THE 12th ASIAN ACADEMY OF MANAGEMENT INTERNATIONAL CONFERENCE 2017

PROCEEDINGS

PARKROYAL PENANG RESORT, PENANG MALAYSIA
6th - 9th OCTOBER 2017
http://aamc2017.usm.my/

EDITED BY: Hooy Chee Wooi, Ruhani Ali, Aizzat Mohd Nasurdin,
T. Ramayah, Khairul Anuar Mohammad Shah

"CHARTING THE FUTURE OF GLOBAL ECONOMY: SYNERGISING BUSINESS AND EDUCATION"

Suspicious Banking Transaction Detection Using Shewhart X-Bar Control Chart

Teh Sin Yin
School of Management, Universiti Sains Malaysia, 11800 Minden, Penang, Malaysia.
tehsyin@usm.my

Chang Yun Fah[ψ]
Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman,
Jalan Sg. Long, Cheras, 43000 Kajang, Selangor D. E.
changyf@utar.edu.my

Wong Voon Hee
Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman,
Jalan Sg. Long, Cheras, 43000 Kajang, Selangor D. E.
wongvh@utar.edu.my

Ee Jia Wen
Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman,
Jalan Sg. Long, Cheras, 43000 Kajang, Selangor D. E.

Abstract

Financial organisation (i.e. bank) is constantly looking at method improving fraud detection to detect and stop the highest-risk transactions. This paper presents a Statistical Quality Control (SQC) approach, i.e. Shewhart $\bar{X}$ control chart for suspicious banking transaction detection based on bank indicator rules and control chart rules. One million bank transaction records performed by 2000 accounts have been simulated. There are a total of 150 accounts randomly selected with 50 of them being indicated as suspicious transactions accounts. Two types of transaction records (i.e. deposit and withdrawal) were plotted on the Shewhart $\bar{X}$ chart in pair. A banking transaction is marked as suspicious when the chart indicates a matching pattern with bank indicator rule or the control chart rule. There are 45 out of the 50 accounts correctly detected as suspicious with 90% of sensitivity and 100% of specificity. Overall, the new method effectively detects suspicious transactions and improve client risk profiling.

Keywords: suspicious transaction, SQC, control chart, sensitivity, specificity.

Acknowledgement: This research is supported by the Research University Grant (RUI) 1001/PMGT/816250, Universiti Sains Malaysia (USM).

1. Introduction

In today's globalised era, money laundering is being committed by criminals around the world to hide their unlawful activities. According to the Laws of Malaysia Act 613, money laundering is defined as engaging in a transaction that involves profit of illegal activities; converting or using illegal profits; or transferring illegal profits in or out from Malaysia. The cooperation of professionals across various industries such as banker, financial advisor, accountant and lawyer in reporting suspicious transaction could help in minimising the incidence rate of money laundering (Frankl & Kurcer, 2016). There are many parties work hand in hand with government in combating money laundering, e.g. cash threshold report (CTR) reporting obligations are imposed on banking institutions and the licensed casino in Malaysia where cash transactions performed by client that exceeding RM50,000 threshold level is required to reported to the government.

A few useful methods such as data mining (Kharote & Kshirsagar, 2014; Luo, 2014; Suresh, Thammi Reddy & Sweta, 2016), link analysis (Helmy, Zaki, Salah & Badran, 2016) and graph mining (Michalak & Korczak, 2011) were applied in the previous studies to detect suspicious transaction that could possibly lead to money laundering. The common characteristic between these methods is to identify the abnormalities in client historical banking transaction records (e.g. deposit, withdrawer, etc.). This paper proposes a Statistical Quality Control (SQC) chart namely Shewhart $\bar{X}$

[ψ] Corresponding Author: Chang Yun Fah, Lee Kong Chain Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Jalan Sg. Long, Cheras, 43000 Kajang, Selangor D. E., Malaysia; Email: changyf@utar.edu.my.

chart in detecting suspicious transaction that probably is a result of money laundering. In order to achieve the objective, bank transaction records were simulated based on actual yearly transaction records with some fraudulent transaction or high risk suspicious transaction. An algorithm for suspicious transaction was developed to detect high risk transaction patterns in control chart that matching with the bank indicator rule.

The remaining of this paper is organised as follows: In the Methodology section, data preparation, the operation of the Shewhart $\bar{X}$ chart, and the control chart rules together with the bank indicator rules are outlined. Next, results and discussion based on the simulated dataset are presented. Finally, conclusions are drawn in the last section.

