The Hong Kong Association of Banks

Guidance Paper on Combating Trade-based Money Laundering

1 February 2016

This Guidance Paper on Combating Trade-based Money Laundering (**Guidance Paper**) has been developed by the Hong Kong Association of Banks (**HKAB**) with input from the Hong Kong Monetary Authority (**HKMA**). The practices recommended in this Guidance Paper do not form part of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for Authorized Institutions) (**AMLO Guideline**).

However, the HKMA considers that the adoption of these practices will assist authorized institutions (**AIs**) in not only meeting the legal and regulatory obligations under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (**AMLO**) and the AMLO Guideline, but also in implementing effective measures to further mitigate their money laundering and terrorist financing (**ML/TF**) risks. AIs should also take appropriate measures to ensure compliance with Hong Kong's sanctions regime, and obligations under Hong Kong law in respect of weapons of mass destruction (**WMD**) proliferation. In addition to meeting requirements under Hong Kong laws, these practices will also help AIs operating internationally to meet relevant overseas sanctions regimes that are applicable to them.

The HKMA therefore expects every AI to give full consideration to the adoption of the practices that this paper recommends where necessary, to improve their anti-money laundering and counter-terrorist financing (**AML/CFT**) systems, taking into consideration the ML/TF risks to which they are exposed.

1 Introduction

1.1 Trade-based money laundering has been recognised by the Financial Action Task Force (**FATF**) in its 2006 study as one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy. A number of other competent authorities and industry groups, such as the Wolfsberg Group, have also highlighted the risks in this area.

1.2 Trade is an important part of the Hong Kong economy. Hong Kong's role as an international financial centre, and confidence in the integrity of the banking sector may be adversely affected if AIs do not have appropriate systems and controls to manage various risks which may arise in the provision of financial services to support this important aspect of the Hong Kong economy.

1.3 The recommendations set out in this Guidance Paper are supplementary to, and do not supplant, any relevant legislation, codes, guidelines or rules applicable to AIs. They are neither intended to, nor should be construed as, an exhaustive list of the means of meeting AIs' statutory and regulatory requirements, nor does it provide prescriptive guidance on specific transactions or relationships. In particular, this Guidance Paper must be read together with the following legislation, as well as related subsidiary legislation and guidance:

(a) AMLO;

(b) Organized and Serious Crimes Ordinance (Cap. 455);

(c) Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405);

(d) United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575);

(e) United Nations Sanctions Ordinance (Cap. 537); and

(f) Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap.526).

1.4 It is open to AIs to take alternative measures to manage relevant risks relating to ML/TF, sanctions and WMD proliferation. HKAB recommends that such alternative measures, and the rationale for adopting them, be appropriately documented, bearing in mind the HKMA's expectation for AIs to give full consideration to the practices specified in this Guidance Paper.

2 About Trade-based Money Laundering

Key Concepts

2.1 "Trade-based money laundering" was originally defined by FATF in 2006 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.'

2.2 The FATF Paper on Best Practices (2008) broadened the definition to include terrorist financing, such that the current FATF concept is defined as follows:

> *"[Trade-based money laundering] and terrorist financing (TBML/FT) refer to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origin or finance their activities."*

2.3 This definition recognises that terrorist organisations also engage in a variety of criminal activities, ranging in scale and sophistication from low-level crime to serious organised crime.

2.4 This Guidance Paper refers to this expanded concept as "**trade-based money laundering**". However, it is not intended to be limited to ML/TF. As noted in the introduction and in paragraphs 1.3 and 1.4, sanctions[1] and WMD proliferation risks should also be mitigated. As a result, references to "**ML/TF**" in this Guidance Paper should be read broadly to include these issues, where appropriate.

2.5 The crux of this concept is the use of trade transactions to facilitate ML/TF. For the purposes of this Guidance Paper, the term "**trade transactions**" is intended to be interpreted broadly to refer to both domestic and international transactions in respect of goods or services between a buyer and a seller. The precise scope of the concept relies on the individual AI's own judgment, using a reasonable approach. Indicative examples of certain typical products and services provided by AIs (as intermediaries in trade transactions) are set out in paragraph 2.7. A reference to "**trade-related activities**" in this Guidance Paper refers to activities carried out by AIs involving trade transactions.

2.6 The focus of this Guidance Paper is on the trade-related activities of AIs with their customers and relevant third parties, which can include non-banking entities. However, AIs should also consider the trade-based money laundering risks of their bank-to-bank relationships, and take appropriate steps as necessary.

Trade Products

2.7 While there is no exhaustive list of trade-related products and services, some indicative examples of products or services that typically fall within the scope of "trade finance" services provided by AIs, and therefore within the scope of this Guidance Paper, include:

- Bank guarantees
- Documentary collections
- Financing under open account transactions
- Forfaiting and risk participation
- Import/export loans
- Packing loans
- Pre-shipment loans
- Structured trade financing
- Trust receipts
- Warehouse financing

[1] Sanctions include United Nations Security Council sanctions and other national and regional sanctions. They include: (a) country-based financial sanctions that target specific individuals and entities; and (b) trade-based sanctions, for example, embargoes on provision of certain goods, services or expertise to certain countries.

- Import/export invoice discounting
- Letters of credit ("**L/C**")
- Financing for transactions under L/Cs

In addition to the above examples, AIs should consider, based on their own business activities and internal classifications, what other products and services fall within the ambit of "trade transactions".

2.8 The types of products and services offered by a particular AI should be factored into relevant risk assessments and related controls, as described in paragraphs 3 and 7. Annex A also describes a typical L/C structure.

