Best Practices of AML Audit of Trade Finance in Singapore

Henry Lim
1. Executive Summary

Trade-based money laundering/terrorist financing (TBML/TF”) is a complex money laundering methodology that operates across international and national borders, and is often combined with other money laundering methods such as the layering of financial transactions, use of shell companies, bulk cash and hawala underground remittance systems. Therefore, it is very difficult for banks to distinguish TBML/TF from legitimate activities of international trade by checking paperwork. As the third line of defense in banks, the internal audit function is uniquely suited to provide independent assurance of the adequacy of anti-money laundering/counter-terrorist financing (AML/CTF) controls in the bank.

Referencing Singapore Central Bank and the Monetary Authority of Singapore’s (MAS) Guidance on AML/CTF in trade finance and correspondent banking, issued on October 22, 2015, (Guideline), this white paper will explore best practices of internal audit (IA) function’s review of front to back customer due diligence (CDD) processes to gain assurance of the authenticity of trade-based transactions and by close relation, the legitimacy of the underlying trades.

The reader should take note that the key risk of TBML/TF schemes is false invoicing and other forms of falsification of trade documentations that misrepresent the quality and quantity of goods and ports of origin/destination. In Section 2, this white paper will explore key control requirements surrounding CDD processes, which the IA function of banks should review to gain assurance of the authenticity of trade-based transactions and by close relation, the legitimacy of the underlying trades.

In addition, considering the inadequacies of implementation of CDD controls and monitoring/review of suspicious transactions noted by MAS in their 2014 thematic reviews, Section 3 of this white paper will also explore the related control requirements that IAs should check, specifically on the adequacy of periodic AML/CTF risk assessments conducted by the compliance department/AML office to detect poor implementation of CDD controls in relation to trade finance business; and investigation process of red flag indicators for TBML/TF.
2. Background

Singapore, as a small Southeast Asia country, is a major transshipment center of cross-border import and export of goods between Asia and the other four continents. As one of the 25 systemically important financial centers in the world ranked by IMF, Singapore has also served as the regional funding center for trade flows within Asia as well as between Asia and the rest of the world. Therefore, it is of significant interest to the government and related central banks to comply with global ML/TF regulations and best practices/guidelines from international bodies such as FATF.


In 2014, MAS issued nine warnings and reprimands to financial institutions in 2014 and also imposed financial penalties on six financial institutions. Examples of improvements include missing periodically review of the monitoring parameters and thresholds; strengthen of internal controls to assure proper follow-up; timely implementations of new regulations and missing documentation. MAS required the financial institutions to promptly address all deficiencies and take steps to strengthen their controls and risk management framework.

As a result of MAS’ observations of weaknesses from these reviews, the Guidance on AML/CTF in Trade Finance and Correspondent Banking was issued on October 22, 2015 (Guideline). The Guideline aims to provide banks, merchant banks and finance companies (collectively referred to as banks) with guidance on the AML/CTF controls in trade finance and correspondent banking activities, assisting them in their benchmark against industry norms, implementation of sound risk management practices, and identification of control gaps.

To banks operating in Singapore, this Guideline represents a huge compliance challenge. On the other hand, MAS empowered the IA function of the banks to be responsible for assessing whether existing policies, processes and internal controls are independent, effective, and appropriate and remain sufficient for the banks’ business; and to have sufficient stature within the bank to ensure that senior management reacts to and acts upon its recommendations. FATF’s Recommendation 15 has similarly stated that the bank’s AML programs should include “an audit function to test the system.”
Given the reputation of MAS being one of the most stringent regulators in the world, this white paper offers readers a glimpse into some of the key TBML/TF controls that MAS had asked for, and contextually illustrate what IA functions should audit to determine an effective TBML/TF control program of banks. In the next chapter, audit best practices on CDD processes is explored, followed by research on the audit of risk assessment and investigation controls.

3. CDD Controls Auditing

A robust CDD approach is the cornerstone to prevent or deter criminals from using the financial systems for money laundering and terrorist financing. MAS’ definition of CDD goes beyond know your customer (KYC) during customer onboarding or periodic reviews and extends into CDD related to pre-transaction checks (PTC) of trade-based transactions. Let us explore some of the key controls surrounding CDD that IA should gain reasonable assurance on.