2. Methodology

2.1 Data Preparation

A new approach is proposed to analyse the bank transaction data and identify suspicious transaction patterns via SQC chart. One million bank transaction dataset performed by 2000 accounts is simulated using the programming tool Python on Enthought Canopy (version 2.7, 32-bit) which run on Microsoft Visual Studio Ultimate 2012 and stored in an Ms Excel file. The simulated dataset is generated by a series of random number functions and hence it cannot represent the real world's bank transaction data. This bank transaction dataset contains variables such as client account identity (Account_ID), transaction amount range from RM100 to RM100,000 (Txn_amount), bank branches in Malaysia (Account_branch) and types of transaction made by clients either is "deposit" or "withdrawal". Noting that the Account_ID is generated using a combination of uppercase alphabet together with numbers and it is stored in an array. The Txn_amount is classified into four categories where category A (53.50%) containing transaction amount in the range of RM100 to RM5000; category B (41.25%) consists of transaction value in the range of RM5001 to RM10,000; category C (5.245%) covering transaction amount of RM10,001 to RM50,000; and category D (0.005%) for transaction amount above RM50,000. The number of transaction for each account is ranging from 400 to 930 in two years duration.

The transaction dataset simulated was tracking the transactions performed from 1st Jan 2013 to 31st Dec 2014 (2 years). The transactions simulated per account were grouped into 5 transactions per period. The total period for an account depends directly to the number of transactions performed within the two years. Sample points used to construct the Shewhart $\bar{X}$ chart is the average amount of the transaction for a period. The Account_branch feature is based on a particular banking financial institution's branches allocated in Malaysia. Any transaction involving an amount of RM50, 000 and above requires the conduct of Customer Due Diligence (CDD) on the client who is conducting the transaction and the beneficiary as indicated by Bank Negara Malaysia Anti-Money Laundering (AML) guidelines (Central Bank of Malaysia, 2001).

2.2 Shewhart $\bar{X}$ Control Chart

Suppose that the bank transaction records follows a normal distribution and X_{ij} represents the n_j transactions for j^{th} account within the past 2 years, where $i = 1, 2, \ldots, n_j$. For this case, the subgroup size k is set as 5. Without loss of generality, mod(n_j) of 5 is considered and hence there is a total of $s_j = n_j/5$ subgroups for j^{th} account. The average and range of the transactions with subgroup s_j are

$$\bar{X}_{ij} = \frac{1}{k}\sum_{i=0}^{k-1} X_{(ki-n),j} \text{ , and} \tag{1}$$

$$R_{ij} = \max\left(x_{ij}\right) - \min\left(x_{ij}\right). \tag{2}$$

The estimator of the transaction grand average, $\bar{\bar{X}}_j$ and average range $\bar{R}_j$ are for j^{th} account are computed as

$$\bar{\bar{X}}_j = \frac{1}{s_j}\sum_{i=1}^{s_j} \bar{X}_{ij} \text{ , and} \tag{3}$$

$$\bar{R}_j = \frac{1}{s_j}\sum_{i=1}^{s_j} R_{ij} \text{ .} \tag{4}$$

The population standard deviation (σ) of the control chart is unknown. Thus, it is estimated from the s_j subgroup ranges. The control limits of the Shewhart $\bar{X}_j$ chart are computed as follows (Montgomery, 2013):

$$LCL = \bar{\bar{X}}_j - 3\frac{\bar{R}_j}{d_2\sqrt{k}}, \quad (5)$$

$$CL = \bar{\bar{X}}_j, \text{ and} \quad (6)$$

$$UCL = \bar{\bar{X}}_j + 3\frac{\bar{R}_j}{d_2\sqrt{k}}. \quad (7)$$

The value of constant d_2 depends on the sample size. For this case, the sample size *k* is 5, hence the d_2 is equals to 2.3259.

2.3 Control Chart Rules and Bank Indicators for Suspicious Transaction

There are 5 bank indicators and 5 control chart out-of-control process rules used in detecting suspicious transactions. An account is indicated as suspicious if the pattern of transaction process violates the control chart rule or bank indicator rule for suspicious transaction. However, violation of bank indicator rules is more significant in this project because these indicators explain the suspicious banking transaction behavior shown. Both withdrawal and deposit transaction patterns are analyzed in pairs to give an overview of the suspicious transactions performed by the client. Control chart analysis is performed on 150 accounts randomly selected from the 2000 simulated accounts.