Who is the Customer?

2.9 Trade is a complex and specialised area. There are multiple parties with interconnecting relationships and intricate structures. The essential questions required to assess whether customer due diligence ("**CDD**") requirements under the AMLO may apply, such as "who is the customer?" or "has a business relationship been established?" can be difficult to answer definitively.

2.10 There is no "one size fits all" approach. However, generally, AIs need to identify who the customer is and determine whether a customer relationship exists between an AI and a particular party in the context of particular trade-related arrangements. Indicative factors of a customer relationship may include the following:

(a) Who instructs the AI?

(b) What is the nature and degree of connectivity between the AI and the person?

(c) What are the precise activities conducted by the AI?

(d) In what capacity does the AI carry out those activities?

(e) Who benefits from the AI's services?

(f) Which other parties are involved and what are their roles?

(g) How are financial matters structured by the AI, such as the booking of revenue and profit, handling of operational costs and making of payments?

(h) What is the legal structure and how is it documented and treated from a tax perspective by the AI?

(i) What broader rights and obligations apply to the trade transaction, including under internationally accepted standards that are adopted by the industry?

2.11 **Annex A** describes the two key parts of a typical L/C transaction structure and who would typically constitute the "customer" in certain relationships. Importantly, structures vary and reasonably minor changes in facts can impact the "customer" assessment.

2.12 Some AIs may act as trade finance operation hubs to provide a range of services for their offshore branches or other banks. AIs acting in this capacity should assess whether a business relationship exists with the outsourcing branch or third party bank and the underlying customers, and whether correspondent banking controls are required.

Broader AML/CFT Obligations

2.13 Even where there is no "customer" relationship for the purposes of the AMLO, AIs should remain mindful of their broader AML/CFT obligations under Hong Kong law. This includes

having appropriate procedures identifying the steps to be taken in relation to non-customer third parties, such as beneficiaries (or recipients) of an L/C issued by an AI, and where appropriate having regard to the level of ML/TF risk involved. Such procedures may include, for example, checking public sources of information and internet searches. Paragraph 6 and Part 2 of Annex B also describe recommended approaches to transaction screening generally.

3 Trade-based Money Laundering Controls

Key Principles

3.1 Establishing and maintaining adequate and appropriate risk-based controls to address trade-based money laundering risks are an essential element of AIs' trade-related activities. Specifically, section 19(3) of the AMLO requires AIs to establish and maintain effective procedures not inconsistent with the AMLO for the purposes of carrying out key duties under Schedule 2 to the AMLO,[2] in respect of each kind of customer, business relationship, product and transaction.

3.2 Accordingly, AIs should develop written policies and procedures to assess and mitigate ML/TF risks arising from their trade-related customers and activities ("**Trade Controls**").

3.3 Key principles relating to Trade Controls are as follows:

(a) **Institutional** / **Business-level Risk Assessment** – AIs should adopt a risk-based approach to their assessment of risks in relation to trade-related activities, as well as the formulation and implementation of Trade Controls. The risk assessment may form part of the AI's own institutional risk assessment or a distinct trade-related risk assessment, which gives appropriate consideration to ML/TF risks, sanction and WMD proliferation risks. The risk assessment should be well documented and kept up-to-date. Reference should be made to the HKMA circular dated 19 December 2014.[3]

(b) **Customer** / **Transaction-level Risk Assessment** – AIs should perform customer-level or (for non-customers) transaction-level risk assessment by making reference to the risk-based approach as set out in Chapter 3 of the AMLO Guideline and, based on the assessment results, conduct appropriate CDD and ongoing monitoring measures by making reference to Chapters 4 and 5 of the AMLO Guideline respectively. See paragraph 4 for further details.

(c) **Coverage** – Trade Controls should set out the AI's methodology for assessing, monitoring and mitigating trade-related activities, including specific types of transactions, having regard to assessed risk levels. This methodology should take into account the suggested practices described in **Part 2 of Annex B** and include necessary information and documentation. Trade Controls should also take into account AI's own sanction policies which may specify various measures or restrictions in relation to sanction regimes in respect of particular countries, products or services.

(d) **Red Flags** – When developing their Trade Controls, AIs should take into account relevant red flag indicators. A non-exhaustive list of red flags indicators is provided in **Part 3 of Annex B**. AIs should consider assessing which red flags in Part 3 of Annex B are applicable, and may also adopt additional or different indicators or risk factors that are appropriate having regard to their own business coverage, scale of operations and particular scenarios. In order to identify concerns at an early stage, where possible and appropriate, red flags should be considered at the pre-relationship and pre-transaction levels. Relevant staff should also be made aware of, and be required to escalate red flags that are identified after the relationship has been established and/or after transactions have been carried out.

---

2 Specifically, sections 3, 4, 5, 9, 10 and 15 of Schedule 2 to the AMLO.

3 "FATF Risk-Based Approach Guidance for the Banking Sector and Money Laundering and Terrorist Financing Risk Assessment" dated 19 December 2014.

(e) **Review and Escalation Procedures** – Trade Controls should set out clear red flag review and escalation procedures. These should include higher levels of authority for trade transactions that have been identified with higher risk factors. They should also specify the suspicious transaction reporting mechanisms involving the money laundering reporting officer ("**MLRO**"). See paragraph 8 for further details.

(f) **Exception Reports** – AIs should make use of rule-based exception reports or detection scenarios to the extent reasonably practicable. See paragraph 7 and Part 2 of **Annex B** for further details.

