screen to the user/customer indicating the points wherein skimmers can be installed.
(v) All documents in relations to customer’s accounts given to customers must contain details of security and possible breach of the security in the form of hard copy in their native language. These documents may be revised on regular basis. Mobile phones can be used for shorter messages.

(vi) Bank must create a well thought award and punishment system for employees handling sensitive data of the banks. One possible way to record and store their logs in data warehouse which converts data in to read only data.

(vii) Credit card is a part of retail banking. Limits of withdrawals in a given day should be low except for premier customers in the home country. Overseas withdrawals limit may be further reduced. The number of transactions in a day should also be limited to a maximum of three to four.

(viii) Banks must implement EMV standards of security or may devise better standards of security. Customer transaction data must be subjected to analytics/ data mining and rule based real time access of customer privileges. In addition, systems should not be limited to data of logs, systems, software bugs, and numerical figures but should be extended to weaknesses of hardware technologies.

(ix) Banks in many countries do not have system to compulsorily change the PIN of debit cards within a given period of 3 months or 6 months or more. Customers are fully relaxed with respect to most important data of cash out. There is a need to implement such restrictions across the board.

Banks are using large set data sets often stored in data warehouses owned by peer banks across countries, using many independent information systems owned and maintained by different entities to execute customer transaction, and different set of hardware and communication technologies. Therefore, it is necessary to devise methods and processes to identify and fix the security risks in near real time for each component rather than for a system is a whole.
REFERENCES