3.1. KYC Identification

An essential part of the auditing activities or KYC is validating if all the required activities for KYC are fortified in the controls of the organization. Some attention areas regarding trade-finance customers that should be reviewed with increased scrutiny, next to structural sound and complete collection of customer’s document are:

- The types of goods traded
- The counterparties (i.e., buyers, sellers, producers, counterparty banks etc.) by which the customers typically trade with to import/export these goods
- The countries and ports typically used by the customer and their individual risks and exposure
- A sample of trade documents such as commercial/proforma invoices, bill of lading, etc. With the collection of sample trade-based documents from customer(s), IA should further check if these documents are verified for authenticity and filed as benchmarks for comparison of authenticity in future trade-based transaction processing by the trade operations staff.

MAS’ guideline has not explicitly prescribed a list of customer documentations to be collected as part of KYC, so it is the author’s opinion that IA should validate that the bank has conducted a risk assessment to define the minimal required documents that need to be verified during CDD.
3.2. **CDD – Verification of Counterparties Related to Customers**

The purpose of verifying counterparties related to customers and subsequently checking for related party transactions is to detect collusion for trade or tax fraud. The illegal movement of funds across the border involves falsifying trade documentations to mis-declare value of goods (i.e., price, quantity or quality), and typically relies on collusion between exporter and importer since the intended outcome from this arrangement is to obtain value in excess of what would be expected from an arm’s length transaction.

In this regard, IA should check that adequate procedures exist for the bank to identify and verify related persons whom are counterparties of its customers. This can be through document collection of information regarding beneficial owners and directors of counterparties, tracing through potentially extensive and complex network of relationships using company registered information and/or from research on the internet based on the company’s website information or news articles. The information should be made available and used by trade operations staff to detect related party transactions when monitoring trade-based transactions of its customers.

3.3. **CDD – Verification of Strategic or Dual-Use Goods**

In the audit to determine if the bank has implemented adequate controls at KYC or transaction processing to check if goods traded by the customers may be strategic or dual-use goods, IAs should determine if there was sufficient training provided to the bank’s front office and trade operations staff to improve their awareness of the risks of strategic or dual-use goods and the common types of goods with dual use, and their capability to identify red flag indicators which suggest that strategic or dual-use goods may be supplied for illicit purpose. Strategic goods refer to items and their related technology that can be used to produce weapons of mass destruction and missiles capable of delivering such weapons. This includes arms and military equipment and dual-use commercial goods that can be used to develop weapons of mass destruction.

IAs should further evaluate if the bank has implemented adequate controls to determine if the goods may be strategic or dual-use goods and to request for related custom permits to determine if its customers are permitted to trade in these goods. Some of these controls can be:

a. The latest public information on related legislation/regulations and dual-use goods list (i.e., the 2003 Strategic Goods (Control) Act and List from Singapore Customs and European Commission’s TARIC database) are provided and easily referenced by the front office and trade operations staff. The Act was enacted on January
1, 2003, to regulate the trade in strategic goods and strategic goods technology.

b. Front office staff and trade operations staff are provided periodic training and possess a good understanding of the Singapore Strategic Goods (Control) Act, including any subsequent updates of the law.

c. Adequate procedure exists where front office and trade operations staff is require to refer to the Act when evaluating the information of goods traded by customers. To reduce the complexity and error in interpretation of “dual-use” goods, the front office staff should be prohibited from recording a description of the goods using generic wording such as “metal,” “vehicle,” “chemicals,” etc., which does not allow reasonable identification of such goods as “dual-use” or not.

d. Adequate procedure of an escalation process exists for front office staff to pre-consult the AML officer of the bank where there is doubt about whether dual-use goods are involved (i.e., based on the description of goods) or in addition to one or more red flags such as customers and/or trading partners known to be involved in military business; product’s capability do not fit the customer’s line of business; destination country is not known to have related technical industry or capability (e.g., semi-conductor manufacturing equipment shipped to country with no known electronics industry) etc.

e. If the goods traded by onboarding customers are strategic goods or dual-use goods, adequate procedure exists for the front office staff to obtain the related strategic goods permits issued by the Customs Department of the destination country from the customer, and to verify the authenticity of the permits.

