ACAMS® | Advancing Financial Crime Professionals Worldwide®

Trade Based Money Laundering—Capturing the New Frontier through Analytics

Manisha Khanna

CAMS Certified Anti-Money Laundering Specialist®

Table of Contents

Executive Summary 3
Changing Expectations and New Regulatory Guidance 3
Risk Mitigation of Trade Finance Products 5
Challenges in Monitoring Trade Finance Products 6
Red Flags for TBML Monitoring 8
Preparing Data for Effective Screening 10
Analytical Techniques for Detecting TBML Red Flags 14
Framework for Automating TBML Monitoring 19
Systems Audit Considerations for TBML Monitoring 20
Summary and Conclusion 23
References 24

Executive Summary

Trade-based money laundering (TBML) is an extremely different method of laundering criminal proceeds, wherein criminal organizations utilize the trade of goods instead of an actual monetary transaction.

Recent regulatory focus has proven that banks need to play a key role in contributing to policing this method of money laundering, as they are still 'a central house' for all financial transactions pertaining to financing such trading activities. In addition, by nature of their business, banks have access to the complete documentation and profile of their customers as well as the underlying trade and access to the technology to enable an efficient and highly effective monitoring of the laundering activities.

TBML monitoring is a difficult problem for banks to tackle since trade financing, by its very nature, is an extremely document-centric process and there is still a reliance on manual screening which is largely dependent on the document checker's experience. Banks are dealing with corporate customers who are extremely reluctant to share relevant information to enable banks to perform adequate compliance monitoring. In addition, a lot of information is available in an unstructured format and within the SWIFT message body as free text, making the screening difficult for a standard anti-money laundering (AML) monitoring solution, which typically looks for unusual behaviors in structured data. Hence, banks are facing a huge challenge in automating such monitoring activity.

This white paper shall focus on how banks can utilize developments in the data analytics space to automate and increase the effectiveness of their detection of TBML and hence, reduce the risks of coming under regulatory spotlight pertaining to trade finance.

Changing Expectations and New Regulatory Guidance

There has been an increasing pressure from regulatory authorities across the globe to screen trade financing activities for money laundering.

- In the U.K., the Financial Conduct Authority (FCA) released a report [1] which highlighted that banks had not taken adequate measures to mitigate the risk of money laundering and terrorist financing activities in their trade finance business.
- In South East Asia, the Monetary Authority of Singapore (MAS) released a detailed guidance [2] on anti-money laundering/counter-terrorist financing (AML/CTF) controls in trade finance and correspondent banking for financial institutions.
- In its annual banking stability report, the Hong Kong Monetary Authority (HKMA) [3] stated a noticeable increase in mainland-related trade financing activities and requested the internal audit functions of AIs active in this business to conduct a thematic review to verify the adequacy and effectiveness of their risk management and internal controls for TBML monitoring. HKMA also identified trade finance as the main focus for its AML efforts in 2015 [4]. The Hong Kong Association of Banks (HKAB) recently released the Guidance Paper on Combating Trade-Based Money Laundering [5].
- In America, recent enforcement actions by the Office of Foreign Assets Control (OFAC) [6] called out deficiencies in identifying TBML activities.

- The Australia Institute of Criminology (AIC) [7] regarded TBML as arguably a significant concern for a country like Australia that relies heavily on trade and foreign investment.
- Japan is also highlighted as posing a high TBML risk because of the presence of organized crime and its status as a major trading power [7].
- Bank Negara Malaysia (BNM), in its National Risk Assessment [8] also cited that a high volume of international trade makes the country prone to TBML.

In other jurisdictions with high trade volumes, financial institutions have been under similar regulatory pressures to identify trade-related sanctions violations. Figure 1 lists many of the recent regulatory bulletins and pronouncements of significance to TBML compliance.

Figure 1: Regulatory Bulletins on TBML

Recent Regulatory Bulletins & Reports

Office of the Comptroller of the Currency's (OCC) Handbook on Trade Finance and Services [9], released April 2015, stated that noncompliance with AML laws may result in monetary penalties and prevent the bank from collecting on a transaction.

The Monetary Authority of Singapore (MAS) released a detailed guidance on AML/CTF controls in trade finance and correspondent banking for financial institutions [2] in Singapore in October 2015, following its National Risk Assessment report [10] published in January 2014 where the AML/CTF controls for trade finance and correspondent banking areas were identified for improvement.

Hong Kong Association of Banks (HKAB) released a guidance paper on combating TBML [5] on February 1, 2016, with input from the Hong Kong Monetary Authority (HKMA).

Global Financial Integrity's (GFI) report *Illicit Financial Flows from Developing Countries: 2004-2013* [11], released in December 2015, revealed fraudulent misinvoicing of trade transactions to be the largest component of illicit financial flows from developing countries, accounting for 83.4 percent of all illicit flows. It further highlighted that any effort to significantly curtail illicit financial flows must address trade misinvoicing.

The U.S. Department of Treasury's National AML Risk Assessment, 2015 [12] stated that TBML can have a more destructive impact on legitimate commerce than other money laundering schemes.

FinCEN issued an advisory in May 2014 [13] regarding TBML, providing red flag indicators drawn from analysis of suspicious activity reports (SARs) and law enforcement input. This was an update to the 2010 advisory issued by FinCEN, [14] which was issued to inform and assist the financial industry in reporting instances of suspected TBML activities.

FCA's July 2013 report on the bank's control of financial crimes risks in trade finance [1] described how banks in the U.K. control money laundering, terrorist financing and sanctions risks (collectively 'financial crime risks') in trade finance business and provided the findings from their thematic review highlighting significant deficiencies in TBML controls.

APG's report on TBML, July 20, 2012, [15] stated that the lack of TBML investigators and absence of systems capable of cross-referencing trade and trade finance data are significant limitations.

FATF's report on TBML (Paris, June 2006) [16] stated that TBML represents an important channel of criminal activity and, given the growth of world trade, an increasingly important money laundering and terrorist financing vulnerability.

The Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual [17], stated that trade finance activities of banks are subject to AML laws and that the international trade system provides criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection.

Collectively, the regulatory changes are greatly impacting the trade finance business globally, with nonbanking players entering the trade finance market and banks looking for de-risking options in certain geographies and struggling with managing the expectations of their corporate customers. With these key developments and renewed focus across the regulators, law enforcement and financial intelligence

units (FIUs), TBML appears to be the next frontier of enforcement, thus becoming an area of interest for the global banking industry.

Risk Mitigation of Trade Finance Products

Banks need to conduct a comprehensive risk assessment of their trade finance business, taking into account their customer base, geographical locations, products offered and emerging risks. The trade finance money laundering risk assessment could be a part of banks' broader enterprise-wide risk assessment (ERWA) framework [2].

