The below detection logic is to help determine data requirements for a probabilistic model.  We'll use the [Wolfsberg Principles](http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Credit_Cards_AML_Guidance_(2009).pdf) as a guide.

Detection Logic

1. **Overpayments and Refunds to credit card balances**

* Scenario Description
  + This scenario purports to detect AML risks in which a money launderer may be using dirty money to overpay credit card balance and get a refund of clean money from the credit card issuer.
  + Overpayment = (Payment made) > (Payment Owed)

In the example below, there are two overpayments that resulted in negative balance that’d be refunded to the customer (e.g. in 90 days).

|  |  |  |  |
| --- | --- | --- | --- |
| **Transaction Date** | **Transaction Type** | **Transaction Amount ($)** | **Credit Card Balance** |
| 1/1/15 | Purchase | 100 | 100 |
| 1/15/15 | Purchase | 100 | 200 |
| 1/23/15 | Purchase | 100 | 300 |
| **1/31/15** | **Payment** | **-600** | **-300 (to be refunded to customer)** |
| 2/10/15 | Purchase | 100 | -200 |
| 2/19/15 | Purchase | 200 | 0 |
| 2/25/15 | Purchase | 300 | 300 |
| **2/28/15** | **Payment** | **-700** | **-400 (to be refunded to customer)** |

* Threshold for Overpayment
  + **Red** where # of overpayments is 70% or greater in the # of months in the time period covered by the transaction data (e.g. 7 overpayments in a 10-month period)
  + **Yellow** where # of overpayments is between 30% and 70%.
  + **Green** where # of overpayments is below 30%.
* Threshold for Refunds
  + **Red** where # of Refunds is 50% or greater in the # of months in the time period covered by the transaction data (e.g. 5 refunds in a 10-month period)
  + **Yellow** where # of overpayments is between 25% and 50%.
  + **Green** where # of overpayments is below 25%.

1. **Method of payment to card balances**

* Scenario Description
  + This scenario purports to detect AML risks in which a money launder may be using money from hard-to-trace source to pay off credit card balance.
  + Categorize the credit payments by the payment methods and look for unusual patterns, e.g. consistent or large usage of ACH by a domestic customer to pay off the credit card
  + The following fields should be part of transaction data schema.

|  |  |
| --- | --- |
| **Transaction Type** | **Credit\_Debit\_Flag** |
| Payment | C (Credit) |
| Refund | C |
| Reversal | C |
| Award | C |
| Purchase | D (Debit) |
| Fee | D |
| Interest charge | D |
| Penalty | D |
| … | … |
| **Payment Method** |
| Cash |
| Wire |
| ACH |
| Paper Check |
| e-Check |
| Online Transfer |
| Payment at ATM |
| … |

* + Threshold
    - **Red** where # of payments by Cash, Wire or ACH is 50% or greater in the # of months in the time period covered by the transaction data (e.g. 5 of such payments in a 10-month period)
    - **Yellow** where # of such payments is between 30% and 50%.
    - **Green** where # of such payments is below 30%.

1. **Payment source is owned by non-account holder**
   * Scenario Description
     + This scenario purports to detect AML risks in which a money launder may be using dirty money to pay off credit cards owned by other people

|  |  |  |
| --- | --- | --- |
| **Payment Method** | **Payment Source Account ID** | **Payment Source Owner** |
| Cash | N/A | N/A |
| Wire | Wire sender’s (i.e. the payer) Bank Account Number | Name of the Sender / Payer |
| ACH | Wire sender’s (i.e. the payer) Bank Account Number | Name of the Sender / Payer |
| Paper Check | Bank Account Number on the paper check | Owner of the account on the paper check |
| e-Check | Bank Account Number on the e-check | Owner of the account on the e-check |
| Online Banking Transfer | N/A (Assumption is the online banking transfer is allowed only between accounts owned by the same customer) | N/A |
| ATM payment | N/A (Assumption is the credit card payment at an ATM is allowed only between accounts owned by the same customer) | N/A |
| … |  |  |

* + Threshold
    - **Red** where # of payments by non-account-holder is 40% or greater in the # of months in the time period covered by the transaction data (e.g. 4 of such payments in a 10-month period)
    - **Yellow** where # of such payments is between 25% and 40%.
    - **Green** where # of such payments is below 25%.