3.4. CDD – Reasonableness Check on Quality and Quantity of Goods

To detect false invoicing and falsification of other trade documents, besides checking the authenticity of letterheads, amendments and approving signatures, another key method is to check the reasonableness of the price quoted for the goods stated in the invoices.

IA should review these controls on reasonable checks on quality and quantity of goods shipped by customers based on trade documents:

a. Adequate procedures exists by which bank had assessed past transacted goods through the bank and determined the source of indicative market value of these goods, using available commercial tools and/or combined with data from reliable data sources. Commodity goods such as oil and gas, precious metals/gems, and agricultural products have a well-established commodity price index that provides reliable and up-to-date market value of goods (i.e., Bloomberg). Other consumer goods such as mobile phones, pens,
Calculators, computers, etc., can be based on third-party tools offered to the Customs Department. For example, the Harmonized Commodity Description and Coding System was developed by the World Customs Organization and comprises about 5,000 commodity groups, each identified by a common six-digit code. This system is commonly used as a basis for customs tariff.

b. The bank should not accept any indicative market price of goods from customers without independently comparing the customer’s price information against its own sources. Instead, a control process should have been established to require the bank to perform independent price checks (i.e., reasonableness of invoice prices of goods/commodities against prevailing market prices), particularly when market prices are available, and to guide staff on the level of acceptable price variance, the threshold of price variance and the escalation/reporting process where the threshold of price variances has been exceeded for different types of goods. To prevent conflict of interest, the front office staff should not conduct such price checks.

c. Adequate procedures exist for a periodic assessment of the market price data, price variance criteria and threshold established by the bank, to ensure that the data is updated and fit for purpose.

d. Adequate procedures exist for the bank to request for specific details of goods from trade documents (i.e., invoices, packing list, Bill of Lading). Details such as HS/HTS code of goods and detailed descriptions of brand and model of goods facilitates checking of market prices and comparative quality of goods. Information of the weight of goods is available in packing lists and the types of vessel and shipping container information are available in the Bill of Lading. By comparing the weight of goods versus the vessel/container size, the bank can reasonably determine inconsistencies in paperwork that trade documents may have falsified to hide TBML/TF shipment of goods.

3.5. CDD - Sanction Screening

Sanctions are defined as rules or regulations set to enforce a certain restrictive action against persons (individuals, entities, vessels), activities or countries/regions.

International sanctions are issued by the UN Security Council and are binding on all member countries, including Singapore. Unilateral sanctions comes from individual countries like the U.S. (OFAC), EU, Japan (MOFA), MAS, etc. While generally binding on the issuing country—due to the nature of international trade and the global financial network—there is often extra-territorial applicability.

Sanctions are generally categorized as comprehensive sanctions or designated/targeted sanctions. Comprehensive sanctions target specific countries or regions such as North Korea, Syria, Sudan, Cuba...
Designated/targeted sanctions target specific persons, goods or activities. For example, UN al-Qaeda-related Sanctions (designated persons) and OFAC Sectoral Sanctions Identification (restricted activities on SSI listed entities). Most sanctions regimes, especially those under OFAC, apply the same prohibitions or restrictions on the related parties of the sanctioned person. This applies even if the related party itself is not listed on the relevant sanctioned list.