The BSA/AML Examination Manual [17] states the below key factors that increase the risks of money laundering (see Figure 2):

- Involvement of multiple parties in both sides of trade
- More document-centric than other banking activities, susceptible to document fraud
- Over and under valuation of goods
- Collusion between buyers and sellers
- Disguising identity of applicant via use of corporate vehicles such as shell companies, or offshore front companies

Figure 2: Key Factors Increasing Money Laundering Risks for Trade Finance

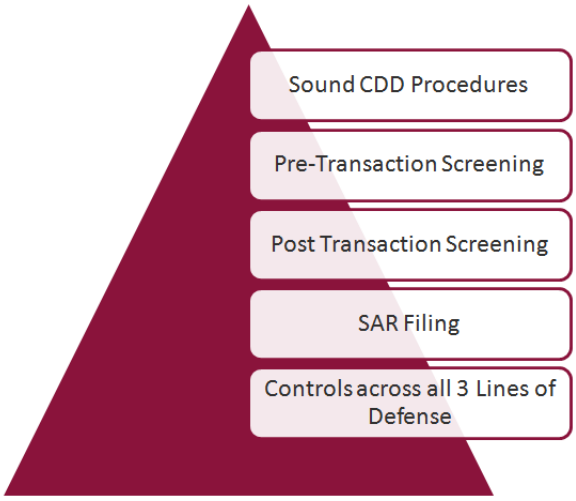
BSA also suggests banks adopt effective money laundering controls for trade finance and proposes the following risk mitigation approaches (see Figure 3):

- Sound customer due diligence (CDD) procedures which should include:
    - Thorough understanding of customers' underlying business
    - Varying degree of due diligence depending on the bank's role in transaction
    - Thorough understanding of trade finance documentation prior to facilitating trade related activity
    - Enhanced due diligence for high-risk jurisdictions
    - Gathering of sufficient information on applicants and beneficiaries including identities, nature of business and source of funding
- Pre- and post-transaction screening should ensure

- Reliability of documentation at every transaction step and based on the role played by the bank
- Review of documentation for anomalies or red flags that could indicate unusual or suspicious activity
- Society for Worldwide Interbank Financial Telecommunication (SWIFT) message monitoring for names of parties with respect to Office of Foreign Assets Control (OFAC) lists
- Banks with a high volume of SWIFT messages to determine if their monitoring efforts are adequate to detect suspicious activity and is commensurate with the size and complexity of the bank's trade finance portfolio—particularly if their monitoring mechanism is not automated

- SAR filings should
  - Include appropriate information to enable the classification of the activity as TBML
  - Include TBML or Black Market Peso Exchange (BMPE) abbreviations in the narrative section of the SAR
  - Have the appropriate box checked in Part II of the SAR report indicating TBML [14]

Figure 3: Risk Mitigation Approaches for Trade Finance Products



Even though BSA has provided a framework for money laundering risk mitigation of trade products, there are concerns with expanding the current AML/CTF monitoring to the trade finance business line by the banks. The next section discusses some of these challenges.

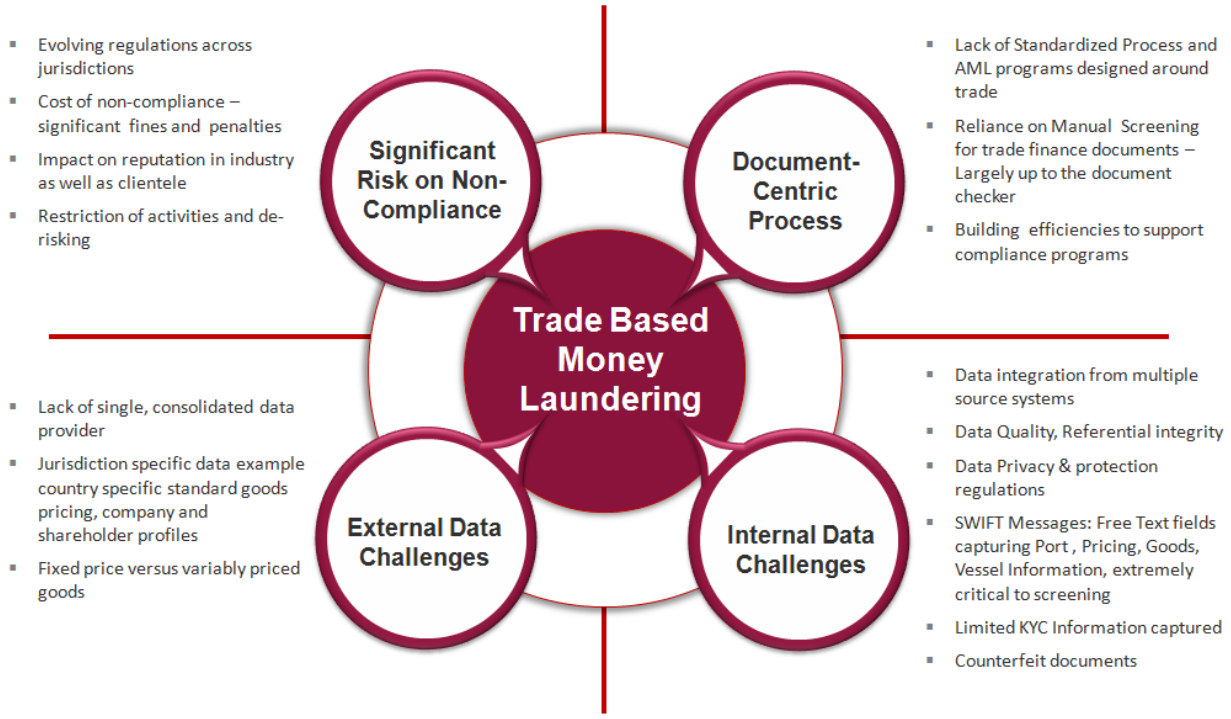
Challenges in Monitoring Trade Finance Products

While the importance of TBML screening and AML risks and vulnerabilities are widely accepted, one of the main concerns banks are facing is a high budgetary, regulatory and operational burden to implement TBML controls. In an article published by the Global Trade Review Magazine [18] it was stated that "Regulatory and compliance issues tend to lead over commercial objectives. Clearly good compliance is

necessary, however the overzealous application tends to add overheads and time to all things associated with financing trade.”

Figure 4 provides a summary of key challenges in TBML monitoring from the bank’s perspective, gathered via individual interviews conducted by the author [19] across various staff from Tier I and Tier II banks engaged in trade finance and related compliance operations.

Figure 4: Challenges in monitoring Trade Finance products



One of the participants in the interview [19] indicated that the general challenges in the automation of TBML monitoring include:

- Lack of specialized and consolidated AML and sanctions monitoring
- Cost of automation
- Limited internal expertise
- Suspected high volume of false positives

Another participant shared that there is a lack of AML programs designed around trade and most programs have to either be built from scratch or redesigned significantly. Their bank is taking a threefold approach to address the heightened regulatory expectation which includes creating specialized FCC teams, targeted AML trainings and systems automation.

Most of the banks indicated dual-use goods and sanctions screening, certain types of vessel checks and SWIFT message screening for AML red flags as their top three priorities for automation, while the screening of hard copy documents is still preferred to be left to manual review.

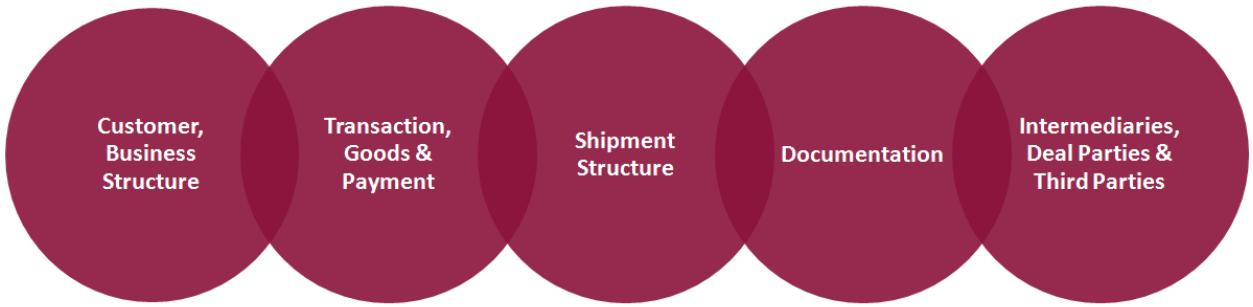
When enquiring about the state of data availability for achieving this automation, most of the banks indicated that the internal data is available in their core transaction processing systems but they lack a single consolidated data provider for external data across jurisdictions and customer base they deal in, including but not limited to dual-use goods list, real-time vessel information, company shareholders and business information, etc. In addition, the quality of data and the effectiveness of such a screening process was questioned as most of the critical data required for screening is either captured in a nonstandardized format or is available as a free text within SWIFT messages.