QI Macros SPC software for Excel is integrated into Microsoft Excel's interface to plot the Shewhart $\bar{X}$ Control Chart. Therefore, control chart rules in the software are used to analyse abnormality patterns on the control chart. Suspicious transaction signal is triggered when the control chart violet one of the following rules (Arthur, 2016):

1) Two out of three consecutive points fall outside the 2-sigma control limits.
2) One or more points plot outside the 3-sigma control limits.
3) Non-random pattern of the control chart.
4) A run of six or more consecutive points steadily increasing or decreasing.
5) 14 points in a row alternative up and down.

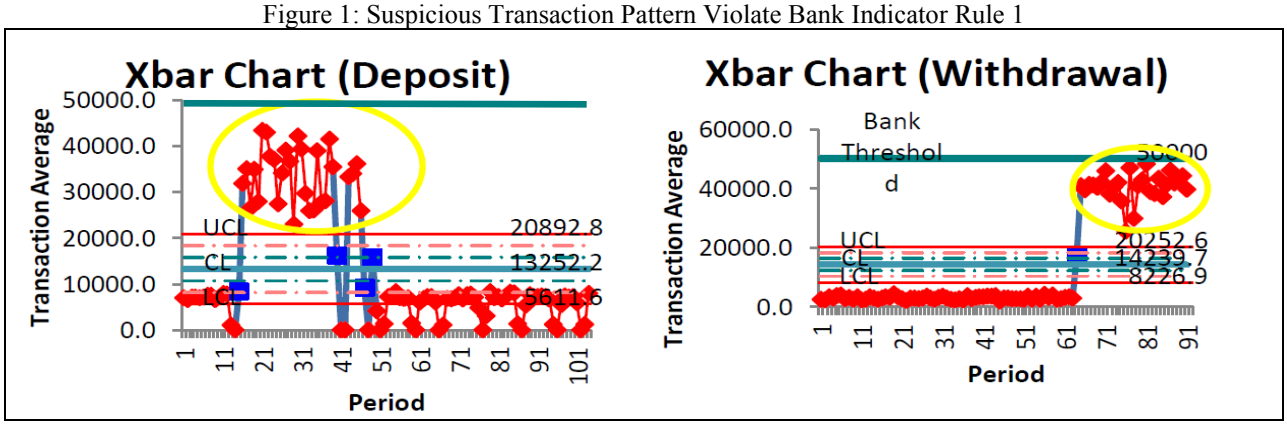
There are many indicators that may point to a suspicious transaction for banks. Among all the indicators, there are a few indicator rules which can be detecting using control chart. The following indicators are applied in this study (FINTRAC, 2010):

1) Deposit or withdrawal of large amounts of money which significantly differ from the client's usual transactions or usual pattern of activities.
2) Frequent transfers in large and round sums in certain periods.
3) Transactions performed in "cyclic" patterns and are non-random.
4) Accounts with a large number of small cash deposits and a small number of large cash withdrawals, or vice versa.
5) Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.

