



Analytics Offering Through AMLOCK - An Approach Document



Analytics Offering Through AMLOCK

1. Background

3i Infotech has a strong presence in the BFSI sector in India with AMLOCK as one of the leading products. AMLOCK had been sold across verticals within BFSI. Currently, it has around 80 clients across the globe. AMLOCK primarily has banking clients across like India, Sri Lanka, Vietnam, Philippines, Kenya and Oman. In India, the solution has more than 35 clients, largely in the banking sector and also the market leader in India. Some of the largest banks in India have deployed the solution.

The solution has been in the market for more than 13 years now; the same has been upgraded a couple of times. The last version release of AMLOCK was in 2012-13 and 3i Infotech is currently working on the next version AMLOCK.

As a part of the next version release (a major version upgrade and to be completed on a quarterly incremental basis), 3i Infotech has been considering of strengthening of the solution using analytical methods of AML monitoring.

Currently, AMLOCK has largely been a standard rule based solution and, hence, it is felt that there are many opportunities for improvements through analytical angle of AML monitoring. From clients' perspective, analytics aided decision making shall be a welcome move as the KYC and transactional data being handled by them as a part of AML monitoring has been increasing steadily and is becoming increasingly impossible to manage either manually or through simple rule based solutions.

In the above background, 3i Infotech has been considering working with a few leading analytics firms to strengthen the offerings around its AML solution. The details of the same have been described in this document in subsequent chapters.

2. Business Objective

The objective is to increase the AMLOCK business by enhancing AMLOCK with additional offerings, retain the existing customers with new offerings, commanding a higher ticket size and leveraging its strong customer base.

3. AMLOCK - Current Landscape

AMLOCK has around 80 clients across the globe and had been sold across verticals within BFSI. The current landscape of the product shall be as under:

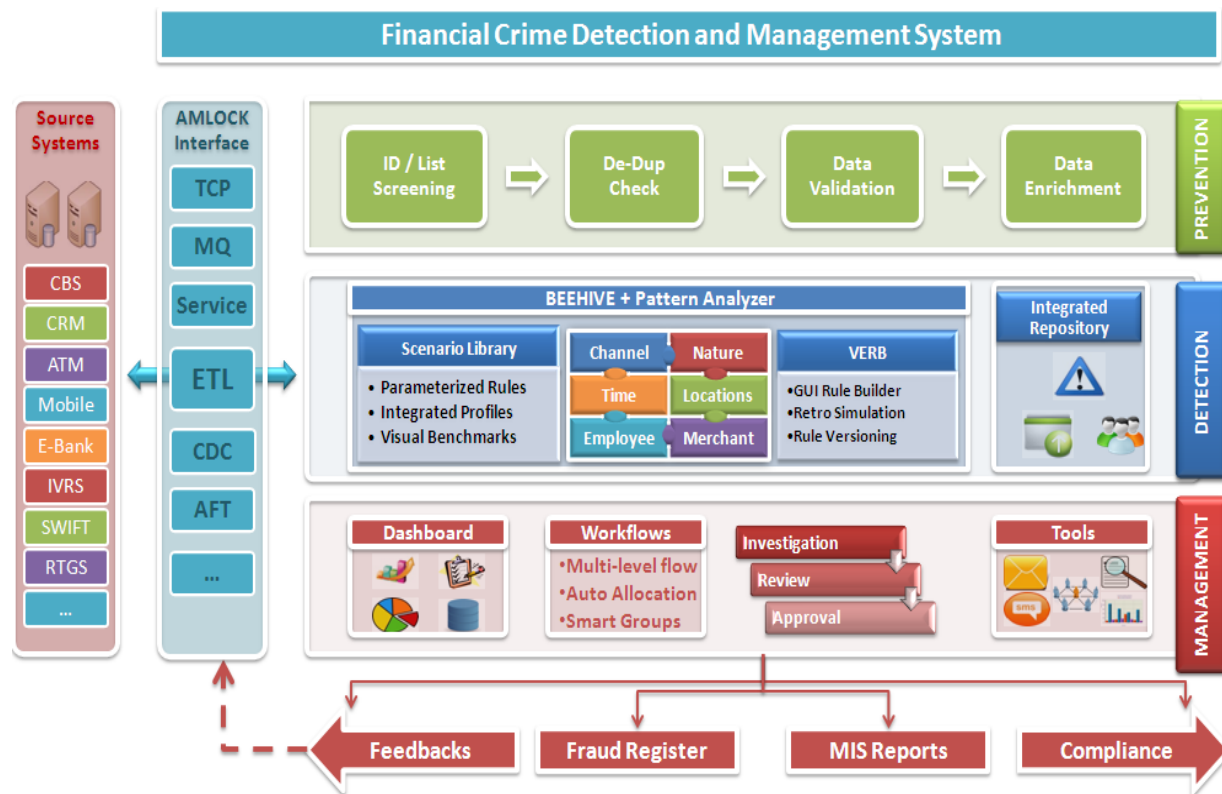
Geo Segment /	Banking	Telecom	Others
SAG	40	2	1
APAC	12		

MEA	16		
Others	4	1	2

4. Current Solution Architecture:

AMLOCK is an integrated Anti Money Laundering and Financial Crime detection and management solution to suit the requirements of Banks and Financial institutions. It encompasses the following components:

- KYC Policies & Procedures (includes List Screening and Manage Customer Profiles – Risk Categories)
- Monitor Transactions: Setting Threshold Limits, Identify Suspicious Activity based on deviation from base profile, Behavioral Analysis
- Integrated Workflow for easy investigation
- Reporting



5. Analytics Offerings

3i Infotech has initiated the discussion in this regard with a few leading analytics firms and shall deploy the following methodology (given below in brief):

- Step 1: Identify the analytics offerings around AMLOCK
- Step 2: Short-list the same from quarterly incremental offerings basis
- Step 3: Prepare the 'use case' for such offerings
- Step 4: Share the 'use case' with the analytics firms (post agreement and other legal documentation etc).
- Step 5: The analytics firm to complete the POC on the offering and share output to 3i Infotech
- Step 6: On verification of successful output, 3i Infotech to market the offerings among its clients (pilot will be done in India only)
- Step 7: In the interim, 3i Infotech and the analytics firm to complete the integration between AMLOCK and the new offering
- Step 8: Carrying out implementation of the offering at the client's place (joint exercise between 3i Infotech and analytics firm); the resource combination to be decided on a case to case basis.