Therefore, sanctions are increasingly used as a political weapon in foreign policy, leading to banks coming under huge pressure from stricter sanctions requirements. To increase efficiency of sanctions screening given large volumes of customers and customer transactions, reputable screening tools are used at KYC and PTC stages of CDD. With regard to sanctions screening controls, IAs should therefore check adequacy of controls in the following areas:

- Adequate procedures exist to:
  - Screen customers, customers’ beneficial owners and counterparties
  - Screen customers using international sanctions lists, national sanctions lists and the bank’s sanctions lists, if any. Typically, the sanctions tools used by the bank should include international sanctions lists, national sanctions lists and the bank’s sanctions lists.
  - Ensure that changes to sanctions lists are updated to the sanctions tools promptly, accurately and completely. For example, OFAC sanctions change rapidly and there are occasions where even if the wording of the sanctions remains unchanged, interpretation and enforcement changes. Therefore, what may have been previously permissible by OFAC may not necessarily be permissible now
  - Audit trails are maintained for the sanctions screening performed for the trade-based transactions.
  - Adequate procedures exist for post-transaction reviews of closed screening hits.
  - IAs should also check if the bank has implemented a false hit list control so that alerts of good customers and transactions with a partial name match to a sanctioned entity or country are suppressed. If this control exists, IAs should check that adequate procedures exist to ensure that existing customers that are recently sanctioned will be promptly removed from the false hit list and not re-added back to the list subsequently.
  - Adequate procedures exist on how to screen customers, including the analysis, resolution and documentation of potential hits. Escalation process to the AML officer should be established for real sanctions hits. Sufficient trade-based transaction details should be obtained to check that goods do not benefit the country under strict embargo, for example:
• Trading partners or counterparties of the customer (including buyers, sellers, shippers, consignees, notifying parties, shipping agents, etc.). Nature of the goods traded
• Country or countries of origin of the goods
• Flag of vessel, flag history and name history
• Name and unique identification number (e.g., International Maritime Organization number) of any vessel used
• Beneficial owner, commercial operator and registered owner of the vessel involved in the transaction to trace the history of former ship owners with focus on country of residence
• Port of loading, ports-of-call and port of discharge (including whether the goods originate from, or are sold to any sanctioned country) and within the trade routes used

• Specifically with regard to screening of maritime vessels, adequate procedures should exist to detect vessels flying under a flag or are owned by shipping companies and beneficial owners under strict embargo, for example:
  • Where there are screening hits against vessel names, discrepancies or ambiguity in trade documents, transshipments or the use of multiple ports, trade operations staff should be required to conduct additional checks, which can include location checks of vessels (such as the last known port and destination) against third-party independent sources; additional screening of the customer’s trading partners not named in the trade documents

• With regard to screening maritime vessels, IAs should verify if the screening service provides identity, location, and ownership structure of an embargoed or sanctioned vessel as well as any financial crime-related risk connected to international sanctions, money laundering, organized crime and terrorist financing. Maritime vessels should be identified using its unique IMO ship and company numbering identifiers as such vessels could have been renamed and/or reflagged (to register a foreign ship so that it flies the flag of the registering nation) to avoid association with sanctioned bodies. The screening service should also provide intelligence on vessels and related parties with direct or indirect involvement in activities by the sanctioned countries. These parties may or may not be violating any sanctions, but their activity warrants further due diligence based on its possible relevance to sanctioned countries.
3.6. **CDD – Verification of Invoice Summaries**

IAAs should understand the business nature of invoice-financing facilities granted by banks as part of their trade finance business to fund the working capital requirements of their customers, such as factoring agreements and invoice discounting agreements. Factoring is a contract between the bank and the customer where revolving finance is provided against the value of the customer’s sales ledger that is sold to and managed by the bank. On the other hand, invoicing discounting requires the customer to manage the sales ledger.

Both of these products facilitate third-party payments by customers’ debtors. As the vast majority of debtors settle outstanding invoices by cheque or electronic payments, the risk is at the layering and integration stages of money laundering where there is no actual movement of goods or the value of goods is overstated to facilitate the laundering of funds. These factors will generally increase the risks:

- Cross border transactions
- Goods with reduced paper trails
- Goods where the bank allows the customer to collect the debt, and therefore the bank is not require to conduct periodic monitoring/onsite inspections
- Confidential or bulk goods

With this understanding of the related business processes, IAAs should recognize that the bank may accept summaries of invoice details from customers in lieu of actual invoices and shipping documents. Therefore, IAAs should check that adequate procedures exist for the bank to follow up with customers to obtain the commercial invoices and transport documents and to detect if there are any false or inaccurate information in the invoice summaries. This should be a key control as the effectiveness of the bank’s sanctions screening is dependent on the accuracy and completeness of such information. The checks can also be an effective deterrent control to discourage customers from providing false or inaccurate information.