(g) **Roles and Responsibilities** – Trade Controls should ensure clear division of roles and responsibilities and ownership of risks relating to critical functions.

(h) **Documentation** – Trade Controls should require decisions relating to trade transactions, workflow procedures and red flags to be documented appropriately for audit trail purposes, having regard to the record-keeping standards in Part 3 of Schedule 2 to the AMLO and Chapter 8 of the AMLO Guideline.[4] They should also include mechanisms to ensure that customer information, including applicable trade processes and relevant updates, is captured in the relevant AI's customer database, in order to facilitate the assessment and ongoing monitoring of customer activities.

(i) **Management Oversight** – AIs should involve senior management in the design and implementation of Trade Controls, as part of senior management's general oversight over ML/TF risk management. Reports that provide senior management a useful view of how trade-based money laundering risks are arising and being managed should form part of regular and ad hoc reporting requirements. Subject to the importance of trade-related activities in the AIs' operations, AIs may also consider placing trade-based money laundering within the remit of a regional or global committee that addresses financial crime and/or trade-related activities.

3.4 Additional recommended content for Trade Controls is set out in the paragraphs below relating to risk assessment, CDD, transaction screening and monitoring, suspicious transaction reporting, risk awareness and training.

3.5 Trade Controls need not be documented in a single set of policies and procedures, but they should be readily identifiable by and made known to relevant staff members who engage in trade-related activities.

Internal Escalation Procedures

3.6 Trade Controls should provide clear guidance on a good transaction review process. For reference, a sample review process is outlined as follows:

(a) "**Level 1**" review by trade processors with a good knowledge of international trade, customers' expected activity and a sound understanding of trade-based money laundering risks, who are responsible for assessing ML/TF risks in each transaction and escalating potentially suspicious transactions.

(b) "**Level 2**" review by staff with specialist expertise able to further assess the merits of an escalation from a Level 1 processor and the relevant suspicion itself. These staff members are likely to require extensive knowledge of trade-based money laundering risk and make appropriate use of third-party data sources to verify key information.

(c) A "**Level 3**" compliance / investigation team takes referrals from Level 2 processors. This team may conduct a further investigation to determine additional measures which may be required to mitigate a risk, and whether the obligation to make a

[4] Reference may be made to paragraph 3.8 of the AMLO Guidance for guidance on the documentation of risk assessments.

suspicious transaction report arises. Where there are unacceptable ML/TF risks, AIs should not process the transaction.

The sample review process is not intended to be prescriptive. AIs should tailor their own review process to their particular needs. Smaller operations are likely to require fewer stages of review due to the volumes of transactions involved and the nature of their businesses.

Communication, Update and Review

3.7 AIs should ensure that relevant staff in front line and operational units are made aware of Trade Controls and kept informed of updates. Communication between such staff is also important in relation to accounts and relationships generally (see paragraph 5.4).

3.8 AIs should also conduct periodic reviews of their Trade Controls to ensure they reflect current laws and regulations, business needs and (if applicable) industry trends.

3.9 AIs should conduct independent reviews on Trade Controls, including sample testing, to assess their effectiveness and adequacy. This review should be conducted by Compliance and Internal Audit, in accordance with the requirements of paragraphs 2.16 to 2.17a of the AMLO Guideline. External review may also be considered, depending on the risks of ML/TF and the size and nature of the AI's business.

3.10 Trade Controls should also address, where relevant, how staff should handle descriptions which are unclear or worded in a foreign language and/or non-Latin script as part of trade-related activities.

4 Risk Assessment and the Risk-based Approach

4.1 AIs should adopt a risk-based approach to CDD. This includes taking into account the four overarching risk factors of country, customer, product / service and delivery / distribution channel, as set out in Chapter 3 of the AMLO Guideline, together with any other relevant factors that come to an AI's attention in the context of their trade-related activities. In this respect, AIs should make reference to the typical trade-based money laundering typologies in **Part 1 of Annex B**, having regard to their business coverage, scale of operation and particular scenarios.

4.2 Due to the paper-based nature of many trade transactions and the limitations of automated transaction monitoring in a trade context (as to which, see paragraph 7.6), such risk assessments are comparatively reliant on the judgment of staff. Trade-related risk-assessments should therefore be carried out by well-trained processing staff, with appropriate supervision from experienced staff.

4.3 AIs should also make available appropriate tools to staff to conduct trade-related risk assessments. The precise tools that are appropriate for a particular AI or business line will depend on the nature of the relevant business and ML/TF risks involved. They may include products and services provided by reputable third party service providers. Such tools may be developed internally or obtained from reputable and reliable third parties.

4.4 Once a risk assessment has been carried out, AIs should apply the appropriate level of CDD corresponding to the assessed level of ML/TF risk, including enhanced due diligence for high risk customers, in accordance with Schedule 2 to the AMLO and Chapter 4 of the AMLO Guideline.[5] Risk assessments also inform the level and degree of transaction screening and monitoring conducted – see paragraphs 6 and 7 for further details.

[5] Reference to Chapter 12 of the AMLO Guideline should also be made in the context of private banking relationships, if applicable. Correspondent banking relationships are subject to the requirements in Chapter 11 of the AMLO Guideline.

5 Trade-related CDD Requirements

5.1 Knowing customers is a key part of the controls required to mitigate trade-based money laundering risks. CDD is particularly important for AIs to manage and monitor the risks associated with customers on an ongoing basis throughout the relationship.

