"REK-BER" AND MONEY LAUNDERING

Sigit Handoyo
Universitas Islam Indonesia
e-mail : sihando@yahoo.com

ABSTRACT

Kemajuan di bidang teknologi membawa orang dapat melakukan apapun dengan sangat mudah dan cepat termasuk dalam hal penyediaan fasilitas untuk melakukan transaksi secara online Dewasa ini banyak sekali transaksi bisnis yang dilakukan secara online sehingga antara pembeli dan penjual tidak perlu bertatap muka secara langsung.Namun ketika timbul masalah kepercayaan, maka dibutuhkan pihak ketiga untuk menjembatani sebagai suatu media untuk memudahkan bertransaksi. Rekening Bersama atau lebih dikenal dengan istilah Rek-Ber adalah media untuk membantu mempertemukan kebutuhan antara pembeli dan penjual yang dalam hal ini digunakan untuk memastikan keamanan dalam melakukan transaksi. Rek-Ber dapat menggunakan satu atau lebih bank sebagai partner untuk membantu bertransaksi antara pembeli dan penjual dengan cara mentransfer uang. Kemudahan Rek-Ber ini selain memberikan fasilitas yang memudahkan antara pembeli dan penjual, juga mempunyai dampak negatif yang potensial yang akan timbul yaitu pemanfaatan Rek-Ber untuk melakukan pencucian uang (money laundering) hasil dari tindak kejahatan. Potensi dan kerentanan Rek-Ber ini semakin besar tatkala Rek-Ber memilih lembaga keuangan yang tidak mempunyai dan tidak menjalankan program anti-money laundering sebagai partner. Untuk mendeteksi pola terjadinya pencucian uang, bank-bank sebagai partner Rek-Ber dapat menggunakan Data Mining Technology untuk mengungkap aktivitas tindak pidana pencucian uang tersebut.
Kata kunci: Rek-Ber, money laundering, data mining technology

INTRODUCTION

Every financial-related crime such as corruption, bribery, smuggling, workers smuggling, smuggling of immigrant, banking, illegal trafficking in drugs, and various white collar crime needs media to hide its illicit money and it needs to be converted into legal money. There are many ways to convert illegal money into legal money such as by buying some properties using another person's name like relatives, building cash intensive businesses like restaurants, bars, casinos etc. (Standberg, K. 1997). However, generally, illicit money is converted to be legal money through financial institution like bank as a media. Advance in technology used by banks may ease all activities in crimes and is being taken advantage in converting proceeds easily and quick. Since many banks nowadays commit to combat money laundering activities by reporting suspicious activities report (SAR) and currencies transaction report (CTR) to their financial authority in their country, money launderers have been finding other ways to convert that illegal money.

In Indonesia, nowadays, online business transaction is being well known for almost

anyone. By providing advance in technology, merchants may offer their products efficiently and effectively. Some features and facilities are provided to make online business transaction very easy to be carried out. One of those facilities offered in online business transaction is "RekeningBersama" or Rek-Ber or Common Account. This facility is provided by some online business transaction providers to make both buyers and sellers easy to carry outa transaction. Rek-Ber is operated still by using some banks as partners for payment facility. Due to the weakness of an operation control of this facility, this facility would be becoming vulnerable to be engaged on money laundering activities.

NATURE OF MONEY LAUNDERING

Money Laundering is an activity to convert illegal money into legal money by laundering in such ways through any media, particularly through financial institution system like banks. Another definition of Money Laundering is defined as "….to knowingly engage in a financial transaction the proceeds of some unlawful activity with the intent of promoting or carrying on that unlawful activity or to conceal or disguise the nature, location, source, ownership, or control of these proceeds" (Watkins et. al., 2003).

Basically money laundering process is comprised 3 phases (Madinger, J. and Zalopany, S. 1999) : placement, layering and integration. Firstly, placement, traditionally attempting to place cash derived from criminal acts into the financial system. This step aims to hide temporarily the money before the launderer takes the next step. Secondly, layering or transferring illicit money from the financial institution in the first phase to camouflage that illegal money. By conducting layering, it is difficult for law enforcement agencies to trace the origins of such assets. Thirdly, integration which is the process to accumulate its illicit money after finalizing from the second phase in one or some places like putting this illicit money into in legal business. After finishing the third phase, it is difficult to detect whether that money legal or illegal.

MONEY LAUNDERING AND ITS TYPOLOGIES IN INDONESIA

Money laundering activities in Indonesia has been long time ago seemed untouchable and it was seemingly being hidden by certain parties until 2001 when Indonesia was to be considered as one of Non-Cooperative Countries and Territories (NCCT) in combating money laundering activities. Thus, in 2001 Indonesia urged to sign the MoUof the cooperation in eradication on money laundering activities.