Given these challenges, most banks are enhancing their controls and introducing further manual checks for trade finance screening. At the same time initiatives are in progress to explore automation of such activities to enable operational efficiencies which directly translate to customer experience as well as repeatability and auditability of such a process. Responding to this global change and to the challenges faced by their clients, one of the market leading banks stated that it has invested ahead of time to ensure that it can meet regulations on financial crime [20].

Red Flags for TBML Monitoring

Below are some of the red flag checks (excerpt from [15] and [2]) of potential TBML activity which banks can potentially look for introducing in their pre- and post-transaction screening processes classified by various areas requiring scrutiny (see Figure 5).

Figure 5: Classification of TBML Red Flags



Business structure:

- The type of item being shipped is not in line with the exporter's or importer's regular business activities, e.g., manufacturer of toys exporting IT equipment
- The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities (e.g., a third of the turnover)
- Customers conducting business in high-risk jurisdictions

- Customers in high-risk activities, including those subject to export/import restrictions such as weapons, chemicals, metals, gems, crude oil

Transaction, goods and payments structure:

- Transaction structure appears unnecessarily complex to obscure the transaction's true nature, (e.g., the use of multiple intermediaries/parties or shipment locations)
- Goods do not comply with applicable import or export regulations, or involve dual-use and high-risk goods
- Obvious over or under pricing of goods and services relative to fair market value, example gold jewelry at $500 an ounce when the market value is at $950 per ounce
- Deal involves receipt of cash (or other payments) from third-party entities that have no apparent connection with the transaction
- Frequent amendments to LCs without a reasonable justification; or that include changes to the beneficiary or location of payment
- LCs are routinely cancelled or utilized
- Method of payment inconsistent with risks (e.g., advance payment for a new supplier in a high-risk country
- Multiple or double invoicing
- Obvious misrepresentation of quantity or type of goods imported or exported
- Unusual trigger point of LC payments (e.g., before goods are shipped without documentation)

Shipment structure:

- Shipping which uses small Non-Vessel Operating Common Carrier (NVOCC) with the potential of collusion, or high-risk/sanctioned vessels
- Shipping via high-risk or transshipment jurisdictions or unconnected subsidiaries
- Shipment by firms/individuals from foreign countries other than city of exporter
- Shipment that does not make economic sense (e.g.,, the use of a 40-foot container to transport a small amount of relatively low-value goods)
- Mismatch in port of loading with vessel location check
- Shipment locations or description of goods that are not consistent with LC

Documentation:

- Packaging inconsistent with commodity or shipping method
- Difficulty in determining the ultimate consignee (recipient) (i.e., via agent)
- Shows a higher/lower value or cost than declared to customs or paid by the importer
- Significant discrepancies between the descriptions of the goods on BL, invoice, or other documents (i.e., certificate of origin, packaging list, etc.)
- Significant discrepancies between the actual goods shipped and the descriptions of the goods on the BL and/or invoice (can only know through inspections)
- Common red flags for LC fraud including incorrect use of banking terms, spelling mistakes and errors in grammar and composition

Intermediaries/deal parties/third party:

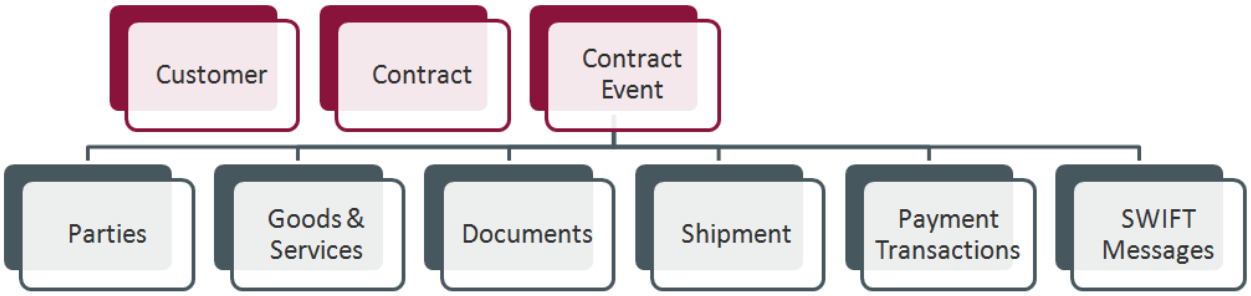
- Transactions from unrelated parties in high-risk jurisdictions
- Transactions involving third parties which are highlighted during sanctions screening as having unacceptably high risk
- Negative news on parties
- A transaction that involves front (or shell companies)
- Connected applicant/beneficiary (e.g., beneficial ownership, signers, shell companies, common shareholders, etc.)
- Originators and recipients of payments have ties to high-risk countries

Preparing Data for Effective Screening

Effective screening of the identified red flags requires accurate data preparation as one of the first steps. As the volume, variety and quality of data can vary based on the operational processes as well as the level of automation within an organization, it is highly important to conduct an assessment of availability and quality of data. Such an assessment typically requires partnership with the business owners of the systems and processes, as well as the relevant IT teams supporting these systems.

A closer look at red flags and their perceived detection logic can help firms arrive at detailed data requirements for screening. Below is a nonexhaustive list of typical data streams which shall be required for screening TBML red flags (see Figure 6):

Figure 6: Data Requirements for TBML Screening



- **Customer**: Names, addresses, countries, company registration and other details, data on key executives, stakeholders, beneficial owners.
- **Contract**: Type of trade finance contract (that is, letter of credit, guarantee, shipping guarantee and reimbursement); relationships to other trade finance contracts.
- **Contract event**: Various life cycle events of a trade finance contract depending on the contract type, such as issuance of a contract, amendments to a contract, or cancellation of a contract.
- **Contract parties**: Parties associated to a specific event of a trade finance contract, with details of any amendment throughout the contract life cycle. Critical party details include internal and external party identifiers, name, location, role on the trade finance contract, relationships to internal and external parties and addresses. External parties can include shipping company, insurance company, or company involved as a trade finance broker, etc.

- **Contract goods and services**: Details of the individual good(s) or service(s) involved during a specific life cycle event of the contract, information on goods pricing, weights, etc.
- **Contract documents**: Details of the documents involved during a specific life cycle event of the contract.
- **Shipment**: Shipment locations, shipping vessel number/identifier.
- **Payment transactions**: Invoice details, payment details, payee information.
- **SWIFT messages**: SWIFT messages associated to the contract. Some of the critical SWIFT messages are MT103/202, MT130/23, MT700/701, MT710/711, MT400, etc.

The screening data needs to be captured for various types of trade finance products offered (such as import/export letter of credit, guarantee and import/export documentary collection) across various life cycle events (such as issuance/booking, amendments, cancellations, closure, etc).

In addition, some of the external data which can be useful for screening purposes include:

- High-risk goods including dual-use goods lists
- Vessel information, including real-time information of the vessel's location and a high-risk vessel list
- Company information, including the company business profile and shareholder information
- Information about contract parties, including the business profile and shareholder information
- High-risk country list, including tax haven countries, NCCT countries and free trade zones
- Standardized goods pricing information
- Negative news on contract parties
- Sanctions lists

Screening against data that is not fit for purpose can increase the screening time, reduce accuracy and increase risks and costs. Figure 7 demonstrates a sample of an MT700 SWIFT message with some key fields (see highlighted text) which are required to be screened.