IAAs should also determine if adequate procedures exist for post-financing verification checks, which should be performed by a function independent of the front office, typically by trade operations staff. If verification checks are done on a sampling basis, the related sampling methodology should be established to ensure consistency in applying the sampling approach. Furthermore, the sampling methodology should ensure that higher risk customers and transactions are always selected and lower risk accounts are also selected to minimize customer risk profiling errors.
3.7. **CDD – Detection of Multiple Invoice Financing**

If invoice-financing facilities are granted by the bank, IAs should also check if adequate procedures exist to detect if customers have submitted the same invoice for financing more than once, including multiple payments in the same time period (i.e., same amount, same or related vendors, same invoice or purchase order, and same or similar goods) or multiple invoices with same details (i.e., description of goods, amount, invoice number, purchase order number date).

4. **Risk Assessment and Investigation Controls Auditing**

In the overall AML risk assessment of the bank, IAs are likely to come across the specific TBML/TF risk assessment of the trade finance business in relation to the customer, geographical location and product risk factors. However, the risk assessment of the banks may focus on assessing inherent risks (i.e., risk that exists before the application of controls) and residual risks (i.e., risk that exists after the application of controls) and may not incorporate lessons learned from investigation reports of suspicious transactions detected pre- or post-transaction processing to refine and adjust the assumptions made to determine inherent risks and strengths of internal controls to mitigate the risks.

IAs should review both AML risk assessment and investigation controls to opine on the adequacy of design of controls to drive improvements in AML/CTF controls of the bank.

4.1. **Periodic Risk Assessment of Trade Finance AML/CTF Controls**

To validate the adequacy of enterprise ML/TF risk assessment undertaken by banks, IAs should have sufficient understanding of the methodology of risk assessment, especially with regard to the risk factors being assessed, the criteria and weights assigned to score the risk factors, and the assumptions made to adjust results based on qualitative parameters.

TBML/TF risk assessment should consistently follow the same principles and approach of the enterprise methodology so that the related results can be considered within the overall ML/FT risks that are to be managed by the bank. However, there are specific attention points for auditing that should be taken into consideration:

a) The ML/TF product risks and related internal controls of trade finance products and services offered by the bank have been identified and sample tested by the AML officer to be robust and operating effectively. IAs should further interview the AML officer to
check if the AML officer can demonstrate their understanding of the trade finance business and articulate what are the sanctions and money laundering risks of each trade finance product offered by the bank and the related internal controls implemented in the bank to detect and manage these risks.

b) The bank’s TBML/TF assessment are not just focused on controls related to sanctions screening and transaction screening to detect sanctioned or sanctions-linked transactions of customers. Money laundering controls such as the detection of falsified invoices, transport documents and related party transactions should also be assessed to give assurance that related KYC and trade finance transaction processing controls exist and are robust.

c) All applicable AML/CTF regulations and guidelines related to detecting TBML/TF are considered and incorporated into the bank’s internal controls. This area is especially challenging and may not be evaluated adequately due to the diverse existence of AML/CTF regulations and regulatory expectations in the Asia region.

d) Interviews with the front office and trade operations staff to observe that both functions are aware of the interdependency of the functions to closely collaborate to detect suspicious trade-based transactions, and that they can articulate examples and consistent details of the collaboration process within the examples. For example, if the trade operations staff had identified a suspicious transaction, the front office staff may be called upon to support the trade operations staff and request for more information from the related customer on the transaction in a tactful manner so as not to tip off the customer.

e) The assessment should evaluate the adequacy of trade finance AML/CTF training provided to the front office and trade operations staff, including the quality of training and training participation. IAs should also consider evaluating the training materials to at least cover the entire related bank’s internal controls and how to detect and document the assessment of red flag indicators, including narration of case facts, reason of suspicion and retention of document evidence.
4.2. Investigation and Follow-Up of Red Flag Indicators

Most literature in AML/CTF focus on the study of patterns (i.e., red flag indicators) of TBML/TF activities. However, what is of more importance to the IA audit program is the check of subsequent actions to detecting the red flag indicators, such as further investigations and reporting of these illegal activities, and to have remedial actions to improve controls and minimize TBML/TF risks for the bank.