3. Results and Discussion

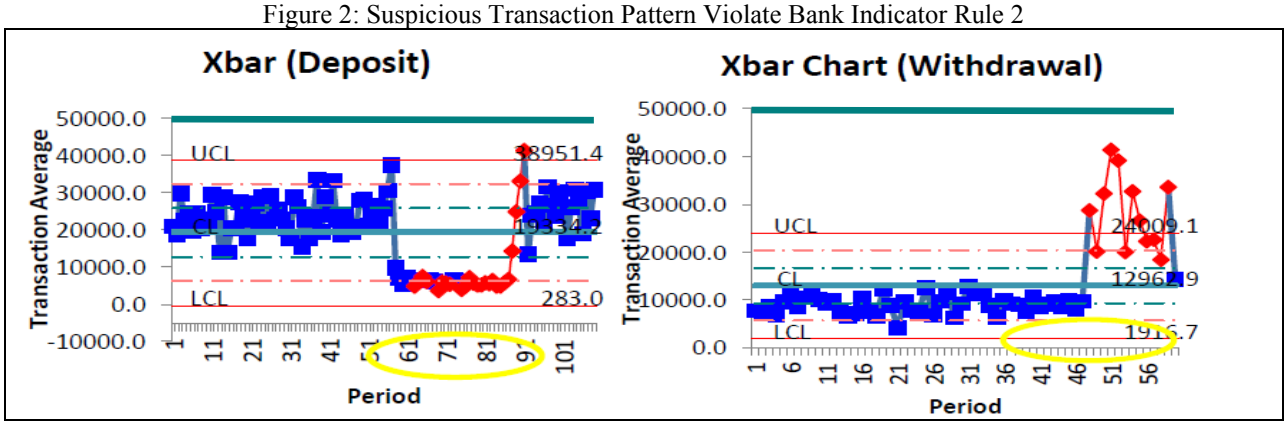
Figure 1 shows a client account with suspicious transaction pattern violated bank indicator rule 1 where the client performed transactions which are significantly different from his/her previous transaction activities. It can be observed from the deposit chart that the process of depositing large amounts of cash only started from period 17 to period 49. The transaction amounts then went back to normal after period 49. The same patterns are observed in the client withdrawal chart, despite the difference in periods of huge cash withdrawals. From the withdrawal chart, the previous withdrawal amounts were below LCL and, the amounts shot up dramatically beyond UCL starting on period 64. There are many out-of-control points plotted outside the 3-sigma control limits which are also matched with control chart rule 2. This client banked in huge cash sums within certain period until the money was fully deposited, subsequently withdrew the money through several withdrawal transactions. The amount of money deposited and withdrawn during that period was just below the bank threshold in order to avoid bank investigation. Total deposit and total withdrawal are believed to have an equal amount. Therefore, the transaction pattern is indicated as suspicious case.

Figure 1: Suspicious Transaction Pattern Violate Bank Indicator Rule 1



Compare both deposit and withdrawal charts together in Figure 2, it can be clearly observed that the total periods of deposit (101) about double of the total period of withdrawal (56). The withdrawal amount starts to fluctuate above UCL during the period where there is no deposit occurring. This abnormal transaction pattern falls under bank indicator rule 2 (frequent transfers in large and round sums in certain periods). Deposit chart also violated control chart rules 1, 2, and 4, whereas withdrawal chart violated control chart rules 1 and 2. Thus, this client account is marked as account with suspicious transaction.

Figure 2: Suspicious Transaction Pattern Violate Bank Indicator Rule 2



From Figure 3, the abnormal pattern has violated both control chart rule 3 (non-random pattern) and bank indicator rule 3 (a cyclic pattern is obvious from the withdrawal process). Both rules emphasize on the randomness of a transaction process. The client performed normal deposit within the range from RM1200 to RM8600. Meanwhile, the client withdrew the money with a certain pattern. From the withdrawal chart, it shows a withdrawal happened every 3 periods and lasts for 4 periods at a fixed withdrawal amount of RM 5500 for the first 3 periods in every cycle. At the fourth period of every cycle, the withdrawal amount decreased to RM4500 and eventually dropped to RM 0. There is no transaction being made within that 3 periods and then it shot up to a fixed withdrawal amount of RM5500 and the cycle repeats again.

Figure 3: Suspicious Transaction Pattern Violate Bank Indicator Rule 3

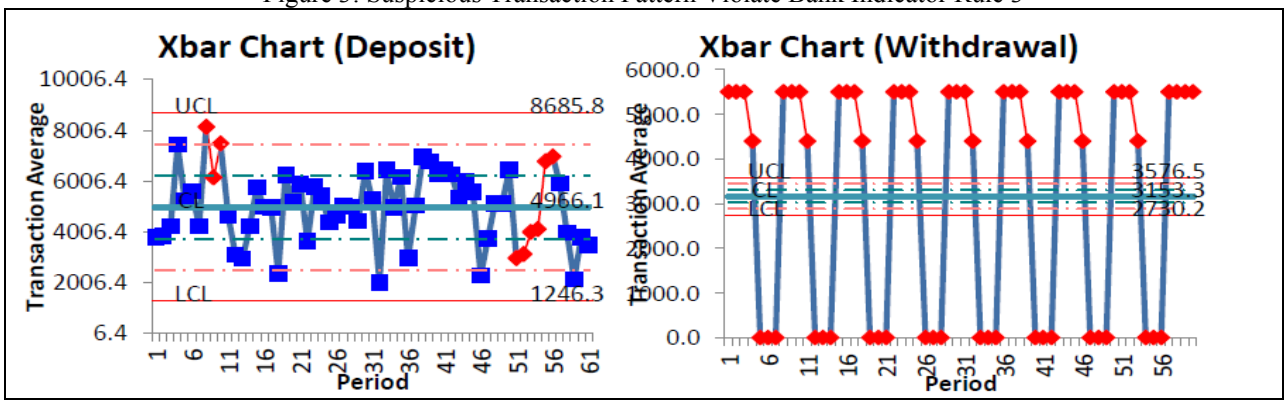


Figure 4a: Suspicious Transaction Pattern Violate Bank Indicator Rule 4 (Small Deposit, Large Withdrawal)

