Suggested Best Practices for Banks to Combat Trade Based Money Laundering

Noted by the 17th joint meeting of the 12th Supervisory Committee of the Bankers Association of the Republic of China on 2018/5/31

Noted of the amendment to Letter of Jin-Guan-Yin-Fa-Zì No. 10701108990 dated 2018/08/07 by Financial Supervisory Commission

I. This document aims at providing practical implementation comments to member banks for reference in identifying and assessing money laundering and terrorism financing risks of trade finance, without the nature of self-regulation stipulated by the Bankers Association of the Republic of China (BAROC) or any substantial binding force.

According to the report "Trade-Based Money Laundering" (hereinafter referred to as "TBML") published by Financial Action Task Force (FATF) on June 23, 2006, TBML is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. Other organizations, such as Wolfsberg Group, have also put emphasis on the risks of TBML.

Trade is a vital part of Taiwan's economy. Development of Taiwan's economy may be adversely affected, if the banks in Taiwan render financial services without corresponding systems and controls to manage various risks of money laundering and terrorism financing. This document, not only mitigates the risks of TBML but also mitigates the proliferation risks of weapons of mass destruction.

II. This document focuses on the appropriate measures may be taken by customers and the third parties for money laundering and terrorism financing risks arose from trade-related activities . Considering the

numerous types of products and services in trade businesses, the trade-related activities referred to in this document include but are not limited to import and export negotiation, issuance of letter of credit (L/C), purchase of customers' liabilities under letters of credit , purchase of accounts receivables, accounts payable, accepted export bill discounted, materials procurement guarantee, export loans, import financing, import and export foreign loan, acceptance receivable, payment on behalf of Financial Institution, and open account (OA) transaction, etc.[1,2]

Apart from the above-mentioned products and services, banks may include relevant products and services in the risk assessment of TBML based on their own business scope and scale.

III. Apart from abiding by the relevant regulations in the “Regulations Governing Anti-Money Laundering of Financial Institutions” and the “Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures” established by BAROC, banks shall adopt a risk-based approach (RBA) to assess the risks of TBML, or include risks of TBML into the comprehensive risk assessment of money laundering and terrorism financing, establish appropriate measures to perform the review on customers and relevant transactions, as well as ongoing transaction monitoring. Upon discovery of any abnormality in business nature or

Note 1: amendment to Order of Jin-Guan-Yin-Fa-Zi No. 10500106150 dated 2016/05/19 by FSC, the calculation method for the total limit of credit extension, investments and call loans made by the banks in Taiwan region to Mainland China area are illustrated in Article 5, Paragraph 1, Subparagraph 1.

Note 2: Open Account listed in this section defines as: [Open account transactions: these are transactions where the buyer makes a payment once they have received the goods.] Please refer to Section 153 of "The Risk Factor Guidelines" (2017) by the Joint Committee of the three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) and Appendix IV: Open Account of 「The Wolfsberg Group, ICC and BAFT Trade Finance Principles」(2017).

transaction pattern, the relevant enhanced due diligence shall be conducted.

For risks and customer-level of risk on TBML, banks may refer to the Appendix Ⅰ to further enhance the controls, lower or prevent the TBML risks. And banks also may refer to the Appendix II for other relevant control measures.

IV. Banks shall formulate TBML red flags, suspicious transaction review and report procedures (which may be integrated with the existing money laundering red flags and suspicious transaction review and report procedure), and refer to the suggested red flags listed in Appendix III to enhance monitoring measures over TBML transactions.

V. The subject of TBML shall be performed into Banks' training for Anti-Money Laundering and Combating the Financing of Terrorism (hereinafter referred to as "AML/CFT") based on staff's job specification. The content of training program shall refer to and include frequently-occurred transaction typologies and suspicious transaction cases prone to happen, in order to fit each bank's level of risk , and to enhance staff's ability (such as trade-related operations staffs, AML/CFT staffs and internal audit staffs) to identify TBML. In addition, banks shall carry out ongoing training for relevant staffs to fully keep up with the current laws and regulations, business demands and development trend of TBML, enabling them to be fully aware of the risks therein.