It is important to note that TBML/TF red flag indicators by itself are not proof of wrongdoing and serve as indicators that trade-based transactions require further investigation. For a list of TBML/TF red flag indicators, the reader can refer to the Wolfsberg list or FATF list.

IAs should determine that the bank has established a process to identify, detect, investigate, escalate and maintain a relevant and tailored list of TBML/TF red flag indicators. A more comprehensive process can include these requirements:

- Each red flag indicator identified should be supported by how the red flag indicator can be detected in the CDD process by the front office or trade operations.

- The investigation process should require investigators in the bank to document the steps taken to investigate and establish the case, and the reasons of suspecting the transaction. The requirement to obtain and retain supporting documents should be also established to support the case investigation.

- For suspected transactions, the bank may suspend transactions pending the AML officer’s further review of case files and advice on the next steps, such as to file a suspicious transaction report and/or prohibit the transaction, etc.

In the appendix of this white paper, an overview is given on how potentially suspicious trade-based transactions can be investigated and followed up.

5. Conclusion

Regulatory demand places pressure on trade finance business processes, and a heavy load is placed on front office staff and trade operation staff to ensure compliance. Although MAS recognizes the complexity of international trades, and the difficulties faced by banks to detect potential TBML/TF by CDD and verifying trade-based transactions, it is the author’s opinion that they also expects the banks to demonstrate that they have implemented effective controls over TBML/TF over these areas:
- Sufficient understanding of customers’ business operations in their trade-based transactions and related remittances/payments, including trade flows with key counterparties;

- Close collaboration between front office and trade operations;

- Continuous learning and sharing of methods to detect suspicious transactions and unusual customer behaviors enhanced by knowledge on emerging TBML/TF patterns shared by international bodies such as FATF and the Wolfsberg Group;

- Regular updates and awareness training, to capture the latest regulatory requirements and trends resulting from adverse news in AML/CTF breaches by other banks; and

- Efficient use of automated tools to screen more effectively and refinement of rules to handle risks more efficiently.

The IA function plays an important role in providing independent and reasonable assurance of AML/CTF controls of the bank. However, as banks expand their trade finance operations across the globe, the IA function often observes these significant challenges together with their elevated role:

- Risk-based approach placed by regulators on banks to manage AML/CTF risks do not mean regulators’ consent to adopt riskier approach and compromised controls. Therefore, a comprehensive review of the full potential of risks in all business areas within the bank is required.

- The effectiveness of an AML/CTF framework is dependent on human factors. Therefore, the culture of compliance and tone at the top are key.

- Although technology can reduce human error in AML/CTF controls, rapid change of technology may introduce knowledge gaps and create procedural control lapses as well.

To overcome these challenges and expectations in both business and IA functions, senior management of banks must maintain an unwavering tone from the top that risk and compliance is as important as business revenues. The financial institution’s reputation and customers’ assets at the bank will profit from a strong compliance and internal audit function.
6. Appendix: Investigation and Follow Up for Trade-Based Transactions

The following is an example of how potentially suspicious trade-based transactions can be investigated and followed up:

- Define a list of categories of suspicious trade-based transactions for ease of grouping, reporting and searching.
- Assess the list of applicable red flag indicators for trade-based transactions, and link them to the list of categories defined.
- Identify the controls to detect the red flag indicators from the categories of suspicious trade-based transactions.
- Define the steps by which investigations can be carried out based on the detected red flag indicators, and requirements to document and retain the investigation results.
- Define the supporting documents that must be retained by the bank as evidence of investigation results.