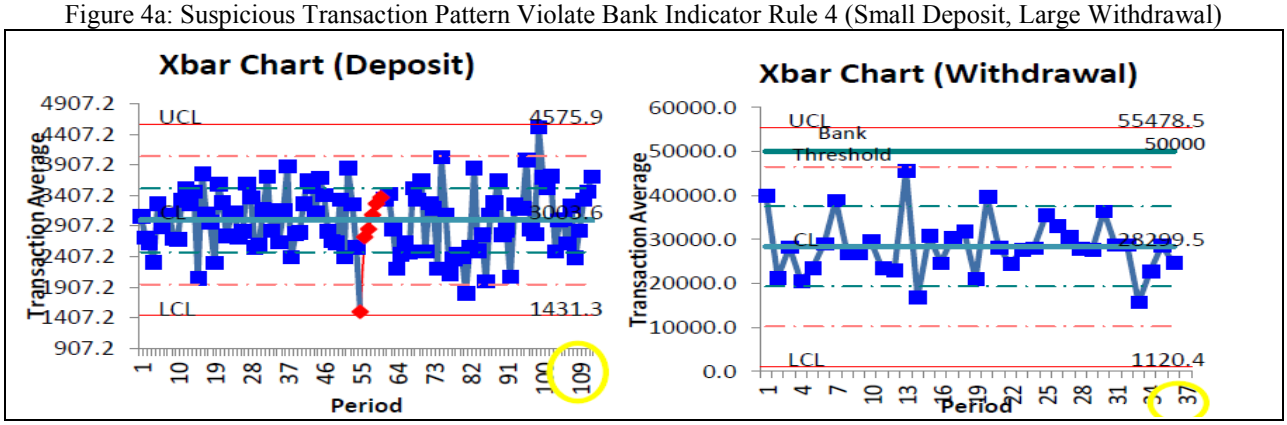
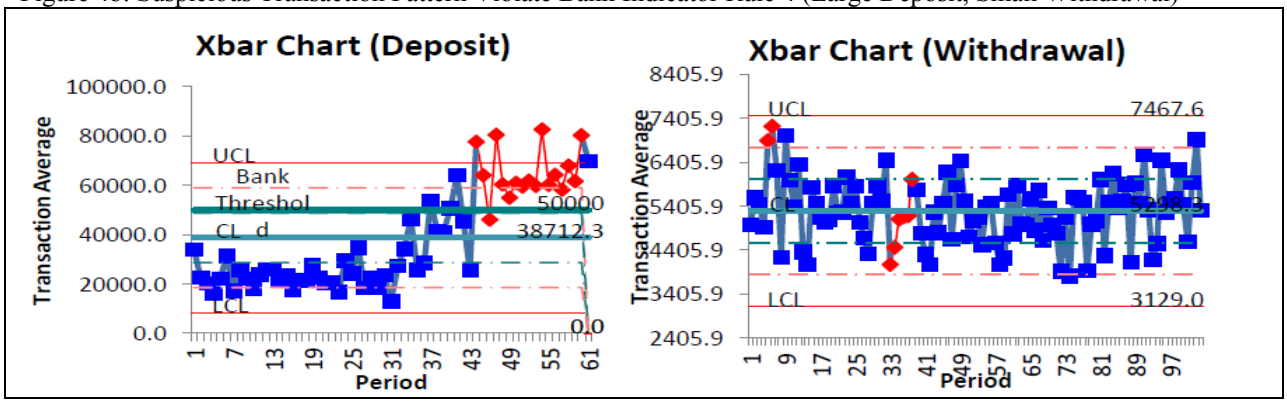