Figure 7: Sample SWIFT Message Having Poor Data Quality

MT700
----------Instance Type and Transmission----------
Original Received from Application - Outgoing Draft
Priority/Delivery : Normal
----------Message Header----------
Swift Input : FIN 700 Issue of a Documentary Credit
Sender Swift address : AGRIFRPPXXX
BANK ABC, 39th Street, Paris, France
Receiver Swift address : CITIUS32XXX
BANK XYZ CITIUS32, New York, NY 10043
----------User Header----------
Message-User-Reference : 002MSOG1206801JH
----------Message Text----------
:27: Sequence of Total
1/1
:40A: Form of Documentary Credit
IRREVOCABLE
:20: Documentary Credit Number
002IL02120680001
:31C: Date of Issue
120308
:40E: Applicable Rules
UCP LATEST VERSION
:31D: Date and Place of Expiry
120315PARIS
:50: Applicant
BOL INTERNATIONALES SA, 87 RUE DE PARIS
PARC ORSAY, BATIMENT SEQUOIA, BP7, 91402 ORSAY CED X
:59: Beneficiary
STAR INTERNATIONL, 19, 5TH STREET, CHARLESTON ROAD,
MOUNTAIN VIEW
:32B: Currency Code, Amount
USD3000000,
:39A: Percentage Credit Amount Tolerance
10/10
:41A: Available With ... By ...
CITIUS32 BY PAYMENT
:43P: Partial Shipments
ALLOWED
:43T: Transshipment
ALLOWED
:44A: Place of Taking in Charge/Dispatch from .../Place of Receipt
FLORIDA
:44E: Port of Loading/Airport of Departure
SIDNEY, AUSTRALIA
:44F: Port of Discharge/Airport of Destination
GOERGE TOWN
:44B: Place of Final Destination/For Transportation to .../Place of Delivery
PARIS
:44C: Latest Date of Shipment
120310
:45A: Description of Goods and/or Services
FURNITURE AND RAW METRIAL /INCO TERM/ CIF:COST, INSURANCE AND FREIGHT
(NAMED DESTINATION PORT) TRADE TERMS : CIF PARIS
CONTAINS - Office Furniture including Metal Framed Seating, Bedside Chairs, Bariatric
Seating, Oversize Seating and raw materials - hardwood plywood, glass, P2O5,
fluorophosphate glass, zirconium fluoride
:46A: Documents Required
2COPY(S) PACKING LIST
BENIFICIARY'S PACKING LIST INDICATING THE DETAILS OF THE MATERIALS SHIPPED AS
MENTIONED UNDER THE CONTRACT
+2COPY(S) INVOICE
SIGNED COMMERCIAL INVOICE IN TWO COPIES INDICATING THIS CREDIT NUMBER
+1/2 ORIGINAL(S) AND 2 COPY(S) SEAWAY DOCUMENTS
COPY OF FAX/TELEX ADVISING APPLICANT PARTICULARS OF SHIPMENT INCLUDING B/L
NO., DATE, VESSEL NAME, NATIONALITY, PORT OF LOADING AND DISCHARGE,
SHIPMENT DATE WITHIN FIVE WORKING DAYS AFTER SHIPMENT DATE
+1/2 ORIGINAL(S) AND 2 COPY(S) AIRWAY DOCUMENTS
CLEAN AIRWAY BILL CONSIGNED TO THE APPLICANT, NOTIFY
APPLICANT MARKED F73, INDICATING THIS CREDIT NUMBER
:48: Period for Presentation
5
:49: Confirmation Instructions
WITHOUT
:78: Instructions to the Paying/Accepting/Negotiating Bank
+PLEASE FORWARD ALL DOCUMENTS TO US BY COURIER SERVICES IN ONE LOT.
+ON RECEIPT OF DOCUMENTS COMPLYING PRESENTATION, WE SHALL REMIT THE
PROCEEDS IN ACCORDANCE WITH THE INSTRUCTIONS OF THE
NEGOTIATING/PRESENTING BANK.

Some of the data quality issues identified in this sample is explained below.

1. **Multiple information stored in a single field**: Field 50: Applicant and Field 59: Beneficiary include the applicant and beneficiary name as well as addresses as free text information. Applicant and beneficiary names are required to be screened for sanctioned entities and the address information can potentially be used to screen for dealings with high-risk countries and tax havens.
2. **Poor spelling on name and address information**: A typing error such as 'STAR International' spelled as 'STAR International' in Field 59 can result in a poor screening result and requires standardization.
3. **Poorly fielded address information**: Common issues include postal/zip codes and counties/states that are entered in generic address lines rather than in dedicated fields as shown in Fields 50 and 59. The fields only indicate a city name instead of the country, leading to a need of standardizing the address information prior to screening.
4. **Ambiguity in port Information**: Port information is another critical field which can be monitored to screen and identify the red flag if any of the shipment locations is from a high-risk/sanctioned country or tax haven. Some issues in this information include a misspelled port name such as

'Sydney' spelled as 'Sidney' in Field 44E: Port of Loading, leading to ambiguity in the identification of whether the port is in Australia or the town of Sidney in Canada. Such an ambiguity can be resolved by using the contextual information. For instance, "Australia" is mentioned in Field 44E with a reasonable probability. However, in another example Field 44F: Port of Discharge, states the port as "George Town," which can be the Port of George Town in Australia, or the city of George Town in Malaysia, or even Georgetown in Washington D.C. Such cases would perhaps require manual intervention for reaching a decision and should be flagged out as an exception. Further enrichment can be considered using third-party data sources, such as world cities and port databases.

5. **Free text description of goods and services**: Field 45A: Description of Goods and Services, is another field which can potentially trigger red flags pertaining to high-risk goods, over and under invoicing, etc. In Field 45A, the goods being shipped are furniture and related raw materials, which seems to be the business STAR International is dealing in. However, there is appearance of dual-use goods such as fluorophosphate glass and zirconium fluoride matching with European Union (EU) Dual-Use Goods List Item# 6C004.e; and a chemical compound P2O5 which indicates phosphate glass also matching with EU Dual-Use Goods List Item #6C004.e. Such issue with nonstandardized information appearing as free text makes the screening automation hard to achieve and requires free text parsing, recognition and standardization capabilities.

While the above example only shows data issues in a sample SWIFT message, such issues can also exist in the operational data captured by IT systems, or available in hard copy documents. Similarly, external data sourced from multiple providers can be in different formats and requires consolidation and optimization prior to screening. For example, country information, list of cities, towns, seaports, airports, etc., might be obtained from different sources and require consolidation and standardization so that it can provide a better match accuracy when addresses and shipment locations are screened.

In addition, many organizations with a global footprint hold their data in international language scripts which may pose a problem in the screening process. Extensive profiling and auditing of the data quality ahead of screening is therefore crucial.

Once the data assessment is complete, the next step is to standardize, parse and enhance this data to enable effective screening. Furthermore, a continuous governance of data quality is essential to ensure effectiveness of the screening process. Figure 8 proposes a five-step data governance framework for acquiring and improvising the screening data:

Figure 8: 5-Step Data Governance Framework

- **Step 1- Identify**: Identify the red flags and corresponding key fields required for automating the AML rules to generate alerts.
- **Step 2- Source**: Identify the source for retrieving or deriving these key fields from internal applications, transactions, SWIFT messages, documents and data sources from across and beyond the enterprise.
- **Step 3- Assess**: Assess data quality, retrieve, normalize, parse and consolidate trade finance data from various sources.
- **Step 4- Enhance**: Enhance completeness, accuracy and consistency of trade finance data along with functionality to minimize false positive alerts. Consider aspects such as standardization, removal of duplicates, parsing of free text, enrichment, handling multiple languages and scripts, etc.
- **Step 5- Monitor**: Apply case management tools to monitor and resolve any data quality exceptions arising in the screening process.

Once the data is available in its best form, the next step is to analyze this data for potential red flags and insights.