5.2 AIs should have Trade Controls that clearly set out the coverage and use of appropriate CDD and other information collected in accordance with the AMLO and AMLO Guideline. This facilitates the assessment and identification of anomalies, and helps to manage the customer on-boarding process and applying risk mitigation measures, where appropriate.

5.3 Without limiting the scope of the AMLO or AMLO Guideline, key customer information related to trade-based activities that is collected may include, but is not limited to, the customer's:

(a) business nature, such as major products, jurisdictions and markets;

(b) delivery / transportation mode for goods or services;

(c) major suppliers and buyers;

(d) products and services to be utilised from the AI;

(e) anticipated account activities;

(f) anticipated major methods and terms of payment and settlement;

(g) internal customer risk assessment ratings by the AI;

(h) any previous suspicious transaction reports filed with relevant authorities, to the extent possible bearing in mind legal and regulatory constraints, including the need to avoid the risk of tipping-off; and

(i) other information from the relationship manager or other relevant staff.

5.4 Given the dynamic nature of the trade cycle and that customers' trade-related activities may change over the course of the business relationship, CDD information should be updated in accordance with section 5 of Schedule 2 to the AMLO and Chapter 4 of the AMLO Guideline. This will generally require an appropriate level of information-sharing between front line staff and staff in operational units during both the customer on-boarding and ongoing review processes.

5.5 Where anomalies regarding customer's trade-related activities are identified at any stage, AIs should consider obtaining further information to assess whether there may be a legitimate explanation to allay the concern. A situation that constitutes an anomaly may not necessarily give rise to, or elevate, the risk of trade-based money laundering. In particular, if there is a legitimate explanation for the anomaly, there may be no such risk implications.

5.6 AIs should ensure proper documentation and record keeping of both the initial CDD assessment and any updated information and explanations. This should include customer information, any decisions made, and any rationale for a decision.

6 Transaction Screening as Part of Trade-related Activities

Principles of Transaction Screening as Part of Trade-related Activities

6.1 Trade Controls should include policies and procedures for transaction screening and relevant alert handling procedures for trade-related activities.

6.2 These should:

(a) follow the guidance in paragraph 2 of the HKMA Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting (**HKMA Transactions Guidance Paper**) and Chapter 6 of the AMLO Guideline;

(b) include methodologies to detect specific trade-based red flags, common trade typologies and scenarios and sanctions. **Part 1 of Annex B** provides non-exhaustive guidance on typical typologies and the fields that should be screened and **Part 3 of Annex B** provides non-exhaustive examples of red flags; and

(c) include screening procedures that provide guidance on dealing with alerts relating to "hits" on particular companies, individuals, commodities, dual-use goods,[6] bills of lading / airway bills and countries.

Sanctions, Terror and High Risk Jurisdiction Lists

6.3 AIs are required by the HKMA to maintain a database of names, particulars of terrorist suspects and designated parties, which should consolidate the various lists that have been made known to it and with which the AI is bound to comply. In addition, AIs should ensure that their designated parties database and sanctioned jurisdictions list are updated in a timely manner. Further details of these obligations are set out in Chapter 6 of the AMLO Guideline and paragraph 2.3 of the HKMA Transactions Guidance Paper.

6.4 AIs should also be alert to persons and transactions associated with high risk jurisdictions and high risk goods / services. The concepts of "high risk jurisdiction" and "high risk goods / services" (or similar) should be properly stated in specific written guidance to staff, ideally within the Trade Controls**.** Trade Controls should also require a more in-depth investigation into the propriety and authenticity of such transactions.

Shipments[7] and "Dual-use Goods"

6.5 AIs should perform "voyage checks" and "port checks" for the purpose of managing ML/TF risks in transactions involving the shipment of goods using a risk-based approach. Appropriate circumstances for such checks may include, for example, where the shipment involves high risk jurisdictions or raises red flags, such as those set out in **Part 3 of Annex B**. These checks should be performed to help verify:

(a) the existence of the shipment, to help address the risk of fraud or ML/TF; and

(b) shipment routes, to help address the risk of sanctions violations or WMD proliferation.

6.6 In such cases, AIs should have regard to:

(a) information that may be available directly from customers or other transaction parties; and

(b) publicly available sources of information that are available at no or minimal direct cost, such as information available on the internet.

6.7 Where information or documents in relation to a shipment requested by AIs is not provided (or otherwise available), AIs should establish a process to follow up with the customer and take reasonable steps to obtain the relevant information and any necessary supporting documents.

---

[6] See paragraph 6.8 for further details in relation to dual-use goods.

[7] Where applicable, AIs should also consider whether similar (or other) checks may be appropriate for other modes of transporting goods, such as aviation and land transport (including road and rail).

6.8 "**Dual-use Goods**" are items that have both commercial and military or proliferation applications. Specialist knowledge is often required to determine whether or not goods have a dual use.

6.9 While this is a complex area, AIs should nevertheless have measures in place, as part of their risk-based systems and controls that can assist in the identification and escalation (for further review) of dual-use goods in trade transactions, taking into account other relevant red flags in a transaction. AIs should therefore consider what policies and procedures may be appropriate in relation to dual-use goods, having regard to the nature and scale of their trade-related activities, as a means to demonstrate effectiveness in this area.

6.10 A number of publicly available sources of information can be used to help identify dual-use goods. For example, for a list of goods of interest, AIs may refer to the "Dual-use Goods List" maintained under the Import and Export (Strategic Commodities) Regulations.[8]

Manual Screening to Supplement Automated Systems

6.11 Trade Controls should supplement automated screening with manual screening. AIs should also have procedures that utilise information gathered during the CDD process in screening, and capture new or amended information received through the life of a transaction.