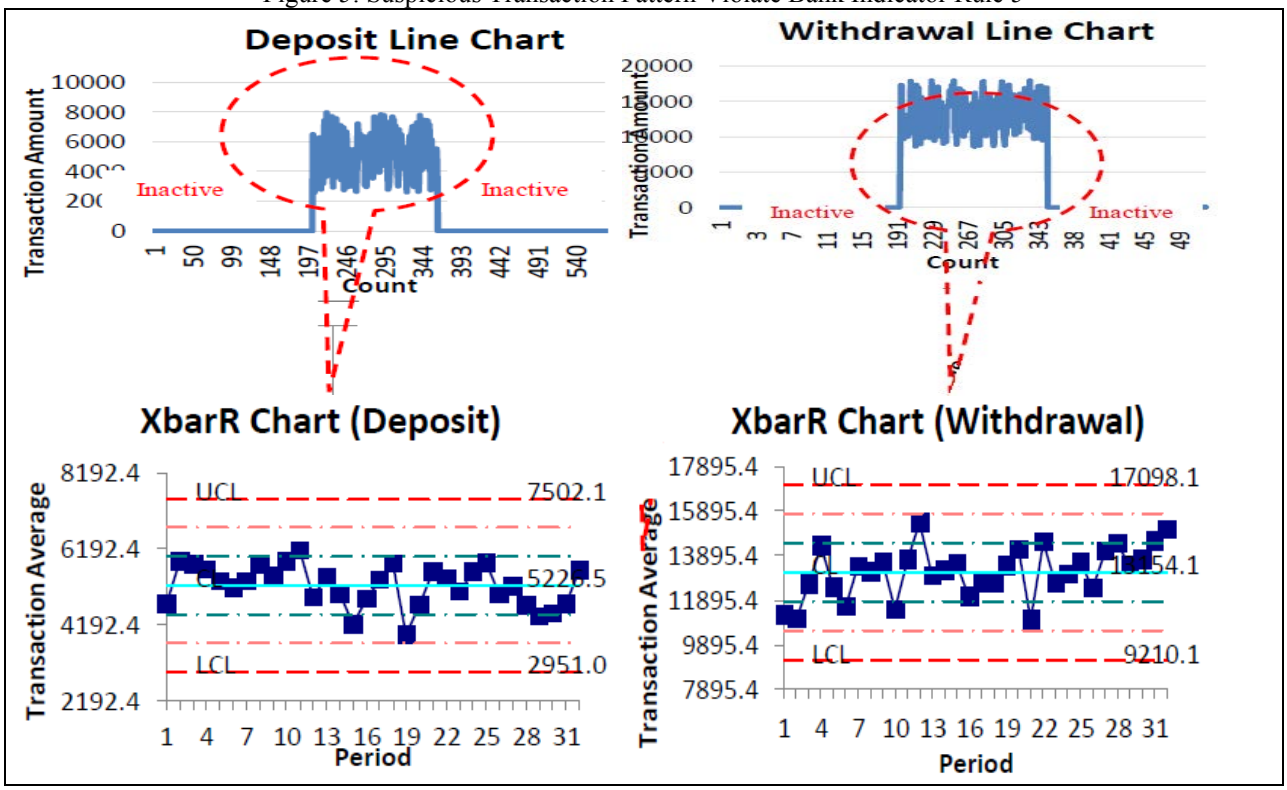