1. **Payment is frequently made at a location that is materially distant from the account address** 
   * Scenario Description
     + This scenario purports to detect AML risks in which a money launder may be using other people at various locations to pay off credit card
     + Payment method includes cash and ATM payment.
     + This will require the following data elements:
       - Payment location / address
       - Address of record associated with the Credit Card account
       - Distance (in miles) between payment location and account address.
   * Threshold
     + “Materially distant” is defined as payment location being more than 100 miles away from the account address
     + **Red** where # of payments at non-account-address is more than 50% or greater in the # of months in the time period covered by the transaction data (e.g. 5 of such payments in a 10-month period)
     + **Yellow** where # of such payments is between 30% and 50%.
     + **Green** where # of such payments is below 30%.
2. **Frequent or large transactions at high-risk countries** 
   * Scenario Description
     + This scenario purports to detect AML risks associated with frequent or large credit card transactions at high-risk countries Payment method includes cash and ATM payment.
     + ‘High Risk’ countries are defined as ‘CURRENT\_US\_COUNTRY\_RISK\_RATING’ of 4 or 5 in the CRR table, for example:

select distinct COUNTRY\_NAME,current\_us\_country\_risk\_rating

from IDP\_PRD\_INTERFACE.USPC.V\_L3\_HRA\_US\_AML\_COUNTRY\_RISK\_RATING

where current\_us\_country\_risk\_rating>3

order by country\_name

* + Threshold
    - **Red** where
      * # of transactions at high-risk countries is 45% or greater against the total # of transactions in the same time period
      * $ value of transactions at high-risk countries is 45% or greater against the total $ value of transactions in the same time period
    - **Yellow** where number (or $ value) of transactions at high-risk countries is between 30% and 45% of the total number (or $ value) of transactions in the same time period
    - **Green** where number (or $ value) of transactions at high-risk countries is below 30% of the total number (or $ value) of transactions in the same time period