Analytical Techniques for Detecting TBML Red Flags

Financial firms can leverage a host of analytical techniques, both for identification of TBML red flags, as well as for investigative analytics once such red flags are identified in the customer, contract or transaction information. Some of these key analytical techniques and their potential application areas are explained below:

1. **Text analytics**: Text analytics or text mining refers to the process of deriving high quality information from free form text [21]. Text mining utilizes a set of natural language processing, statistical and machine learning techniques that model and structure the information content from textual sources for the purpose of finding insight. Some of the useful application areas of text mining in TBML context are as follows:
    - **Information retrieval** or identification of a corpus (large and structured set of texts) is the first preparatory step which can help identify relevant keywords from free text data. The source of such text can be information retrieved from SWIFT messages, operational systems or hard copy documents.
    - **Pattern-based entity recognition**: Features such as country codes, telephone numbers, email addresses, quantities, units, goods pricing, currency, etc., can be extracted by searching for predefined metadata, regular expressions and patterns from the free text data.
    - The information retrieval can further be supplemented with **Optical Character Recognition (OCR)** technology to enable digitization of scanned/faxed images and for facilitating mandatory data elements (applicant, beneficiary, vessel, ship from/to locations, etc) to be auto-captured.
    - Furthermore, advanced statistical methods and **natural language processing** techniques such as tagging, parsing, de-noising, de-duplicating, transliterating and translating can be applied on the retrieved data to enhance the data quality.

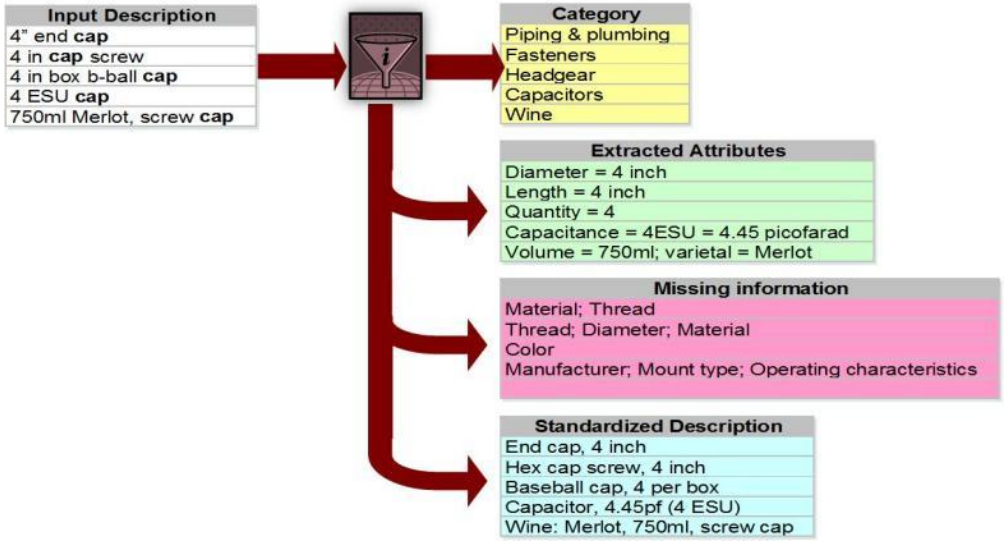
- Named entity or **semantic recognition** can be used to identify named text features such as people, organizations, place/port names and so on. This can also include disambiguation, i.e., the use of contextual clues in the recognition process which may be required to decide where, for instance, "Sidney" is referring to 'Sydney' in Australia or town of Sidney in Canada.
- **Fuzzy matching** can be used to find correspondences between segments of texts. This technique can be used for applications such as dual-use goods matching, sanctions screening of party and vessel names.

Figure 9 shows some of the sample goods descriptions appearing in the contract in a nonstandardized format and a step-by-step application of text mining techniques to derive a standardized description. Text mining techniques used in this example are:

- Information retrieval (keyword Merlot identified using a product metadata reference list)
- Semantic recognition to determine the product category (750ml Merlot categorized as Wine)
- Transliteration of text (4'' as 4 inch),
- parsing the text and extracting relevant attributes using pattern-based entity recognition (Volume = 750 ml)
- Deriving a standardized description which can be further used for fuzzy matching.

2. **Rule engines**: Red Flags which require checks on **volume, velocity and variance** can be modeled as business rules. Various threshold parameters can be set to define the criterion by which a rule should trigger an alert. Business rules can further be layered with other techniques such as profiling and trend analysis, text analytics, etc., to create scenarios which enable detection of anomalies in behavior. Some of the example red flags which can be implemented using this technique include shipment through a high-risk location, frequent amendments to LCs, large number of cancelled or unutilized LCs and port of loading not provided in LCs, etc.

Figure 9: Standardization of Free Text in SWIFT Message



3. **Profiling and trend analysis**: Data profiling is the process of analyzing an existing data source to provide statistics and summary information about the data [22]. Typical AML systems build and maintain profile information across various dimensions such as customer, account, counterparties, transaction types, etc., across various periods of time, such as daily, weekly, monthly and yearly. Some of the profiles which can be useful for analysis of TBML red flags are:

    - Distribution of goods typically imported/exported by industry code
    - Distribution of goods typically imported/exported by a customer
    - Number of shipments via high-risk countries/tax havens by a customer over a time period
    - Distribution (average, peak, min, max) of goods unit pricing by the originating country

    This profile information—once constructed using historical databases and periodically updated based on new transactions—can then be used to conduct trend analysis to determine a change in behavior of a customer in goods and locations they deal in; and/or to detect potential deviation from usual goods pricing information (over invoicing/under invoicing).

4. **Sequence mining:** Sequential pattern mining is a topic of data mining concerned with finding statistically relevant patterns between data examples where the values are delivered in a sequence [23]. Multiple shipment requests from a customer can be checked to see if he/she is using a sequential number of containers potentially indicating a fraudulent/nonexistent container. Another application area is the validation of the container number provided by the customer using the shipping company's numbering and sequence generation algorithm. For example, the International Maritime Organization (IMO) number consists of the letters "IMO" followed by a unique, seven-digit number ("NNNNNNN," where N is a single-digit number, e.g., "1234567"). The integrity of an IMO number can be verified by its check digit, which is the rightmost digit. This is done by multiplying each of the leftmost six digits by a factor corresponding to their position from right to left and adding those products together. The rightmost digit of this sum is the check digit. For example, for IMO 7654329: 7×7 + 6×6 + 5×5 + 4×4 + 3×3 + 2×2 + 9x9 = 220 [24].

5. **Link analysis**: Link analysis is a technique to discover and analyze relationships across two or more entities to derive a network [25]. A link analysis technique can be used to identify hidden relationships across various contract parties and ports and between other participants (beneficial owners, signers, common shareholders) in the trade lifecycle. Through network analysis, a pattern of trade between specific parties displaying various dubious names and characteristics can be identified to flag shell companies or individuals colluding to launder money. Network visualization can then be used to graphically visualize the relationships to ease investigation.