Figure 4b: Suspicious Transaction Pattern Violate Bank Indicator Rule 4 (Large Deposit, Small Withdrawal)



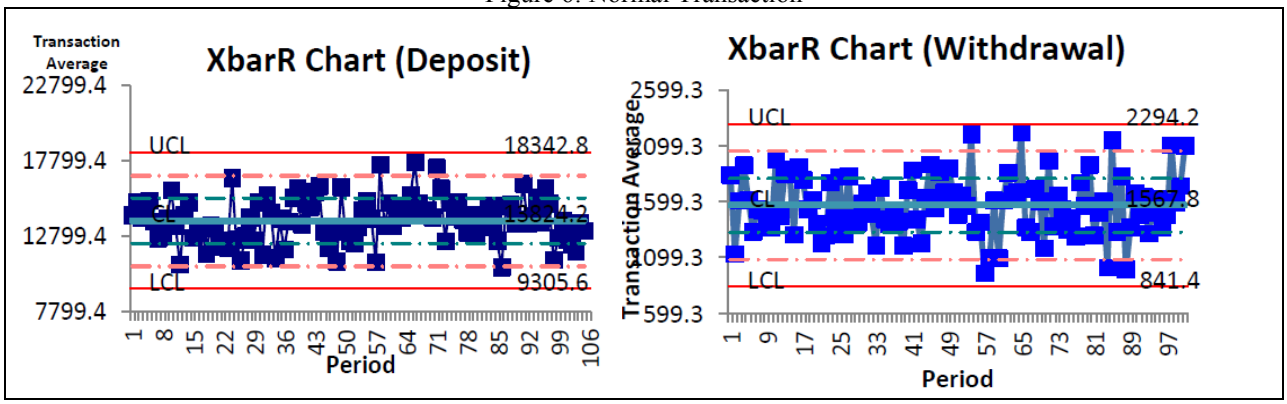
In Figure 4a, the transaction period and the transaction amount had a big gap between the deposit chart and withdrawal chart. The client continuously deposited small cash sums in long-term period and withdrew large amount of cash in short-term period. In this study, 1 period represents 5 times of transactions. In other words, the client performed 545 times (109 periods × 5 times) of deposit in small cash sums and 185 times (37 periods × 5 times) of large amount of cash withdrawal within two years. The ratio of deposit and withdrawal is 3:1. The range of amounts involved in both types of transaction is huge. Thus, the transaction process violates bank indicator rule 4 where large number of small cash deposits and a small number of large cash withdrawals. Deposit chart also triggered an alarm violated control chart rule 4 where a run of 6 points in a row alternative up is observed at period 55. The transaction pattern in Figure 4b is similar to Figure 4a, but the client reversed the pattern of the transaction. The client deposited large cash sums within a short-term period and withdrew in small cash sums within a long-term period. Moreover, deposit chart violated control chart rule 2 and rule 5 where 5 points plotted outside the 3-sigma control limits, and 14 points in a row alternative up and down, respectively. Withdrawal chart violated control chart rule 2 and rule 4 (a run of six consecutive points steadily increasing).

Figure 5: Suspicious Transaction Pattern Violate Bank Indicator Rule 5



In Figure 5, the line charts show the overview of transaction patterns performed by a client. The transaction patterns in the red-dashed circle were magnified and analysed using control chart. Both deposit and withdrawal charts failed to detect any abnormality because the magnified transaction process does not violate any of the control chart rules or bank indicators. However, from the line chart, it can be seen that the client suddenly deposited and withdrew large cash within certain period from an inactive account. The account turned back to inactive status after the money was completely withdrawn. This account will be treated as normal if it is investigated during the active transaction period only. When the whole process comes into view, it will be detected as a suspicious account under bank indicator rule 5 where an inactive account suddenly received large cash deposited followed by frequent cash withdrawals until the transferred sum has been removed. In contrary, Figure 6 shows an example of normal transaction account where the transaction process pattern was in random neither violate the bank indicator rule nor control chart rule.

Figure 6: Normal Transaction



A confusion matrix is developed to evaluate the accuracy of a statistical model that classifies subjects into more than one category. In this study, confusion matrix is used to measure the sensitivity and specificity of the results. There are 150 accounts in total and 50 of them are suspicious accounts. Table 1 shows the accuracy in the number of detecting

suspicious accounts. Sensitivity and specificity is one of the statistical measurements for binary classification test. Sensitivity measures the proportion of suspicious transactions while specificity measures the proportion of normal transactions that are correctly identified. In Table 1, normal account correctly indicated as normal is represents by true positive (TP); suspicious account correctly indicated as suspicious is represents by true negative (TN); normal transaction incorrectly indicated as suspicious is represents by false positive (FP); and suspicious transaction incorrectly indicated as normal is represents by false negative (FN).

Table 1: Confusion Matrix

		Actual		Total
		Suspicious	Normal	
Outcome	Suspicious	45 (TP)	0 (FP)	45
	Normal	5 (FN)	100 (TN)	105
Total		50	100	150

The sensitivity of the proposed SQC method in identifying suspicious transactions is the ability of the control chart to correctly identify normal accounts with normal transactions. The result indicates a 90% of sensitivity to identify high risk transaction as suspicious transaction (true positive). Nevertheless, there is still 10% of suspicious transactions undetected (false negative). On the other hand, 100% of specificity for the proposed SQC method refers to the ability to correctly identify all accounts with normal transaction. The sensitivity and specificity are calculated as follows:

$$\text{Sensitivity} = \frac{TP}{FN+TP} = \frac{45}{5+45} = 0.90 \text{ and } \text{Specificity} = \frac{TN}{FP+TN} = \frac{100}{0+100} = 1.00 .$$

4. Conclusion

In conclusion, it is a tedious task when comes to tracking the suspicious transaction patterns in the big dataset of bank transaction records. Analyse of the client banking transaction patterns is a crucial way to combat money laundering in the society. There are a few approaches were used in the previous researches. The completion of this study has provided an alternative way to identify the abnormalities in client historical banking transaction records. The Shewhart $\bar{X}$ chart is proposed to perform the analysis based on the past deposit and withdrawal transactions records of a client.

