Lan Zou

Task 16

**1.     Rule based Fraud Detection**

  To avoid money launching problem:

If any account suddenly transfer large amount to a strange (meaning never have similar amount transfer happened before, or to any new receiver account), which the transfer is not periodic or highly frequently. If the transfer is in a huge amount(such as 0.1 million or higher) and rare compared to historical transfer.

Even when the huge amount transfer is divided into couple smalll transaction to the same or similar accounts. The system should monitor the total amount to check if it is huge amount transfer.

Also the IP address is another clue for the rule. If all the potentially criminal transfer are from or to a single IP address in a short time.

Transfer in and out from the same account should also get attention, particularlly when the amount is huge and round.

This rule is targeted on money launching fraud, by focused on the amount in transcation, account and IP address to get the information of usually and highly criminal transferring behaviour compared to the historical record. This rule is observed in transaction and reflects 80% probability of having money laundering fraud.

**2. When Can Fraud be Detected**

This can refer to terror financing fraud, where one promising a reward and ask another to send money to get.

The Remitly system should set alert that ask the purpose of transferring from their sender, like whether the transfer is a for a reward or for any product that asked to send money first but to a totally new receiver. If the sender check this box and notice the transfer is for a reward as cash or non-cash, all transaction between the same sender and receiver is highly criminal. The Remitly system should terminate all transaction with the purpose to get a reward, and ask the sender no longer send any money under the same or similar situation or receiver.

Also Remitly should blacklist all the potential criminal receiver in the database and block all the transaction to and from the account. If necessary, Remitly should notice other banking or financing system or police station to avoid similar fraud account.

If the address of the receiver is in a ISIS identified area, such as Mexico, and unseen in the historical record from the sender’s accounts, the transaction is in observed with possible flag.

Additionally, if the receiver account or the sender account is new account or never used for a long time but suddenly active to transfer a large amount money, the transaction is in possible flag.

**3. Fraud Information Sources**

Information from the credit reporting agencies can be useful. The credit reporting agencies set up a system related to couple major credit card company, such as Bank of America, AMEX, citi bank and Chase.

For example, citi bank has the highest market sharing rate compared to all other bank over the world in 2015. They has data and clients not only in the US or Asia, but also EU or Africa, so many international transfer is via citi bank and the bank hold many international transaction recording. Citi bank is also known as one of the bank highly sensitive to anti-money or hot money transfer by observing their clients account activities for years or even decay. At the end of every year, the credit reporting agencies cooperated with citi banks will ask for an annual financing reporting of their big clients who hold or have large amount of the money in the account or in historical transactions. All these clients will have a special database and record where citi bank can run an internal algorithm to explore the transaction behavior and account activity. Once any unusual activities happened, citi bank will alter credit reporting agencies and report all their information for any future investigation. This information included name, SSN or ID number, address, account activities and account amount.

Credit reporting agencies get the information in their system and ask whether lower their credit score, ask for a explanation and proof, or directly close their credit card or related account. On the other word, the detail information of some of potential criminal account and account holder is in observed.

If Remitly can get support from credit reporting agencies, the credit histories of some of their client is noticed and alter from potential criminal activities.

**4. Instant Payment Clearing**

Alice’s bank will send a payment request under the standard of ISO-20022, include the information of message ID, account information, party information, physical address, agent, amount, remittance, and bank transaction code. After gathering information, the system will generate a payment order containing receiver's information: name, bank account information, payment amount detail to the bank of instant processing. The the processing bank will create a payment order to SWIFT.org. SWIFT will send the information and amount to the recipients.

**5. Instant Payment Clearing**

SWIFT GPI may be helpful in this situation. It build a trust network among different banks. Under SWIFT, the receiver's bank trust the supplier's bank to pay at the end of the day when the money is received before cut-off time. The local clearing and settlement are attached after each transaction, besides that, SWIFT is actively worked with payment infrastructure to enhances this. A tracker observe each transaction in the database, once the transferring status changes, all the information will send to receiver's bank, with a UIUD and UETR code. UETR allow the receiver's bank track the transaction like a expressing tracker with every step updated in the tracker database. All this transaction in under a central service system, which require information under SLA, included end-to-end same day processing of payments, transfer of full original amount, transparency of fees/ FX rate, end-to-end tracking of payments, transfer of payment information. Under SWIFT, the speed, transparency, traceability, unlimited, and instant payment can be achieved among different banks.