Figure 10: Sample Network Indicating Potential TBML

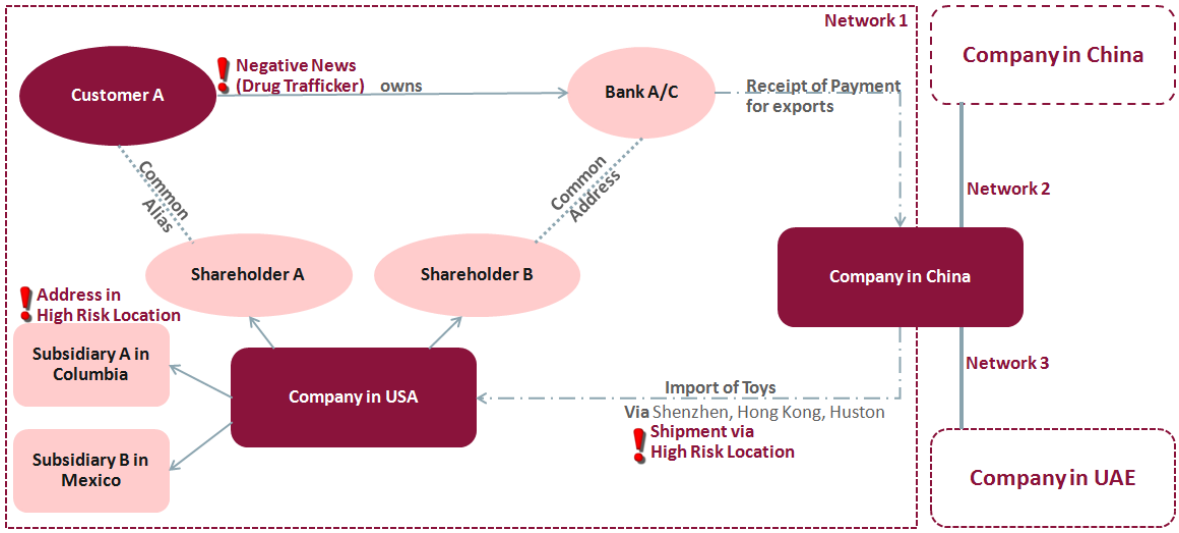


Figure 10 shows an import LC transaction financed by the bank for a company in the U.S. who is importing toys from a company in China. The network visualization shows the company's shareholders connected via hidden links (common alias, common address) to the customer making the payment transaction. In addition, other alerts/red flags were identified such as a negative news on Customer A indicating involvement in drug trafficking, U.S. company's subsidiary in a high-risk country and shipment via a high-risk location. The Chinese company is found to have additional business relationships with companies in China and UAE commanding further investigation of the interconnected parties. Similarly, network analysis of the port information can identify trends in specific shipment patterns for specific ship and commodity types by the trade partner to determine outlier activity or activity that occurs in particular suspect areas (e.g., through certain suspicious transshipment ports) [26].

6. **Statistical analytics**: Statistical analysis is the process of quantitatively describing and analyzing the main features in a dataset. Statistical techniques can be used to create mathematical models, which can be applied to help inform better decisions. Some examples of the statistical techniques that can be useful in TBML context are:

    - **Unit price analysis**: Using public information algorithms can detect if unit prices are higher or lower than global and regional benchmarks [27].
    - **Unit weight analysis**: Can be used to detect instances where money launderers are attempting to transfer value by overstating or understating the quantity of goods shipped relative to payments [27].
    - **Interquartile price range analysis**: Interquartile range analysis [28] of goods pricing can be used to benchmark and determine whether a transaction is abnormal. A transaction can be considered overvalued when its price exceeds the upper-quartile price range and undervalued if its price is below the lower-quartile range. This can be combined with profiling techniques to build benchmark data and determine appropriate interquartile ranges on goods pricing segmented across goods types and geographies.

7. **Visual and predictive analytics:** Advanced statistical models (also known as predictive models) can allow anticipating possible future outcomes to take immediate actions in order to make adjustments to impact the future. Not only should banks review the red flags, but they should also proactively try to assess new patterns they might not be aware of. Supervised learning techniques can be used to build predictive models using historic (labeled) alert data to flag customers and transactions with similar features/attributes as previously alerted clusters. In addition, outlier analysis can be used to determine potential over and under invoicing with respect to historic average and peak goods pricing. Unsupervised learning techniques can be utilized for deriving the probability of money laundering being conducted by a customer using techniques such as clustering, neural networks, etc.

   Building predictive models can be supplemented with visual analytics where the data is visually explored and used to determine which predictive model to use to "fit" the data. For example, if the data visually looks linear, then a linear regression technique could be applied. However, if the data plots out logarithmically then a logistic regression technique could be applied. Furthermore, each model/classifier might demonstrate a different level of performance on different subsets/segments of data, suggesting that different classifiers contribute complementary information to the classification and prediction task; they can be combined using decision fusion techniques to increase recognition accuracy [29]. Although doing such complex analyses typically requires teams of experienced statisticians and data scientists, new tools and data visualization technologies have made statistical modeling more accessible to the average business user [30].

8. **Big data discovery**: Big data analytics is the use of analytical techniques against very large, diverse data sets that include different formats such as structured/unstructured, different frequencies such as streaming/batch and different sizes from terabytes to zettabytes. Usually, big data has one or more of the following characteristics—high volume, high velocity, or high variety. With the trade finance business data coming from a variety of internal and external sources and heavily in an unstructured (document-centric) format; big data discovery has a definite role to play; especially for investigative analytics and ad-hoc information discovery to supplement the red flag detection and monitoring capabilities. To enable the big data discovery process, financial firms can start collecting raw data in data lakes from different sources (traditional source system extracts, documents, emails, news, third-party data, etc.). A data lake is a storage repository that holds a vast amount of raw data in its native format without any transformation. Big data discovery tools can then be used to allow transformation of this raw data stored in data lakes into actionable insights. Big data discovery tools typically provide a user interface to allow users to combine data sets, search, navigate and visualize new insights with drag and drop ease; providing an extremely powerful capability to allow investigators to make data driven decisions.

9. **Web analytics**: Web analytics is the measurement, collection, analysis and reporting of web data. Web crawling or spidering software can be used to download relevant web pages matching specific search terms and criterion. TBML monitoring efforts can leverage these tools combined with big data analytics, whenever additional details from the web are needed such as container details and negative news to further enhance investigator's decision making [26].

Framework for Automating TBML Monitoring

Many of the trade finance departments within banks are currently still relying on the manual screening of AML red flags, especially due to the lack of availability of proven technologies as well as cost implications to achieve such automation. These processes are extremely laborious and error prone due to their manual nature. To effectively mitigate TBML risks, financial organizations should consider an automated approach to transaction monitoring [26] and analytics has a definite role to play.

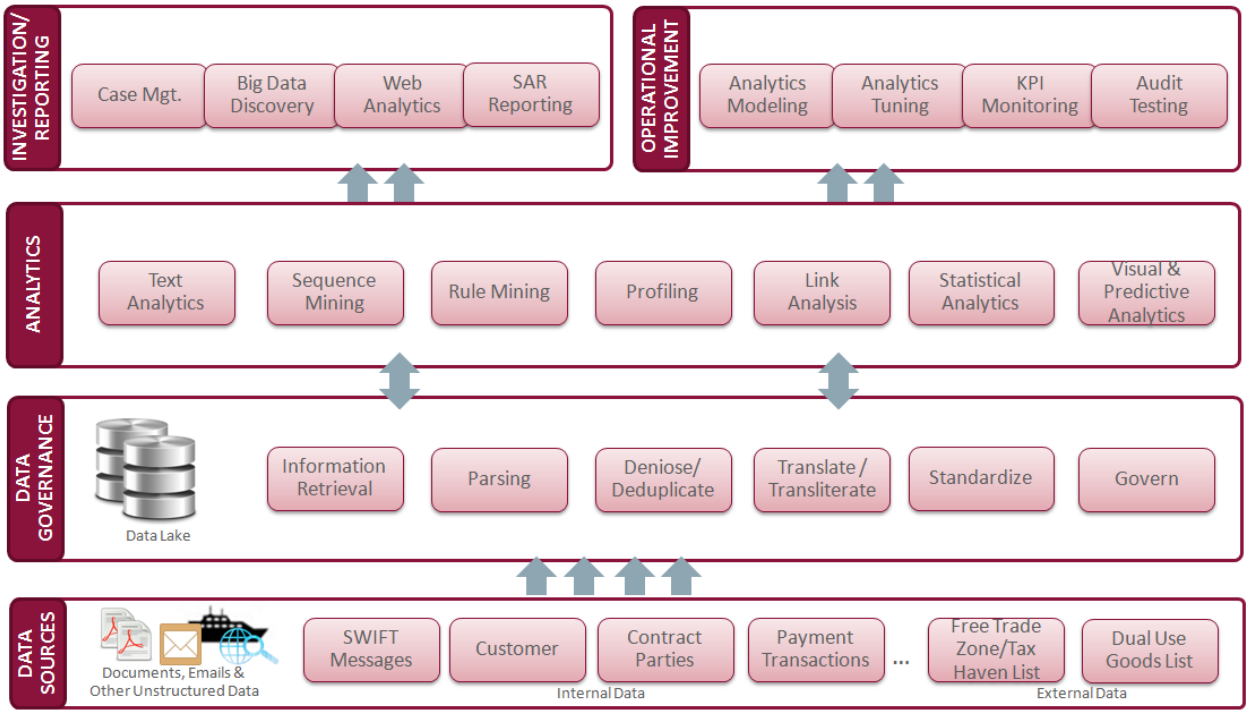
Figure 11 provides reference architecture for TBML monitoring. It includes:

- Collection of data from various sources
- Data quality governance and management
- Automated monitoring of TBML red flags using various analytical techniques
- Enterprise-wide case management
- Investigative analytics
- Management reporting and SAR filing

Wherever possible, such automation shall be supplemented with strong operational processes to capture necessary screening data from internal as well as public data sources and during the KYC process, mitigating manual entry errors and providing an audit log for human decisions.

In addition, it is highly important to establish audit processes to provide ongoing testing, threshold tuning and gap analysis to cover any TBML activities that are seen to be fallen through the cracks. Further details on systems auditing approaches are discussed in the next section. Well designed processes and systems which are easy to use and change can help firms achieve long-term cost effectiveness for satisfying the ever changing regulatory expectations.

Figure 11: Reference Architecture for TBML Monitoring



Systems Audit Considerations for TBML Monitoring

A strong internal audit capability is a critical aspect of the BSA program. Approximately 75 percent of the BSA/AML-related consent orders issued by the OCC since 2010 included articles requiring improvement of the banks' independent testing as defined by the regulators and internal audit function [31]. Verification and audit of automated systems to ensure the effectiveness and efficiency of the detection process is one of the key elements in internal audit performed by the third line of defense.

Figure 12 shows some of the key areas which auditors should look for when auditing the proposed framework for TBML monitoring.

1. **Data availability and quality:** Data validation is a fundamental component of effective AML control auditing. Considerations should be given to areas such as:

    - Data completeness: Verify that the source data reconciles with an independent system of record. For example, the number of transactions in the source system over a period of time reconcile with the number of transactions provided in the control file to the AML monitoring system, the total number of customers match the ones reported in management information report, etc.

Figure 12: TBML Systems Audit Considerations

- Data quality: Verify that elements critical for surveillance are in line with expected data conditions; for example, validate values of applicant, beneficiary, vessel, ship from/to locations for a random sample of records to ensure its captured correctly.
- Referential integrity: Verify that relationships between core data accurately and completely map to referential data; for example, derived country codes in customer addresses match the format and values specified in a high-risk country list.
- Data exception management: Verify how the data exceptions were flagged and handled and if corrected records were re-ingested to the system and re-screened based on updated data.
- SLA checks: Verify if the data was made available to the AML systems in accordance with set SLAs and any late/missing files were handled promptly and appropriately.

2. **Scenario Selection and Implementation:**

- Scenario selection: Ensure that the business has selected and identified appropriate red flags according to the trade finance products offered, jurisdictions and customer risk profiles.
- Scenario review: Verify if there is a process to periodically review the red flags based on changing business and customer portfolio.
- Scenario logic: Review documentation describing the understanding of red flag detection logic and verify if such documentation has been subject to reviews and approvals by senior management. Such information can be found in the project requirement gathering documents, meeting minutes, product specifications, etc.

- Scenario implementation: Ensure that the defined logic was implemented appropriately. This can be done by reviewing if the test cases have appropriate coverage, verifying test data and test execution logs, or even looking at the source code itself to ensure correctness with respect to the defined logic.
- Scenario change management: Review the change management process for scenarios and verify if the scenario logic changes are audited and the test data is enhanced as necessary to reflect each subsequent change.
- Scenario detection results: Test a risk-based sample of trade finance transactions (across various dimensions, such jurisdictions, product types, customer segments) to ensure alerts are flagged as per the expectation from red flags.

3. **Parameters/Threshold Tuning:** The absence of periodic tuning of scenarios often results in numerous false positives, which in turn decreases the investigator productivity and leads to delays in SAR filing. Auditors should ensure that there is a periodic review process and a feedback loop from the alert investigation back into the transaction monitoring system to fine tune the deployed scenarios. Some considerations in scenario tuning audit are:
    - Tuning scope: Verify if the tuning scope considered not just problematic scenarios, but all deployed scenarios.
    - Threshold justification: Review the change management process over thresholds and verify the documentation supporting validity and rationale of the set thresholds.
    - Above/below-the-line threshold testing: Threshold values can be adjusted in a tuning environment and alert generation cycle re-executed to identify near-missed alerts in order to conduct a risk review of having lower/higher threshold values on a sample dataset.

4. **Investigation and Record Keeping:** To validate the effectiveness of the investigation and record keeping process, auditor should consider the following:

    - Investigative data: The quality of investigation is directly dependent on the data and information made available to the investigator. Systems audit should review whether the information available on the investigation screen provided all necessary data points for decision making such as customer profile, transaction history and details, related alerts, information on correlated business entities, related SARs filed, counterparty details, etc. Understand the data gathering process followed by the investigator in cases where this information was not readily available in the investigator user interface.
    - Investigation quality and record keeping: Review a random sample of alerts investigated to check the quality of investigation. Verify if all external information used for decision making such as website searches, ad-hoc analytics results, etc., are appropriately logged in the case management tool. Where possible, conduct interviews to understand the rationale behind human decisions and verify if the SAR and no-SAR decisions were well documented.
    - Investigation SLAs: Verify if the legal deadlines and internal SLAs were observed and changing volume of alerts was effectively managed.
    - Data privacy: Review the system security and access control mechanism to ensure that it is well defined and implemented. Verify the system audit logs for a random set of alerts to evaluate any data privacy breaches.

- Decision approvals: Review the case management tool to ensure that the investigator decisions were subject to appropriate management approvals.

5. **Suspicious Activity Reporting:**

   - SAR quality assurance: Ensure that there is a SAR quality assurance process in place to govern the SAR submissions including a maker-checker approval.
   - SAR quality and timeliness: The BSA/AML Examination Manual - SAR Quality Guidance [32] states that banks must file SARs that are complete, sufficient and timely. Verify a small sample of SARs to ensure SAR narratives were well written and essential information (who, what, when, where, why and how) was provided for the suspicious activity being reported. Verify if the SARs filed included appropriate information to classify the activity as TBML (and verify if TBML or BMPE abbreviations are found in the narrative section of the SAR and that the appropriate box in Part II of the SAR report was checked [14]).

6. **System Usage:** The best IT systems could fail to deliver results if there are no well trained people to use and maintain them. Review if the staff is well trained on the system and if they understand the various tools available at their disposition. Verify system usage guidelines; for example, individual password controls, guidelines for data entry (such as selecting the correct disposition codes while logging decisions in the case management tool, etc.). Verify the training attendance records and conduct interviews to understand and evaluate any system usability challenges.

Internal audit must have a strong understanding and knowledge of BSA/AML processes and money laundering risks of trade products. They should also be able to understand the automated monitoring systems and their potential gaps well enough to be able to design a robust audit framework.