<table>
<thead>
<tr>
<th>Categories of Suspicious Transaction</th>
<th>Indicators</th>
<th>Detection</th>
<th>Investigation and Case File</th>
<th>Attachment of supporting documents</th>
</tr>
</thead>
</table>
| High-Risk Entity (CDD)               | Customer is featured in adverse news related to TBML | Adverse news screening tool and process | Review customer’s account. Check for sudden influx of funds during the period the said TBML was committed. Review the KYC documents of the customer and incoming/outgoing remittances of the customer during the period. Further check against underlying trade documents if any to conclude if customer had been using the Bank to support its TBML activities. Case file is made with supporting documents highlighting the analysis made. Trade Operations temporarily suspend the transaction pending further review and advise by AML Officer. | Case file with supporting documents e.g.:  
Media reports, Desktop research, screening tools’ results  
Income range, print screen of customer profile, bank account opening form  
Relevant supporting documents of transactions e.g. cheque images, details of source/beneficiary of funds, SWIFT messages  
Relevant bank statements of transactions  
Business registration details of customer (ACRA screening or equivalent)  
Relevant trade documents such as Bill of Lading, Commercial invoice, packing list etc.  
Particulars of the original purchasing party.  
Particulars of the new purchasing party.  
Relevant supporting documents that customer declined to put his name on.  
Particulars of the beneficial owner, if
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Counterparty Details</th>
<th>Transaction Details</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-Risk Entity (CDD)</td>
<td>Counterparty of the Customer is featured in adverse news related to TBML</td>
<td>Adverse news Screening tool and process</td>
<td>Review customer’s account. Check for customer’s making wire transfers to counterparty during the period that the said TBML was committed. Review the KYC documents obtained for the customers and wire transfer instructions to check if wire transfers were abnormal considering the customer’s known business activity and trading partners. Further check underlying trade documents if necessary to conclude if customer had been using the Bank to support TBML of the counterparty. Case file is made with supporting documents highlighting the analysis made.</td>
</tr>
<tr>
<td>Dubious/Uneconomical activities</td>
<td>Customer submitted falsified trade documentation when there was no actual transaction of goods.</td>
<td>Information is provided by Whistleblower that trade documents of a trade-financed shipment made by customer were falsified and that no goods have arrived.</td>
<td>Information provided by whistleblower is reviewed against said falsified trade documents to determine if there are reasonable grounds to suspect falsified of documents (e.g. obvious errors or inconsistencies in the documentation).</td>
</tr>
</tbody>
</table>
been shipped. trade documents given the new information provided).

Case file is made with supporting documents highlighting the analysis made. Trade Operations temporarily suspend the transaction pending further review and advise by AML Officer. STR may be filed.
7. Glossary

- The term **trade-based money laundering and terrorist financing** (TBML/FT) refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities. Besides money laundering and terrorist financing, this process is also applicable for evading tax and custom duties, circumvent specific jurisdiction’s restriction of capital outflow (e.g., China) and to obtain tax incentives by abusing transfer pricing. Examples of how TBML/TF may be carried out include, but are not limited to: misrepresentation of the price, quantity or quality of imports or exports; and money laundering through fictitious trade activities and/or through front companies.

- The term **trade-based transaction** refers to whatever information a bank collects, by paper or electronically, on its import-export forms or supporting documentation. For example, such information usually includes a description of the goods being imported or exported, their quantity, value, weight, customs or tariff code number, the mode of transportation by which the goods are being imported or exported, and/or the name and address of the exporter (consignor), importer (consignee), and shipping company.

- The term **trade finance** refers to the financial component of an international trade transaction (i.e. managing the payment for goods and related services being imported or exported). Trade finance activities may involve, among other things, managing payments for open account trading, or issuing letters of credit, standby letters of credit and guarantees.

- The term **Front Office staff** refers to relationship managers or officers of banks that maintain close customer relationships and conduct know your customer reviews in CDD processes.

- The term **Trade Operations staff** refers to back office operations that process Letter of Credits, payments and remittances to counterparties for underlying trade-based transactions.
8. References

1) Internal organization’s training materials on TBML/FT controls and an experienced IAD team in KYC/AML audits.


Software and services to track prices of consumer products - https://www.semantics3.com/

Google Play or Apple Appstore application – Price Match, ShopSavvy

    http://www.bloomberg.com/energy