Appendix I: References for Trade Based Anti-Money Laundering Risks and Customer-Level of Risk

I. Trade finance is a complex and specialized field. There are multiple parties with interconnecting relationships and intricate structures, thus banks may take the Risk Factor listed in this Appendix into consideration when carrying out risk assessment on TBML or Enterprise-Wide Risk Assessment (EWRA). When conducting customer risk rating (CRR), banks may consider the customer risk factors in this Appendix to increase the efficiency of risk assessment.

II. In customer risk assessment project, customer risk rating, and ongoing customer due diligence , apart from following the annex of Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures “Guidelines for Banks Regarding Assessment of Money Laundering and Terrorist Financing Risks and Adoption of Prevention Programs”, the following alerts can be incorporated for assessment so as to adjust customers’ level of risk.

A. Business Nature:

1. The type of import and export goods is inconsistent with the customer’s regular business activities. For example, the major business of a customer is toys import/export trading, but the goods are iron sand or petroleum instead. It does not fit its original business activities.
2. The transaction amount of the goods is not consistent with the scale of the customer’s regular business activities. The transaction amount of the customer in one time or a single batch of goods accounts for half of or several times over the

turnover.

3. The customer suddenly conducts businesses in high risk areas. The customer normally conducts businesses in general or low-risk areas, but it suddenly develops businesses in high risk areas.
4. Customer's original business scope or type of underlying goods is easily utilized for money laundering or terrorism financing, embargoed/restricted goods, or high risk goods.
5. Substantial changes to business nature without explicit reason or reasonable explanation.

B. Transaction Pattern

1. Disguising the true nature of transaction with extremely complex transaction structure. In establishing business relations with a customer, a normal pattern for transactions will generally be adopted. After a period of time, however, the customer resorts to extremely complex transaction structure to disguise the true nature of transactions.
2. Goods in transactions are against import or export laws and regulations, or they involve dual-use goods and high risk goods. The price of goods and service is relatively high or low compared with the fair market price in general.
3. Receiving cash or other payments from the third party without any obvious connection. If the payment for goods after delivery is not paid by the counterparty, but by the third party without any obvious connection, such as ordering customer is money services business (MSB), there is the possibility of a delivery to a sanctioned country or region with the payment collected through other channels.

4. Substantial changes to transaction pattern without explicit reason or reasonable explanation.

Appendix II: Suggested Best Practices for the Control Measures Taken

To reduce the associated risks of TBML, banks may refer to the following items for taking risk mitigation measures.

I. Control system

A. Ensuring Trade Controls contain appropriate procedures for handling the suspicious transaction reports and red flags, as well as escalation management process.

B. Ensuring the red flags of the customers and transactions are identified at various stages of relevant trade transactions.

C. Requiring relevant staffs to conduct appropriate customer due diligence(CDD), and use information from CDD to assess：

1. Whether the trade transactions are commensurate with the customer background；
2. Whether the type of commodity being shipped fits the customer's regular business activities.

D. Implementing reports or systems (such as suspicious reports and detection scenarios) that can monitor the customer business pattern or activities, such as the following examples：

1. Transactions involving high risk jurisdictions；
2. Transshipment involving sanctioned countries.

E. Establishing appropriate screening procedures for transactions.

F. Ensuring that red flags are regularly updated and easily accessible to related staffs.

G. Formulating appropriate reviewing procedures for dual-use goods, based on the nature and scale of each bank's trade-related activities.

II. Customer Due Diligence

A. Documenting an internal assessment framework, for the purpose of the AML/CFT in a given trade transaction or other trade-related scenario. Moreover, banks need to identify who the customer is and determine whether a customer relationship exists between a bank and a particular party in the context of particular trade-related terms.