As money laundering is an activity to convert illegal money to be legal money, generally, many cases of money laundering activities in Indonesia relate in corruption case. This situation makes sense since Indonesia was granted as one of the top ranked of the most corruption countries in the world in 2003.

It is no wonder that Indonesia has been becoming a heaven for financial criminal to launder their illegal proceeds. It was stated (PPATK Annual Report, 2011)that there were 108,145 CTRs and SARs or Rp.100 trillion reported by financial institutions in Indonesia that potentially a money laundering activities. The highest case is from corruption activities stated 44.1%, followed by concealment 23.4% and bribery 3.8%.

Basically, typology of money laundering is the same for any country. The difference typology of money laundering among many countries depends on what factor will influence the push or pull factors such as condition of their politics, social, and economy. Based on PPATK report, typology of money laundering in Indonesia can be categorized as following:

1. Transferring of money from government institution into account of a key person. This typology of money laundering

involves perpetrator government employee who is also involved in corruption. By using another person's bank account, this perpetrator would be able to launder his/her illegal money. In a developing country, like Indonesia, this typology is very common since a weakness of internal control of the government system can make possibility to do this illegal activity.

2. Using a fake identity to make new bank account to be used to layer his/her flowing illegal money recorded in banks. Perpetrator will immediately close his/her account once transferring process of his/her money accomplished. In Indonesia having a fake identity is not really difficult to be carried out. Because of this reality, this typology is easy to be done.
3. Cash bribery using dirty money. By using this typology, fraudster is doing twoo criminals in one strike. Firstly, fraudster is doing bribery which is doing corruption, and secondly, he/she is doing money laundering to achieve his/her goals.
4. Other type of bribery such as giving luxurious things as a gift sourced from illegal activities or crime.
5. Using life insurance. In this typology, launderer will join life insurance by paying a lot of money for the premium regularly but not for a long term. In a few months he/she will closing down the insurance with a certain reason and will take the money he/she has paid plus some fines from the insurance company. Once, he/she took his/her money from insurance company, the money has already been washed.
6. Conspiracy on using bank account. Money launderers may use this typology by using some bank accounts to laundry their money. By using many accounts, money launderer may transfer using many accounts in one time. By transferring little money to many accounts, it may give money launderer to layer their illegal money safely. This is like when we pour water form a jug to many glasses slowly but sure.
7. Using Tax Return. Money launderers will pay much tax exceed from their obligation. In the end of tax period, they will request tax return from tax office. In this case, tax office must be scrutinized to be familiar with the profile of tax payer.
8. Budget Mark-up. This is done to take some money from the exceed budget seems that illegal money like part of budget to financing.

TYPE OF BANKS ARE CHOSEN BY LAUNDERER

Banks have important role in money laundering activities. Bank having poor anti-money laundering controls is having significant possibility to be engaged in money laundering because some of their customers who are engaged in criminal behavior will take the advantage of the opportunities. These banks become correspondent banking for the other foreign banks which typically highly risk bank in money laundering that are used by criminal to transfer their illegal money to open account at other correspondent banks. Due to the lack of resources and staff, those banks tend to use their correspondent banks to carry out the operation of their banks.

There are three kinds of high risk potential correspondent banks in money laundering activities: shell Banks, offshore banks, and licensed and regulated banks (Minority Staff of the Permanent Subcommittee on Investigations. 2001). Shell banks are high risk banks principally because they are so difficult to monitor and operate with great secrecy. Offshore banks are banks which have licenses which bar them from transacting banking activities with citizens of their own licensing jurisdiction or bar them from

transacting business using the local currency of the licensing jurisdiction. Finally, licensed and regulated banks are banks that officially established in a country but have weakness in money laundering control activities.

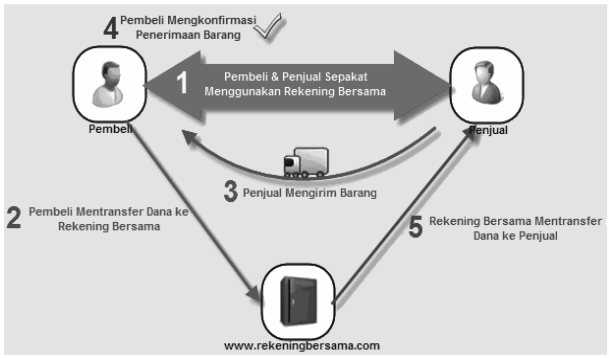
Once a correspondent account is open in a bank in a country, not only the foreign banks but also their clients can transact business through the banks in that country. As a consequence, those correspondent banks become a gateway for money launderers to carry out their actions in financial system. For example, this case occurs in the US. High risk foreign banks have been able to open correspondent accounts at US banks and conduct their operations through their US accounts, because, in many cases, US banks fail to adequately screen and monitor foreign banks as clients (Minority Staff of the Permanent Subcommittee on Investigations. 2001).