1. **Unusual ATM withdrawals for cash advance**
   * Scenario Description
     + This scenario purports to detect AML risks associated with unusual pattern of credit card cash advance withdrawals at an ATM
     + This will require the following data elements:
       - ATM location and address
       - Credit card cash advance date/time and amount
       - Account holder address
       - Distance between the ATM location and the Account holder address
   * Threshold
     + **Red** where
       - # of cash advances is 20% or greater against the total # of all credit card transactions in the same time period, or
       - $ value of cash advances is 20% or greater against the total $ value of all credit card transactions in the same time period
     + **Yellow** where
       - # of cash advances is between 10% and 20% against the total # of all credit card transactions in the same time period
     + **Green** where
       - # of cash advances is below 10% against the total # of all credit card transactions in the same time period
2. **Frequent Credit Card transactions at locations “materially distant” from the account address** 
   * Scenario Description
     + This scenario purports to detect AML risks in which a money launder may be having other people at various locations to use the same credit card
     + Transaction types include ATM cash advances and POS transactions
     + This will require the following data elements:
       - Transaction location / address
       - If ATM or POS transaction, location and address of the ATM / POS
       - Address of record associated with the Credit Card account
       - Distance (in miles) between transaction location and account address.
     + “Materially distant” is defined as payment location being more than 100 miles away from the account address
   * Threshold
     + **Red** where
       - 50% or more of the number (or the $ value) of transactions are at a location that is “materially distant” (see #4 scenario) from the account location, or
       - There are multiple transactions at locations 200 miles or greater within an hour.
     + **Yellow** where
       - Between 30% and 50% or more of the number (or the $ value) of transactions are at a location that is “materially distant” (see #4 scenario) from the account location
     + **Green** where
       - Less than 30% of the number (or the $ value) of transactions are at a location that is “materially distant” (see #4 scenario) from the account location
3. **Merchant credits without offsetting merchant transactions**
   * Scenario Description
     + This scenario purports to detect AML risks in which merchant credits are applied to credit card without the matching (or offsetting) merchant transaction
     + This will require the following data elements:
       - Merchant name and address (and unique ID if available)
       - Transaction type is available to identify refund or reversal or merchant credit
   * Threshold
     + **Red** where
       - Three or more Merchant credits without offsetting merchant transactions in a given month
     + **Yellow** where
       - One or two Merchant credits without offsetting merchant transactions in a given month
     + **Green** where
       - Zero Merchant credits without offsetting merchant transactions in a given month
4. **Hotel room rentals at different hotels over the same time period**
   * Scenario Description
     + This scenario purports to detect AML risks in which hotel rooms were rented in different hotels in the same time period
     + This will require the following data elements:
       - Credit card transaction information has details about the hotel stay, including hotel name and address, and dates of hotel stays
       - If hotel stays were pre-paid, transaction details should include the actual dates of hotel stays that are pre-paid
       - If available, the merchant credits or refunds for pre-paid hotel stays (e.g. dirty money can potentially be used to prepay for hotel stays, then later cancel the stays for clean-money refunds)
   * Threshold
     + **Red** where
       - Two or more simultaneous (or overlapping) stays in different hotels, or
       - Two or more pre-paid hotel stays that were subsequently refunded, or
       - Refund for pre-paid hotel stays without the offsetting pre-paid hotel stays (see #8 scenario)
     + **Yellow** where
       - One simultaneous (or overlapping) stay in different hotels, or
       - One pre-paid hotel stays that were subsequently refunded
   * **Green** where
     + - Zero simultaneous (or overlapping) stay in different hotels, and
       - Zero pre-paid hotel stays that were subsequently refunded
5. **Multiple airline tickets for non-account holders**
   * Scenario Description
     + This scenario purports to detect AML risks in which multiple airline tickets were purchased for non-account holders
     + This will require the following data elements:
       - Credit card transaction information has details about the airline ticket purchase, including the date of purchase, name of passenger(s), from/to itinerary, and dates of travel
   * Threshold
     + **Red** where
       - Four or more purchases of such airline tickets in a given month, or
       - Any refund (or merchant credit) of such purchases without the offsetting transaction
     + **Yellow** where
       - Two or three purchases of such airline tickets in a given month
     + **Green** where
       - One or less purchases of such airline tickets in a given month
6. **Unusually large payments for accumulated balance**
   * Scenario Description
     + This scenario purports to detect AML risks in which unusually large payments are made for accumulated balance
     + This will require the following data elements:
       - History of credit card balance by month
       - History of credit card payments by month
   * Threshold
     + **Red** where
       - Payment amount is two standard deviation (sigma) or more away from the mean of payments over the preceding six months
     + **Yellow** where
       - Payment amount is between one and two standard deviation (sigma) away from the mean of payments over the preceding six months
     + **Green** where
       - Payment amount is less than one standard deviation (sigma) away from the mean of payments over the preceding six months
7. **Out of country** **transactions**
   * Use Case Out of Country – 10: approx. 90% of all transactions are out of country
   * Use Case Out of Country – 40: approx. 60% of all transactions are out of country
   * Use Case Out of Country – 50: approx. 50% of all transactions are out of country
   * Use Case Out of Country – 95: approx. 5% of all transactions are out of country
   * Use Case Out of Country – only US transactions

**Other Scenarios**

* Separate transactions by credit and debit
* See #2 scenario for details on credit / debit transaction types
* Add non-account ids for wires and international ach
* Add locations not on customer balance