1. Indicative factors for identifying a customer of the bank are as follows：

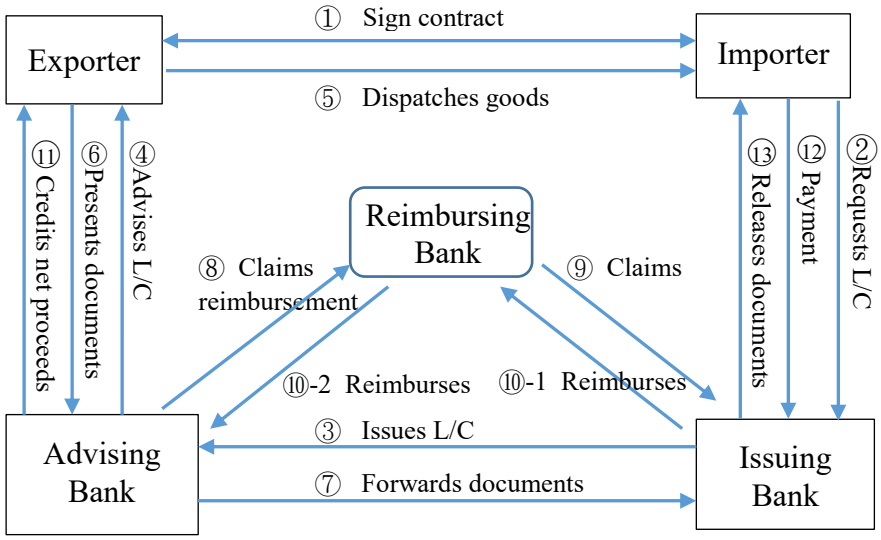
(1) Who instructs the bank?

(2) What are the nature of relationship and degree of connectivity between the bank and the instructing party?

(3) What are the precise activities conducted by the bank?

(4) In what capacity does the bank carry out those activities?

2. Take L/C as an example:



(1) For the Issuing Bank, the customer refers to the Importer；

(2) For the Negotiating Bank, the customer refers to the Exporter；

(3) For the Reimbursing Bank, the customer refers to

the Issuing Bank；

(4) For Advising Bank, the customer refers to the Issuing Bank or the First Advising Bank (if any).

B. Assessing customers' TBML risks based on their anticipated trade-related activities, upon an application for relevant services. Examples of factors for consideration may include：

1. Types of goods
2. Trade volumes
3. Counterparties
4. Complexity of transaction structure
5. Shipment methods (e.g. by sea or by air)

C. Customers engaged with transactions with high risk goods refer to business items or commodities traded of whom are the export or import restricted goods, such as weapons, chemical goods, metals, gem, crude oil, etc.

III. Transaction review

A. Obtain and review as many relevant transaction documents as possible.

B. Under reasonable and feasible circumstances, obtain the latest pricing information for relevant commodities, and carry out price verification. Banks may examine the public domain for the pricing information of the goods shipped, to ensure the stated price on the trade documents are considered reasonable compared to market price, obvious higher or lower than the cost or price reported to the custom, or obvious higher or lower than previous average price in used transactions. Banks may set a price verification procedure based on RBA and keep related records.

1. Ensuring the staffs engaged in trade finance are able to identify the definite red flags.
2. Considering the internal escalation procedure, and requiring the relevant staffs to escalate investigation results as soon as possible.

IV. Monitoring items

A. Identifying and screening all relevant parties to a transaction and other information contained within trade documents against applicable sanctions lists.

B. Screening and recording all relevant fields and information to a transaction with related systems, for example：

1. Counterparty name(s) and location(s)
2. Counterparty bank(s), their capacity in the transaction and location(s)
3. Customer name(s) including individuals and companies
4. Carrier/charter/agent
5. Consignee
6. Country of origin
7. Description of goods or commodities
8. Freight Forwarders or shipping companies
9. Originating and recipient entities of the goods(i.e. importer and exporter)
10. Shipper, consignee, and notification party on transport documents
11. Shipping route (such as the port of loading, port of discharge, port of transshipment, etc.)
12. Vessel name(s)
13. Flag of vessel

Investigating hits before entering to trade, and keeping the decision –making process for records.

C. Using manual screening and review procedures to supplement the insufficiencies of the trade processing procedures, such as:
   1. Issuing multiple invoices;
   2. Significant differences in the descriptions of the goods between customs declaration, invoice and other documents (i.e. certificate of origin, packing list, etc.);
   3. The shipment locations of the goods or descriptions of the goods are inconsistent with the L/C;
   4. Packages are inconsistent with the nature of the goods or vessel type (for example, whether to transport oil by tanker, etc.);
   5. Unable to determine the originating and recipient entities of the goods (i.e. through agent)；
   6. Frequently amended L/C without reasonable ground, including changes to the beneficiary or location of payment;
   7. Common red flags of fraudulent L/C, including unauthenticated SWIFT message, more than two advising banks, inconsistent clauses or clauses unable to implement, etc.