Summary and Conclusion

With the growth of global trade and digitization fueling the next leg up of the trade finance business, the traditional documentary trade business will become more efficient as companies start leveraging technologies such as blockchain, electronic bills of lading and electronic issuance to reduce or even entirely eliminate manual processes. While these developments evolve, it is vital for the banks to establish a strong foundation for mitigating the regulatory compliance risks, which is a combination of processes, controls, sound data model and technologies, so that all relevant transactional data is captured, managed and analyzed to ensure effective monitoring of TBML. Banks have a tough road ahead; however, the collective efforts of banks, regulatory authorities and technological advancements are paving the way to reach a state where effective and largely automated TBML monitoring would be a new normal.

References

[1] Financial Conduct Authority (FCA), *Thematic Review TR13/3 on Banks' control of financial crime risks in trade finance,* https://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf, July 2013.

[2] Monetary Authority of Singapore (MAS), *Guidance on Anti Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking,* http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/Guidance%20on%20AML%20CFT%20Controls%20in%20Trade%20Finance%20and%20Correspondent%20Banking.pdf, October 2015.

[3] Hong Kong Monetary Authority (HKMA), *Annual Banking Stability Report,* http://www.hkma.gov.hk/media/eng/publication-and-research/annual-report/2013/12_Banking_Stability.pdf, 2013.

[4] NewsOnCompliance.com, *HKMA's Anti-Money Laundering Efforts Focus On Trade Finance,* http://newsoncompliance.com/2015/01/hkmas-anti-money-laundering-efforts-focus-on-trade-finance/.

[5] The Hong Kong Association of Banks, *Guidance Paper on Combating Trade-Based Money Laundering,* https://www.hkab.org.hk/download.jsp?isTemp=N&section_id=5&file_name=Guidance+Paper+on+Combating+Trade-based+Money+Laundering+(final).pdf, February 2016.

[6] Department of Treasury, *COMPL-2013-193659 - Settlement Agreement made by and between the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") and BNP Paribas SA ("BNPP"),* https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140630_bnp_settlement.pdf.

[7] Australia Institute of Criminology (AIC), *Trade Based Money Laundering: Risks and Regulatory Responses,* http://www.globalinitiative.net/download/financial-crime/east-asia-oceania/AIC%20-%20Trade-based%20money%20laundering-%20Risks%20and%20regulatory%20responses.pdf.

[8] Bank Negara Malaysia (BNM), *National Risk Assessment Report,* http://amlcft.bnm.gov.my/document/Malaysia_NRA.pdf, 2014.

[9] Office of the Comptroller of the Currency (OCC), *Comptroller's Handbook on Trade Finance and Services,* http://www.occ.treas.gov/publications/publications-by-type/comptrollers-handbook/pub-ch-a-tfs.pdf, April 2015.

[10] Monetary Authority of Singapore (MAS), *Singapore National Money Laundering and Terrorist Financing Risk Assessment Report,* http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Singapore_NRA_Report.pdf, 2013.

[11] Global Financial Integrity (GFI), *Illicit Financial Flows from Developing Countries: 2004-2013,* http://www.gfintegrity.org/report/illicit-financial-flows-from-developing-countries-2004-2013/.

[12] US Department of Treasury, *National Anti Money Laundering Risk Assessment,* Washington DC: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf, 2015.

[13] Financial Crimes Enforcement Network (FinCEN), *Advisory - Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, FIN-2014-A005,* https://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A005.pdf, May 28 2014.

[14] Financial Crimes Enforcement Network (FinCEN), *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering, FIN-2010-A001,* https://www.fincen.gov/statutes_regs/guidance/html/fin-2010-a001.html, February 18, 2010.

[15] Asia/Pacific Group on Money Laundering (APG), *Typology Report on Trade Based Money Laundering,* http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf, July 20, 2012.

[16] Financial Action Task Force (FATF), *Trade Based Money Laundering,* Paris: http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf, June 2006.

[17] Bank Secrecy Act (BSA) , *Anti-Money Laundering Examination Manual – Trade Finance Activities Overview,* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_079.html.

[18] Global Trade Review (GTR), "SIBOS 2015: The return to Asia, September 2015," *Asia Edition,* pp. http://www.gtreview.com/magazine/volume-14issue-1/sibos-2015-the-return-to-asia/, September/October 2015 Volume 14, Issue 1.

[19] M. Khanna, *Interview on TBML Challanges with various multinational and regional Tier I and II banks. Sample participant designations include Global FCC Head for Trade Products, Global Head of Trade Products, Head of FCC Practice, Regional Compliance Technology Head,* Participant names withheld by request: conducted via https://www.surveymonkey.com, December 2015.

[20] Global Trade Review (GTR), "Evolving supply chains key to the growth of trade finance," *Asia Edition,* pp. http://www.gtreview.com/magazine/volume-14issue-1/sponsored-evolving-supply-chains-key-to-the-growth-of-trade-finance/, September/October 2015 Volume 14, Issue 1.

[21] Wikipedia, the free encyclopedia, "Text mining," [Online]. Available: https://en.wikipedia.org/wiki/Text_mining.

[22] Wikipedia, the free encyclopedia, "Data Profiling," [Online]. Available: https://en.wikipedia.org/wiki/Data_profiling.

[23] Wikipedia, the free encyclopedia, "Sequential Pattern Mining," [Online]. Available:

https://en.wikipedia.org/wiki/Sequential_pattern_mining .

[24] Teppo Vuori, "How to compute check characters for IMO Number and Coden," [Online]. Available: http://tarkistusmerkit.teppovuori.fi/coden.htm.

[25] Wikipedia, the free encyclopedia, "Link Analysis," [Online]. Available: https://en.wikipedia.org/wiki/Link_Analysis.

[26] PricewaterhouseCoopers (PWC), *Goods gone bad: Addressing money-laundering risk in the trade finance system,* http://www.pwc.com/us/en/risk-assurance-services/publications/trade-finance-money-laundering.html, January 2015.

[27] Association of Certified Financial Crime Specialists (ACFCS), *Trade Based Money Laundering Tools,* http://www.acfcs.org/wp-content/uploads/2015/04/Trade-Based-Money-Laundering-Tools.pdf, April 2015.

[28] Association of Certified Anti-Money Laundering Specialists (ACAMS) White Paper - J. Scott Mauro, *The New Economy in Financial Crimes: Understanding the effects of Under-Invoicing, Double Invoicing and False Invoicing in Trade-Based Money Laundering and Terrorist Financing (TBML & TF) Schemes,* http://www.acams.org/wp-content/uploads/2015/08/The-New-Economy-in-Financial-Crimes-S-Mauro.pdf, August 2015.

[29] S. D. A. D. Manisha Kalra, "Generic Object Recognition Using a Combination of ICA and Shape Cues," in *IEEE International Conference on Video and Signal Based Surveillance*, November 2006.

[30] TechTarget, "Advanced Analytics Definition," [Online]. Available: http://searchbusinessanalytics.techtarget.com/definition/advanced-analytics.

[31] PricewaterhouseCoopers (PWC), *Internal audit holding the line on BSA/AML compliance,* http://antimoneylaundering-fiba.com/files/1499.pdf, January 2014.

[32] Federal Financial Institutions Examination Council (FFIEC), *Bank Secrecy Act AML Examination Manual, Appendix L - SAR Quality Guidance,* https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf, 2014.

[33] Financial Crimes Enforcement Network (FinCEN), *Suspicious Activity Report Electronic Filing Instructions - Version 1.2,* https://www.fincen.gov/forms/files/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf#page=2, October 2012.

Acknowledgements: This paper has been developed working under the direction of ACAMS Review Board Team. Special thanks to Marc Maramag who was on the ACAMS Review Board and John Foulley, Director, Oracle Financial Services Analytical Applications for their reviews. Additional gratitude to various industry colleagues and thought leaders for participating in the interviews and to my family for their invaluable support.