OTHER WAY TO LAUNDRY

Financial institutions, like banks, are now generally having anti-money laundering prevention. This situation gives launderer some difficulties to launder their illicit money and they keep trying to find other way to launder. However, nowadays criminal may take some advantages of online business transaction to launder their illicit money. All of the steps of money laundering can be done only by using online business transaction. Placement, layering and integration are easy and save to be taken in a short time without suspiciously detected. In short, it can be said by benefiting of the ease of online business, money laundering can be much easier.

Business transaction via on line is one of the ways to launder that is to be chosen by perpetrators because it provides many opportunities for them. Many on line business transactions are really vulnerable to use in laundering illegal money. This type of on line business commonly is in a country that does not have or does not have tight regulation in transferring money using third party. In Indonesia, recently, this kind of business is becoming a booming since this business does not require a rigid requirement issued by government relates transfer of money. This type of business generally needs media to manage transferring money. They call this media in transferring money in this business is "RekeningBersama or RekBer".

In Indonesia, the term of Rekber meaning is a Common Account to be used to make an online business transaction by people who are involved in. Rekber is a third party lied between sellers and buyers. This media is established as an answer to help a difficulty faced by both sellers and buyers to make transaction. Both sellers and buyers are sometime really difficult to belief each other since they have not been met each other before. Thus, they need a third party to get involved in. The mechanism of Rekber can be shown as a chart below:



It can be seen from the chart that Rek-Ber is laid between buyers and sellers. When buyers and sellers agree to make transaction, buyers will pay some money to sellers by transferring their money through Rek-Ber as a media of payment. Once products have been delivered and received, buyers will inform Rek-Ber and ask to pay their money to seller. From this illustration, it seems that there is no matter with the process of transferring of money and there is no relationship with a potential possibility of money laundering activity. However, Rek-Ber is always involving

some financial institutions instead of one. This situation makes a possibility for anyone to use Rek-Ber as a media to laundry illicit money. The ones who will laundry their illegal money will make more than one transaction for more than one financial institution. In money laundering phases, it is considered to placing and layering of illegal money. Thus, it can be said that RE-Ber still has vulnerable on money laundering activities.

DETECTION

Detection on the pattern of the activities of money laundering activities has been developed since several decades. Some techniques have been employed to assist in investigation that activity. There are two techniques to reveal money laundering activities: traditional technique and new technique using data mining technology.

Traditional investigative techniques have some weaknesses that emergence need new approach in terms of time consuming in identification and man-hours consuming. In this approach, identification of money laundering patterns takes a long time because there are difficulties in both processing large volume of data sets and accessing of expert data.

Advances technologies have been developing law enforcement to identify and to detect the patterns of fraud including money laundering activities in several years. Recently, it is introduced technologies to detect those patterns in 1990s, named Data Mining Technologies or new technique. There are three benefits in utilizing data mining technologies which are efficient in time consuming, reducing problems in financial investigations, and the identification of more leads, accurate and timely leads.

Data mining technologies are new innovative approaches utilized to investigate the patterns of money laundering. There are two tools introduced in data mining technology, which are Financial Crimes Enforcement Network AI Systems (FAIS) and Origami software package. Both of them are used to assist in identifying money laundering activities and patterns. FAIS needs report of the large transaction (CTRs and SARs) to evaluate the patterns of money laundering.

In Origami method, investigation is conducted by analysis network to reveal illegal activities through telephone line. Some of the most popular tools in data mining application rely on statistical and artificial intelligence (AI) techniques, such as linear regression, logistic regression, cluster analysis, inductive algorithms, neural networks, fuzzy logic, and genetic algorithms.

Linear regression model, the most basic approach in data mining, is designed by defining a dependent variable (output) and a number of independent variables (inputs). The result of a linear regression model is an equation of a line that best fits the data set, which can be used for prediction process.

Logistic regression is very popular means of data mining because it can solve problems involving categorical variables. While, cluster analysis can be used to mine large data sets for investigative lead generation and to isolate statistically significant relationships between suspect networks, modes of conveyance and locations from which drugs and illegal proceeds are exchanged. Inductive algorithms can assist national and international investigators uncover money laundering patterns by generating decision trees based on historical outcomes.

Neural networks are the technique utilizing digital computers to mimic the operation of the learning structure that exist the human brain. This technique also can be used with continuous or categorical variables and non-linear and collinear data.

Fuzzy logic is the technique utilizing a theory that allows incomplete information to be processed and conclusions derived. While, genetic algorithms are the technique used to

tracked money laundering operations and to solve a variety of optimal tasks.