D. Ensuring new or amended information about a transaction is obtained and screened.

Appendix III: References for Red Flags for Transaction Suspected

I. According to the Article 4 of Red Flags Transaction Suspected to involve Money Laundering or Terrorism Financing listed in the Annex of Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures, the listed typologies are:

A. Discrepancies appear between the description of the commodity on the bill of lading and payment order or invoice, such as inconsistency in the product amount or type.

B. Significant discrepancies appear between the pricing or the value of the product or service reported on the invoice and its fair market value (undervalued or overvalued).

C. The method of payment appears inconsistent with the risk characteristics of the transaction, for example, the use of an advance payment for a new supplier in a high risk jurisdiction

D. A transaction involves the use of L/C that are amended, extended, or change payment location frequently or significantly without a reasonable explanation.

E. Using L/C, negotiable instruments or other means that are issued overseas without trade basis to obtain financing.

F. Commodities shipped are inconsistent with the customer’s industry or operations, or unrelated to the customer’s business nature.

G. Customers involved in high risk suspicious ML/TF activities, including importing/exporting goods that are subject to embargo or restrictions (e.g., military supplies of foreign governments, weapons, chemicals, or natural resources such as metals).

H. The commodity is shipped to or from a high ML/TF risk jurisdiction.

I. The type of commodity shipped is vulnerable to ML/TF, for example, high-value but low-volume goods (such as diamonds and artworks).

II. Apart from the above-mentioned suspicious transaction typologies, banks may refer to the following red flags to establish a set of referable red flags or typologies.

A. Customer

1. Unusual transaction structure or overly complex transaction structure without a clear and legitimate commercial purpose or some reasonable ground.
2. The transaction is not commensurate with known customer profile, structure or business strategy. In a TBML context, this may be where the nature or type of goods shipped is not in line with the business nature of the customer (e.g. a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals), the mentioned goods are not approved by relevant government authorities, or the size or frequency of the shipments appears inconsistent with the scale of the customer's regular business activities (e.g. a sudden surge in transaction size).
3. The customer significantly deviates from their historical pattern of trade activity (i.e. in terms of value, frequency or method of payment) with dubious pricing of goods and services.

4. The customer or parties have suspicious addresses. For example different transacting businesses may share the same address or the enterprises only provide a registered agent's address.
5. The customer reacts aggressively to know your customer questionnaire or tries to force the bank to take CDD shortcuts by citing time pressures.
6. The customer refuses any contact or communication with the bank, without a legitimate reason.
7. The customer is willing to pay unusually high fees to the bank to proceed with the transaction.

B. Documentary

1. The shipment locations of the goods, shipping terms, or descriptions of the goods are inconsistent with the L/C. This may include changes in shipment locations to high risk countries or changes in the quality and quantity of the goods shipped.
2. There are substantial discrepancies in merchandise descriptions, e.g. quantities, weights. .
3. Significantly amended L/C without reasonable ground or changes to the beneficiary or location of payment.
4. The documents show excessively amended terms.
5. The documents contain non-standard clauses, phrases or other unusual characteristics therein.
6. There are unauthorized alterations or amendments to the documents.
7. The beneficiary or applicant refuses to provide documents to prove shipment of goods (indicates possible phantom

shipping or multiple invoicing).

8. There are other dubious indicators such as unusual codes or markings on the monetary instruments (e.g. drafts or bills of exchange, or future dated bills of lading, or transaction under L/C without proper transport document or document evidencing shipment / delivery of goods).
9. There are indications that the descriptions of the goods are coded or disguised.
10. The customer requests (a) an L/C without calling for transport documents or documents evidencing shipment or delivery of goods; or (b) an amendment to a L/C removing the transport document or document evidencing shipment or delivery of goods as required in the original terms.
11. The transaction is without transport documents evidencing movement of goods.
12. The bill of lading describes containerized cargo but without container numbers.
13. There are indications that documents have been re-used.
14. There are indications of double invoicing.
15. The invoice shows “Other/Undefined” charges as an unreasonably high percentage of total transaction value.
16. A documentary credit if overdrawn by more than an unreasonably high percentage of the original value.
17. The goods in respect of a documentary credit are over shipped by an unreasonably high percentage of the original quantity.
18. An L/C is dated later than its date of presentation.
19. The description of goods on the transport documents (if

any) cannot be linked to the document terms and / or the actual invoice.