Both control chart rule and bank indicator rule were used to identify suspicious transaction. If a historical transaction chart showed a pattern that matches with the bank indicator rule or control chart rule, then the transaction is flagged as suspicious and it shall be analysed further to gain more insight. The Shewhart $\bar{X}$ chart are plotted on a few client accounts with suspicious deposit and withdrawal transactions matched with the five bank indicator rules and/or control chart rules to demonstrate its application. The Shewhart $\bar{X}$ control chart approach gives an overall sensitivity of 90% and specificity of 100% on the tested banking transaction records. It correctly identified 45 suspicious transactions out of the actual 50 suspicious transactions.

Since it is impossible in getting the real world's bank transaction data due to the policies of a financial institution, there is a fundamental limitation to the simulated bank transaction records. The simulated transaction records were based on the historical transaction activities. It means that this method can only analyse previous transaction activities of a client. Hence, it is not suitable to predict the future transaction activities that will be performed by the client. Furthermore, Shewhart $\bar{X}$ control chart failed to detect certain bank indicator pattern. For instance, it is not appropriate to construct the Shewhart $\bar{X}$ chart on transaction records that categorised under bank indicator rule 5 since there was zero transaction being made during certain periods.

Future study can modify the Shewhart $\bar{X}$ chart to enhance its ability in constructing transaction records. Besides, one can also identify other type of control chart such as multi-dimensional control chart or multivariate control chart which is able to combine the deposit and withdrawal transaction to give a better view of the resultant patterns. The next big leap forward is to partnering with financial institution and working on the actual bank transaction records. The proposed approach can be optimizing if it is able to analyse both historical and real-time transaction records and enable researcher to predict the client future banking transaction behaviour.

References

Arthur, J. (2016). *QI Macros User Guide for All Versions of Excel 2003-2016*. Colorado Blvd., Denver: KnowWare International, Inc.

Central Bank Malaysia (2001). *Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Banking and Deposit-Taking Insitutions (Sector 1)*. Bank Negara Malaysia.

FINTRAC (2010). *Guideline 2 – Suspicious Transactions*. Ottawa, Canada: Financial Transactions and Report Analysis Centre of Canada.

Frankl, M., & Kurcer, A. E. (2016). *Money Laundering and Terrorist Financing Activities: A Primer on Avoidance Management for Money Managers.* New York: Business Expert Press LLC.

Helmy, T. H., Zaki, M., Salah, T., & Badran, K. (2016). Design of a monitor for detecting money laundering and terrorist financing. *Journal of Theoretical and Applied Information Technology*, 85(3), 425-436.

Kharote, M., & Kshirsagar, V. P. (2014). Data mining model for money laundering detection in financial domain. *International Journal of Computer Applications*, 85(16), 61-64.

Luo, X. (2014). Suspicious transaction detection for anti-money laundering. *International Journal of Security and Its Applications*. 8(2), 157-166.

Michalak, K., & Korczak, J. (2011). Graph mining approach to suspicious transaction detection. Proceedings of the Federal Conference on Computer Science and Information Systems, 69-75.

MONTGOMERY, D. C. (2013). *INTRODUCTION TO STATISTICAL QUALITY CONTROL (7TH ED.)*. ARIZONA STATE UNIVERSITY: JOHN WILEY & SONS, INC.

Suresh, C., Thammi Reddy, K., & Sweta, N. (2016). A hybrid approach for detecting suspicious accounts in money laundering using data mining techniques. *International Journal of Information Technology and Computer Science*, 5, 37-43.

Asian Academy of Management

UNIVERSITI SAINS MALAYSIA
11800 USM, Penang Malaysia
Tel: 604-653 3888 ext. 3985/2525
Fax: 604-658 7448
Website: www.som.usm.my

ISBN 978-967-394-299-2