22/06/18

PaymentS NAME Screening

# BackGround

Every transaction in DBS needs to be scrutinized so that frauds like money laundering, suspicious money transfers can be detected.

For the purpose of checking these transactions there is a central authority that provides data against which we check whether the transaction is fraudulent or not.

The central authority provides us with data list examples are given below: -

**Please find the list in the data folder for problem 2.**

## **WatchListEntries.csv**

Every cross-border transaction done in a bank uses a message encoding called swift message.

Below is a sample swift message(MT103).

{1: F01DHBKHKH0AXXX0000000000} {2: I103DBSSSGSAXXXXN} {4:

:20: IPE-LRT-103-SINGLE

:23B: CRED

: 32A:200418SGD12500,

:50F:/0039456320123

1/Osama Bin laden5

2/SA/SAUDI ARABIA

:59F:/4822311091233

1/Pavan Hitesh

2/The Great Banjara Park

3/SY/Syria

:71A: SHA

-}

We only consider **MT103** type messages for this hackathon

You can read more about how to decode these messages here: -

<https://en.wikipedia.org/wiki/MT103>

Useful API to decode MT103

<https://www.paymentcomponents.com/demo/mt>

From the above swift message, we decode

Sender: - Osama Bin laden

Receiver: - Pavan Hitesh

Country Sender: - SAUDI ARABIA

Country Receiver: - Syria

**Hint: Also keep a big eye on the following tags**

**{1: F01DHBKHKH0AXXX0000000000} {2: I103DBSSSGSAXXXXN}**

**Tag 1 and tag 2 contain bank identification codes, which specify where the banks of this transaction reside. This can play a significantly important role.**

## Scenario

### Osama Bin Laden transfers money to Pavan Hitesh, since Osama is in the suspicious person name list this raises an alert.

# What we are trying to solve?

# COnsider the following message: -

{1: F01DHBKHKH0AXXX0000000000} {2: I103DBSSSGSAXXXXN} {4:

:20: IPE-LRT-103-SINGLE

:23B: CRED

: 32A:200418SGD12500,

:50F:/0039456320123

1/Osama Bin Laden

2/IN/INDIA

:59F:/4822311091233

1/Pavan Hitesh

2/The Great Banjara Park

3/SG/SINAGPORE

:71A: SHA

-}

## Scenario: -

### Osama Bin Laden is an Indian transferring money to Hitesh in Singapore; both the countries are non-suspicious yet because of Osama an alert is raised.

### This is called a false positive scenario there are many such scenarios you can think of and help us bring them down.

### And today we face 30% of such scenarios where false alarms are raised.

# What We will provide?

## List of Suspicious person and org list as described above. These lists are dynamic and keep changing every day regularly please keep this in mind.

## **WatchListEntries.csv**

## ENTRY\_TYPE: **Person** / **Organization**

## ENTRY\_FIRST\_NAME: **First Name**

## ENTRY\_MIDDLE\_NAME: **Middle Name**

## ENTRY\_LAST\_NAME: **Last Name**

## ENTRY\_FULL\_NAME: **Full Name**

## DECEASED: **Is dead or not**

## GENDER: **Gender**

## ID\_SET: **Passport Number, SSN number etc.**

## NATIONALITY\_COUNTRY\_SET: **Nationality**

## DATE\_OF\_BIRTH\_SET: **DOB**

## PLACE\_OF\_BIRTH\_SET: **Birth Place**

## ENTRY\_UPDATE\_DATE: **Last updated**

## IS\_BROKEN: **Is the name broken into first/middle/last**

## CITIZENSHIP: **Which country’s citizen**

## ADDRESS\_SET: **All possible addresses**

## AGE: **Age of the person**

## ALIAS\_SET: **Different name for the same person or organization**

## Data Set

### Training Set

### Testing Set

### Validation set – will be provided few hours before the ending time

## Data Description: -

|  |  |  |  |
| --- | --- | --- | --- |
| **AlertStatus** | **Score[\*]** | **alert\_date** | **Message Text** |
| PASS | N.A | N.A | {Swift Message MT103} |
| False Hit | 95 | 24/03/2017 18:43 | {Swift Message Mt103} |
| Blocked | 100 | 24/03/2017 18:43 | {Swift Message Mt103} |

### **[\*] Score is the score generated by the alert detection system which tell whether to block the transaction or not.**

### **For now, we have a threshold of 85 if the score is less than 85 it goes to pass category else it is blocked and rectified as False Hit later by the operations.**

### **Alert Status Description:**

### **#**PASS**: System marks them as non-suspicious transactions and are allowed.**

### **#**False Hit: **System marks them as suspicious messages but operations tell that they are non-suspicious i.e. False Positive**

### **#**Blocked: **System marks them as suspicious messages and these are blocked by the operations. i.e. False Negative**

### **Hints:**

### **Hint: Message text (Swift Messages) can be used to extract extremely important insights about the data.**

### **Hint: Alert date can also be extracted from Message Text decode it carefully.**

### **Hint: Using the Watch List you can add some detailed insights to your data.**

# What we are looking forward to: -

## Looking for a score/algorithm based or even a PMML model which can help us bring the number of false positive scenarios **by telling us the Alert Status for the validation set.**