Handling Alerts

6.12 As alerts arise, AIs should have Trade Controls to ensure appropriate handling and management of:

(a) alerts of possible matches from name screening; and

(b) transactions connected with sanctioned or high risk jurisdictions, or embargoed goods / services.

Reference may be made to paragraphs 2.8 to 2.11 of the HKMA Transactions Guidance Paper on transaction screening generally.

6.13 Relevant staff should:

(a) review the alerts or transactions concerned to check whether any suspicious or prohibited activities are involved and to determine whether the possible matches are genuine hits for further appropriate action;

(b) follow the AI's internal escalation procedures – see paragraph 3.6; and

(c) maintain a written record of the fact of, and the rationale for, the release of an alert concerning a potential name match or transaction. This should confirm that the staff member had in fact checked, for example, whether the particulars of the trade transaction and/or payment message(s) actually indicated the involvement of designated parties, sanctioned activities or other matters of concern to the AI. Further guidance on this subject is set out in paragraph 2.11 of the HKMA Transactions Guidance Paper.

[8] Please see the website of the Strategic Commodities Control System of the Trade and Industry Department of the Government Hong Kong at http://www.stc.tid.gov.hk/english/checkprod/sc_control.html.

7 Transaction Monitoring as Part of Trade-related Activities

Principles of Transaction Monitoring as Part of Trade-related Activities

7.1 The purpose of transaction monitoring is to alert AIs to activities which appear to be unusual or suspicious for further examination and investigation.

7.2 AIs should establish an effective transaction monitoring mechanism to identify unusual or suspicious trade-based activities. The scope and complexity of the monitoring process should be determined using a risk-sensitive approach. Reference may be made generally to contents of Chapter 3 of the HKMA Transactions Guidance Paper in this respect.

7.3 AIs should take into account the nature of their trade-related products and services, the common trade-based ML/TF typologies and red flags in designing appropriate trade-related monitoring mechanisms. A non-exhaustive list of typical typologies and red flags are provided in **Parts 1 and 3 of Annex B**. Staff should be made aware that trade-based money laundering techniques generally rely on collusion between the seller and buyer, since the intended outcome from the arrangements is often to obtain value in excess of what would be expected from an arm's length transaction. In certain cases, the collusion may arise where the buyer and seller are controlled by the same person.

7.4 AIs should periodically assess and review their transaction monitoring systems in the context of their trade-related activities, taking into account changes in business operations and developments in ML/TF methods. Paragraph 3.11 of the HKMA Transactions Guidance Paper provides further guidance.

7.5 Trade Controls should include senior management oversight over the development and implementation of the transaction monitoring system, in accordance with paragraph 3.7 of the HKMA Transactions Guidance Paper. Staff should collate key financial crime metrics and trends that are relevant to trade transactions for distribution to all relevant staff including senior management and frontline teams.

Manual Screening is a Crucial Supplement

7.6 AIs should be aware of the limitations of automated systems. In particular, owing to the complexity involved in trade-related activities, transaction monitoring involves a higher level of human effort and judgment for the effective identification of unusual or suspicious activities. Automated systems should only act as a "complement" to those efforts.

7.7 As with monitoring generally, AIs should determine the appropriate degree of automation based on the size, nature and complexity of its business on trade products and services. Paragraphs 3.6 to 3.9 of the HKMA Transactions Guidance Paper provide additional details regarding automated transaction monitoring.

8 Suspicious Transaction Reporting

Filing an STR As Soon As Possible

8.1 Chapter 7 of the AMLO Guideline and paragraph 4 of the HKMA Transactions Guidance Paper provide substantial practical guidance in relation to filing suspicious transaction reports ("**STRs**"). This applies equally in relation to suspicious transactions and scenarios encountered as part of trade-related activities. Where knowledge or suspicion arises, an STR should be filed with the Joint Financial Intelligence Unit ("**JFIU**") in a timely manner.

8.2 As with other types of transactions and scenarios, it may be appropriate to undertake further enquiries before an STR is filed. If the AI obtains what it considers to be a satisfactory explanation of the trade transaction or scenario, it may conclude that there are no grounds for suspicion and take no further action. In all cases, the steps taken should be balanced against the risk of tipping-off.

8.3 Where the AI's enquiries do not provide a satisfactory explanation of the relevant transaction or scenario, it may conclude that there are grounds for suspicion.[9] AIs should follow the JFIU's "SAFE" (ie Screen-Ask-Find-Evaluate) approach to identify suspicious activities for reporting.

8.4 AIs should always file an STR when required to do so under the relevant ML/TF legislation.[10] However, between the filing of the STR and receiving feedback from the JFIU, the AI may decide, upon further analysis, that there are no reasonable grounds to believe that the circumstances involve ML/TF under any applicable legislation, and that the relevant transaction and/or continued account operation or other dealings may therefore proceed.

Internal Reporting and the Role of the MLRO

8.5 AIs should ensure that reporting lines to the MLRO are as short as possible, with the minimum number of people between the staff with the suspicion and the MLRO, as required by paragraph 7.24 of the AMLO Guideline.