The analytics firm's resources would be required to work in 3i Infotech's premises for the POC owing to customer data confidentiality requirements.

6. Commercial to the arrangement

Commercials would play a part in the below aspects and would be considered as below:

- Technology: Open source tools shall only be deployed.
- AML Solution: 3i Infotech's AML solution AMLOCK shall be used; no fee to be levied by 3i Infotech for the same.
- POC Cost for the analytics firm: to be considered by the analytics firm as a part of its pre-sales budget.
- Marketing Cost: Fully by 3i Infotech (within its Indian clientele).
- Pre-Sales Cost: By 3i Infotech and analytics firm as per the need of the client / prospect.
- Integration Cost: By 3i Infotech and analytics firm as per the need.
- Implementation Cost: The resources needed for implementation shall be decided mutually between 3i Infotech and the analytics firm and the commercial share between them would be considered on the similar lines.
- Training Cost: 3i Infotech would consider AMLOCK solution functionalities training for a period of 2 days every quarter. This will not be billed. Any additional requirement related to the domain shall be supported on need basis.
- The above arrangement includes both resource cost and incidental expenses.

7. Other Aspects

- NDA would be entered into between 3i Infotech and the analytics firm to initiate the initial discussions.

- Subsequently, a teaming agreement would be signed on the above lines (paragraph 6 above).

8. Enclosures:

1. Use case document of the offerings decided for April to June 2016 quarter.

ANNEXURE 1:

USE CASE DOCUMENT:

Offering 1: Alert Risk Scoring

Problem Statement:

The AML system generates alerts based on the alert scenarios deployed. In the rule based simple alert generation process, the number of alerts that will have no AML suspicious activity shall be quite high. Such alerts are called false positives. The AML compliance team would review all the alerts generated and mark the non-suspicious alerts as false positives. The general trend is that on an average 75% of the alerts generated are false positives and is hence quite time consuming.

Objective:

Using analytics, the alerts to be risk scored i.e. the probability of alert getting concluded as an AML suspicious activity (i.e. not a false positive) to facilitate AML compliance team focus on high risk scores (the system can auto-close low risk scored alerts as well).

Output:

Risk scored alerts (on a scale of 1 to 100; 100 being the highest risk / probable AML activity)

Data input:

- 5 types of alert scenarios to be considered
- Sample Alerts Generated for the alert scenarios in 30 days' time
- Sample customer list for analysis: 100
- 6 month customer transaction data
- Static KYC parameters of the sample customers (Branch Master, Transaction Type Master, Products Master, Customer Type Master, Customer Risk Master)
- Past data pertaining to alerts considered as AML suspicious activity

Offering 2: Automated False Positive Analytics

Problem Statement:

The AML system generates alerts based on the alert scenarios deployed. In the rule based simple alert generation process, the number of alerts that will have no AML suspicious activity shall be quite high. Such alerts are called false positives. The AML compliance team would review all the alerts generated and mark the non-suspicious alerts as false positives. The general trend is that on an average 75% of the alerts generated are false positives.

Objective:

An effective and automated false positive management process would facilitate compliance process in a big way.

Output:

- False Positive Model Screen - Lists out all alerts and also the derived false positive combination parameters which have been identified through scanning historical alerts and actions.
- Option to edit the parameters in the False Positive Model Screen to tweak the parameters - add or remove parameters and change conditions.
- AMLOCK to provide option to review / audit the system tagged false positives.

Data input:

- 5 types of alert scenarios to be considered
- Sample Alerts Generated for the alert scenarios in 30 days' time
- Sample customer list for analysis: 100
- 6 month customer transaction data
- Static KYC parameters of the sample customers (Branch Master, Transaction Type Master, Products Master, Customer Type Master, Customer Risk Master)
- Past data pertaining to alerts considered as AML suspicious activity
- Past data marked as false positives

Offering 3: Peer Group Profiling

Problem Statement:

The AML system facilitates AML compliance monitoring across customer segments. However, the AML solutions normally track transactional deviations from the set patterns from individual customer perspective rather than from a customer segment perspective.

Objective:

Deviations of individual customer transactions in line with the customer segment behaviour can be ignored and deviations not in alignment with group behaviour should be reviewed. The same would be facilitated through an effective customer segmentation process (peer group method).

Output:

- Profiling based on location, occupation, income profile, business type and age.
- For each customer group identify base profile - average balance, average frequency (based on customer type), credits, debits, money transfers, no of beneficiaries, no of senders (using statistical tools such as standard deviation, averages, trend, min-max etc).
- In the Case Manager or Customer Profiling screen, create a tab to display the selected customers transaction vs peer profile and highlight deviations for each parameter

Data input:

- Sample customer list for analysis: 1,000
- 6 month customer transaction data
- Static KYC parameters of the sample customers (Branch Master, Transaction Type Master, Products Master, Customer Type Master, Customer Risk Master)
- Past data pertaining to alerts considered as AML suspicious activity