Related to the detecting, preventing and analyzing the pattern of money laundering, there are two generations of data mining technology which are first generation and second generation. The first generation nowadays is not being used anymore due to its weaknesses such as in detecting money laundering schemes of smaller amounts.

Nowadays, the second generation data mining technology is being used in combating money laundering. This generation consists of four keys risk assessment components (Menon, 2005):

1. Client Risk Assessment by using detailed information and transaction activities which collected at the time that an account is opened to investigate all aspects of the customer's profile. In this step involves analytical activities of the customer's profile but are not limited to:
   a. Watch list name screening, not only the name and account individually but also the names other individuals and organizations that are affiliated with the account.
   b. Country alerting
      Countries which are categorized as a high risk country related to money laundering based on information from Financial Action Task Force (FATF) can be flagged for further investigation.
   c. Channels which used by the account holder can include information on the financial representative of the account, the branch office, and point of origin pertaining to the online banking activities of the account holder.
   d. Business Relationships
      In the business affiliation is usually provide additional profiling criteria including the names, the number of business relationships that are associated with the account holder.
   e. Political Affiliation
      One of the customers having high risk in money laundering is the one who are occupying political offices. Thus it is needed to have more profile from those customers.
2. Transaction Risk Measurement by identifying and filing account related transactions that pose the greatest risk for potential money laundering activities. These transactions involved three categories:
   a. Funds related behaviors, these transactions include internal transfers between accounts, rapid movement of funds in or out of the account, or sudden activity into a previously dormant account.
   b. Transaction related behavior
   c. Miscellaneous behavior, in these transactions which have high frequency in changing accounts including the movement of funds without a corresponding trade and transaction in stock in the short period between buying and selling date.
3. Behavior Detection Technology is to detect suspicious patterns of behavior that may be hidden beneath large volumes of financial data by using specific technology which include:
   a. Scenarios which is a combination of rules and/or conditions which define the transaction pattern that is being detected. For instance, in transferring money from or to the suspected countries which have a high risk in money laundering should involve a code in the transfer receipt.
   b. Thresholds, the data elements those are relevant to particular scenario or pattern. Thresholds have an important role in eliminating of false positive and ensuring only the most relevant results that will be reported.

c. Alerts, such as a signal when the process finds to any possible matches of potential money laundering fraud that is needed to be further investigated.
d. Look back period and its frequency.
Look back period is a period of time, could be a day to 12 months, in monitoring of the scenario in each run of the detection process. Frequency is a periodicity needed by scenario to run the process that can be daily, weekly, monthly or yearly.

4. Workflow and Reporting Tools is to assist in alerting investigation and compliance reporting which include:
   a. Case management
   This tool is consisting case management providing an alert analysis workflow which is integrated with the basic compliance reporting tools.
   b. Record keeping
   In term of the compliance review, this tool record a particular series or records and additional information which needed by federal law or financial institution.
   c. Reporting
   The transaction and watch list filtering solutions that generate Suspicious Activity/Entity Reports, Currency Transaction Reports (CTRs) and any other customized reports for internal stakeholders or federal regulators are provided by this tool.

By employing Data Mining Technologies, it can be traced the pattern of money laundering activities. Rek-Ber that uses banks as a media of transferring money cannot avoid this data mining technologies as banks nowadays are using data mining technologies to read the pattern of money laundering. Except for Rek-Ber that is not involving the banks that do notobey money laundering regulation from Bank Indonesia, it is difficult to detect money laundering pattern.

CONCLUSION

Rek-Ber is a media established by online business transaction providers to facilitate buyers and sellers easy to carry out a transaction safely. However, financial institution or banks involved in Rek-Ber that do not comply regulation from Bank Indonesia relates money laundering activities can be a vulnerable media on money laundering activities. Hence, Rek-Ber providers have to choose financial institutions or banks as a partner wisely and prudence even though still have a possibility for money launderer to laundry their dirty money by using some banks for some transactions at once.

REFERENCES

Annual Report. PPATK.2011

Madinger, J. and Zalopany, S. 1999. *Money Laundering: A guide for criminal investigator.* New York: CRC Press.

Menon, R. and Kumar, S., 2005. *Understanding the Role of Technology in Anti-Money Laundering Compliance.*http://www.infosys.com/finacle/pdf/Anti_Money_Laundering_Compliance.pdf.

Minority Staff of the Permanent Subcommitee on Investigations. 2001. *Report on Correspondent Banking: A Gateway for Money Laundering*. *www.senate.gov/~gov_affairs/psi_finalreport.pdf*

Standberg, K. 1997. Money Laundering.*Law Enforcement Technology*. 4:28-33

Watkins et. al. 2003. Tracking Dirty Proceeds: Exploring Data Mining Technologies As Tools To Investigate Money Laundering. *Journal of Policing Practice and Research.* 4(2);163-178

www. rekeningbersama.com