8.6 The MLRO and persons assisting the MLRO are expected to:

(a) consult relevant trade processing or other specialised staff in appropriate situations to assist the MLRO to assess escalated reports and otherwise discharge their responsibilities, but in no circumstances may such staff filter out such reports;

(b) undertake the following when assessing whether or not to file a STR in a potential trade-based money laundering situation:

(i) reviewing trade finance documents, for example, bills of lading and commercial invoices;

(ii) conducting company verifications and media searches;

(iii) conducting client account activity reviews;

(iv) reviewing existing CDD files and, where required, obtaining information from relationship management teams who may further reach out to customers to the extent possible, bearing in mind the risk of tipping-off; and

(v) reviewing the results of any available screening and monitoring processes; and

(c) based on the information obtained as part of 8.6(b), re-assess the customer risk and make adjustment to the risk rating, if appropriate.

9 Risk Awareness and Trade Specific ML/TF Training

9.1 Comprehensive risk awareness and training programs are an integral part of effective AML/CFT risk mitigation. Chapter 9 of the AMLO Guideline provides guidance on AML/CFT training generally. As part of this, AIs should ensure that relevant staff understand the phenomenon of trade-based money laundering, how it may arise in the context of the AI's business and related Trade Controls.

9.2 More specifically, AIs should ensure that key issues specific to trade-based money laundering are periodically and effectively communicated to relevant staff. This may include, for example:

[9] "Suspicion" is covered in detail in Chapter 7 of the AMLO Guideline.

[10] Namely, under section 25A of each of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) and Organized and Serious Crimes Ordinance (Cap. 455) and section 12 of the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575).

(a) typical trade transactions and structures, to ensure that key trade-related concepts, arrangements, documentation and parties are understood;

(b) typical typologies in relation to trade-based money laundering;

(c) the AI's Trade Controls, including recent or upcoming updates;

(d) emerging risks in trade-based money laundering;

(e) regulatory expectations drawn from guidelines, circulars, seminars and (if applicable) specific engagement with the AI;

(f) industry trends and best practices in combating trade-based money laundering;

(g) case studies and/or information sharing on trade-based money laundering; and

(h) common red flags.

9.3 AIs should identify and engage staff members who will require trade-based money laundering training. Relevant staff may include relationship managers, staff involved in selling products related to trade-related activities, the MLRO and trade operation teams. In addition to front line staff who are responsible for identifying and escalating potential trade-based money laundering, staff within control functions such as compliance, risk and internal audit may also require training. This list is not exhaustive and AIs may identify other staff that fit into this category.

9.4 Such persons may also be able to provide, or contribute to, training depending on their background, role and experience.

9.5 Role-based training should also be included for staff involved in day-to-day trade processes. Such staff may include, for example, relationship managers and trade-related operations teams. The goal of role-based training is to educate staff about the specific risks and responsibilities applicable to them, to assist in preventing, identifying, mitigating and reporting potential trade-based money laundering. For example, a document checker in trade operations will require greater in-depth training on irregular data that may be found on invoices, L/Cs and other trade finance-related documents, which they would be expected to handle on a day-to-day basis.

9.6 In this respect, trade-based money laundering training should be bespoke. Staff training should be refreshed at regular intervals and relevant training records should be properly retained.

Annex A – Typical L/C Transaction Structure

This Annex A illustrates the two key parts of a typical L/C transaction structure and provides guidance on who would typically constitute the "customer" for the purposes of the AMLO. This is intended as a guide only for illustrative purposes – transactions' structures (and terminology) vary and should be analysed according to the facts and circumstances that apply.

1 Issuing L/Cs

1.1 Key Features and Parties

L/Cs are issued to support the sale and purchase of goods. They effectively serve as a third-party guarantee of a buyer's obligation to pay and a means to ensure that the conditions of delivery are met.

More specifically, an L/C is an undertaking issued by a person (usually, but not necessarily, a bank) ("**Issuing Bank**"):

(a) for the account of the buyer of the relevant goods ("**Buyer**", also known as the "Applicant"), or for its own account;

(b) to pay the seller of the goods ("**Seller**", also known as the "Beneficiary") against the value of the draft and/or other documents; and

(c) on the condition that the terms and conditions of delivery are met.

L/Cs are usually subject to the "Uniform Customs and Practice for Documentary Credits" issued by the International Chamber of Commerce ("**UCP 600**"),[11] but may be documented otherwise.

Two additional parties to the initial stage of an L/C arrangement may include:

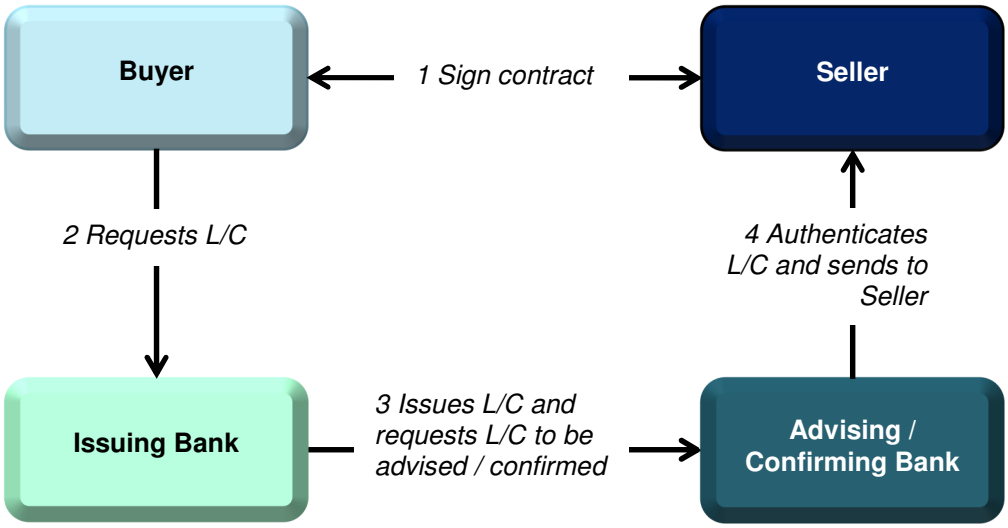
(i) the "**Advising Bank**" which authenticates the L/C to ensure that the L/C is genuine and tells the Seller that there is an L/C issued in its favour; and

(ii) the "**Confirming Bank**", which adds its own undertaking to pay the Seller if all the terms and conditions of the documents are complied with. It adds that undertaking at the request of the Issuing Bank. The Confirming Bank is often also the same bank as the Advising Bank. See paragraph 3 of this Annex A.