20. The customer re-submits a document rejected earlier as a result of financial crime risk concerns.
21. The documentation appears illogical, fraudulent and/or improperly modified from its original content, or certain documentation is absent that would be expected given the nature of the transaction.

C. Transaction

1. The transaction structure aims at concealing information or making the bank be hard to obtain certain information or the true nature of the transaction. This may include indications that a shipment is structured to disguise proliferation risks of weapons of mass destruction.
2. The transaction involves round-tripping or circular transactions.
3. The transaction involves unusual or complicated movement of goods and/or the third party without an obvious commercial purpose.
4. The method of payment appears inconsistent with the risk characteristics of the transaction.
5. The shipment does not make economic sense, takes an uneconomical shipping route, or the shipping route is unclear.
6. The mode or method of shipping is unclear.
7. The customer has unusually frequent round dollar transactions.
8. The transaction involves sanctioned entities.

9. The transaction route involves high risk jurisdictions, or the trade transaction otherwise involves high risk jurisdictions.
10. The commodity is trans-shipped through one or more jurisdictions for no apparent economic or other logistical reason.
11. The transaction involves the receipt of cash (or other payments) from the third party that have no apparent connection with the transaction.
12. The transaction involves an unusually high number of intermediaries, too many or unnecessary parties, or transferable L/C.
13. The tenor of a relevant transaction is not in line with the nature of the underlying commodity financed – for example, in relation to a perishable good.
14. Documents such as an L/C received through unverified channels such as unauthenticated SWIFT message.

D. Commodity

1. The commodity includes dual-use goods.
2. High risk goods:
   (1) Gems;
   (2) Jewelry;
   (3) Cigarettes and other tobacco products;
   (4) Consumer electronics and home appliances, such as high-price mobile phones;
   (5) Telephone cards and other stored-value cards;
   (6) Precious metals;
   (7) Military goods and war materials (including arms, ammunition, bombs, missiles, sensor integration equipment, armored vehicles, electronic equipment, laser systems, flying objects, tear gases and other

irritants, and weapons and software developed for war materials);

III. When formulating or detecting red flags or typologies for transactions suspected, the relevant content has to be reviewed, with reference to the following items:

A. Red flags or typologies: a mismatch in the invoice value (freight charge) and the fair market price.

1. Over Invoicing: by invoicing the goods or service at a price above the fair market price, the seller is able to receive price differences from the buyer, as the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market.
2. Under Invoicing: by invoicing the goods or service at a price below the fair market price, the buyer is able to receive price differences from the seller, as the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market.

Content of this red flag or typology for transactions suspected shall be reviewed:

1. Product taxonomy (i.e. table of product categorization);
2. Category of goods;
3. Goods description;
4. Unit price of goods;
5. Quantity of goods;
6. Market price of goods.

B. Red flags or typologies: fictitious trade

The seller did not ship any goods at all, but simply colluded with

the buyer to ensure that all shipping and customs documents associated with the trade.

Content of this red flag or typology for transactions suspected shall be reviewed:

1. Transaction date;
2. Quantity;
3. Unit price of goods;
4. Presence of transport document;
5. Validity of transport document.

C. Red flags or typologies: multiple invoicing of goods and services.

Issuing more than one invoice for the same trade transaction. By invoicing the same goods or service more than once to justify multiple payments for the same shipment of goods or delivery of services

Content of this red flag or typology for transactions suspected shall be reviewed:

1. Transaction date;
2. Amount of the transaction;
3. Product description;
4. Invoice number;
5. Other banks' account information recorded in the invoice.

※※※※※※※※※※※※※※※※※※※※※※※※※※※※
※ The Clauses are made in both Chinese and English. ※
※ In case of any discrepancy between the Chinese and ※
※ English version, the Chinese version shall prevail.※
※※※※※※※※※※※※※※※※※※※※※※※※※※※※