[11] International Chamber of Commerce Publication No. 600.

1.2 Flow Diagram of a Typical L/C Issuance

The following diagram illustrates the basic flow of an L/C issuance, with a word description below.



The following steps are involved:

Step 1 The starting point is a sales contract between the Buyer and the Seller. The Buyer and Seller conclude that contract and agree to use an L/C as the method of payment.

Step 2 The Buyer initiates a request to the Issuing Bank to issue an L/C to the Seller on the Buyer's behalf. In many cases, the Buyer is an existing customer of the Issuing Bank and is located in the same jurisdiction, but this is not necessarily always the case.

Step 3 The Issuing Bank issues the L/C and asks the Advising Bank to advise, and/or the Confirming Bank to confirm, the L/C to the Seller.

Step 4 The Advising Bank authenticates the L/C and sends it to the Seller.

1.3 Typical Customer Analysis

In the above transaction structure, the following parties would generally be treated as the "customer" for the purposes of the AMLO:

(a) For the **Issuing Bank**, the customer would generally be the **Buyer**.

(b) For the **Advising Bank**, the customer would generally be the **Seller** and/or the **Issuing Bank**, depending on the facts.

(c) For the **Confirming Bank**, the customer would generally be the **Seller** and/or the **Issuing Bank**, depending on the facts.

2 Presenting and Settling Letters of Credit

2.1 Key Features and Parties

Once the Seller dispatches the goods to the Buyer or some other designated person through its carrier, the presentation and settlement process starts.

In short, this involves documents flowing toward the Buyer and funds flowing to the Seller through three key parties:

(a) the Seller's bank ("**Negotiating Bank**"), which reviews the documents provided by the Seller ("**Delivery Documents**") and, if they are in order, advances funds to the Seller and forwards the Delivery Documents to the Issuing Bank;

(b) in certain cases, a bank nominated by the Issuing Bank (called the "**Reimbursing Bank**"), which acts as the Issuing Bank's paying agent to honour claims submitted by the Negotiating Bank and reimburse payments made to the Seller; and

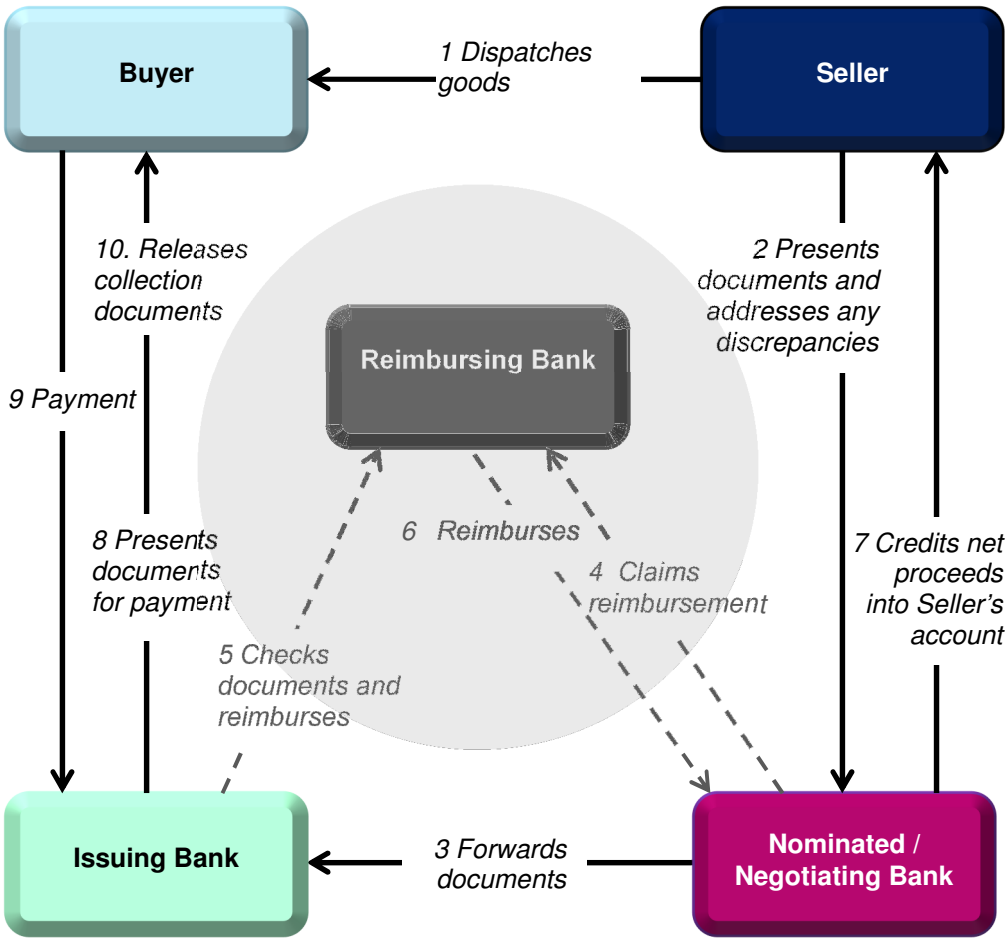
(c) the Issuing Bank, which presents the Delivery Documents to the Buyer and requests funds to repay the Reimbursing Bank, or debits an account of the Buyer.

In some cases, the Negotiating Bank waits for funds from the Reimbursing Bank, and in others, it pays immediately upon being satisfied that the Delivery Documents are accurate and complete.

Some parties adopt much simpler presentation and settlement arrangements – for example, in certain cases, there is no Reimbursing Bank and the Issuing Bank pays the Negotiating Bank directly.

2.2 Flow Diagram of a Typical Presentation and Settlement Process

The following diagram illustrates the basic flow of a typical presentation and settlement process, with a word description below.



The following steps are involved:

Step 1 The Seller dispatches the goods to the Buyer's country.

Step 2 The Seller presents the drafts and/or documents to the Nominated Bank. The Nominated Bank (nominated as the "Negotiating Bank") checks the documents against the terms and conditions of the L/C. If there are any discrepancies, the Bank will contact the Seller and either have them remedied or addressed via an indemnity.

Step 3 The Nominated Bank forwards the drafts and/or documents to the Issuing Bank for checking.

Step 4 The Nominated Bank issues a statement that the documents comply with the terms and conditions of the L/C and claims reimbursement from the Reimbursing Bank.

Step 5 The Issuing Bank checks the documents against the L/C terms and conditions and reimburses the Reimbursing Bank if the documents are in order.

Step 6 The Reimbursing Bank pays the Nominated Bank against the Nominated Bank's statement and a back-to-back reimbursement authority from the

Issuing Bank.

Step 7 The Nominated Bank credits the net proceeds into the Seller's account.

Step 8 The Issuing Bank presents documents to the Buyer for payment.

Step 9 The Buyer pays the Issuing Bank.

Step 10 The Issuing Bank releases documents to the Buyer to enable the Buyer to collect the goods.

2.3 Customer Analysis

In the above transaction structure, the following parties would generally be treated as the "customer" for the purposes of the AMLO:

(a) For the **Issuing Bank**, the customer would generally be the **Buyer**.

(b) For the **Reimbursing Bank**, the customer would generally be the **Issuing Bank**.

(c) For the **Negotiating Bank**, the customer would generally be the **Seller**.

3 Further Arrangements

There may be a wide range of other arrangements involved in an L/C structure.

For example, L/C structure can also involve discounting arrangements. In such cases, a bank (called the "**Discounting Bank**") agrees to pay the Seller for the goods earlier than the Buyer is willing to do so.

The Discounting Bank generally pays the Seller the approved amount (generally, the amount of the invoice or the L/C minus a "discount"). The Discounting Bank effectively purchases the accepted draft, and is reimbursed for this "purchase" by collecting the moneys on the maturity date.

The "customer" of a Discounting Bank for the purposes of the AMLO depends heavily on the facts and circumstances. In a simple scenario, where the relevant relationship is solely between the Discounting Bank and the Seller, the "customer" of the Discounting Bank would be the Seller.

4 Structures Vary

Importantly, structures and arrangements vary in practice. For example, certain banks may perform:

(a) multiple roles for the same customer for convenience or for relationship-building purposes; or

(b) functions for another party within the trade finance process – for example, an Issuing Bank may request another bank to act as the Advising Bank.

In this regard, trade finance does not always occur on "textbook" terms.

This means that it is important to analyse each arrangement by reference to its own particular circumstances when considering where the customer relationship lies.

Annex B – Suggested Typologies, Best Practices and Red Flags

Introduction

This Annex B contains non-exhaustive lists of indicia that could highlight trade-based money laundering, as well as suggested best practices for AIs to manage their trade-based money laundering risks, in addition to those outlined in the main body of the Guidance Paper.

This Annex B is structured as follows:

Part 1 – Typical trade-based money laundering typologies

Part 2 – Suggested best practices

Part 3 – Suggested red flags

These are suggestions only, and should be considered for implementation by individual AIs on a risk-based approach, having regard to the nature and scale of their business and particular scenarios.

It should be borne in mind that there are many legitimate trade transactions that involve, for example, complex shipping routes involving multiple jurisdictions or complex payment mechanisms. Understanding the commercial purpose of any transaction is a key requirement. Ultimately, trade-based money laundering typically involves the use of trade to disguise the proceeds of crime and move value. Conversely, greater transparency in a customer's affairs reduces the risk that the customer is linked to trade-based money laundering, or at least allows the AI to avoid or mitigate that risk.

Part 1 - Typical Trade-based Money Laundering Typologies

Typology and indicative description	Information that may be relevant to assessing ML/TF risk
1. Over-invoicing or Under-invoicing. *A mismatch in the invoice value and the fair market price.* ***Over-invoicing**: By invoicing the goods or service at a price above the fair market price, the seller is able to receive value 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.* ***Under-invoicing**: By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer, 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.*	▪ Product taxonomy (i.e. table of product categorisation) ▪ Category of goods ▪ Goods description ▪ Unit price of goods ▪ Quantity of goods ▪ Market price of goods

Typology and indicative description	Information that may be relevant to assessing ML/TF risk
2. Over-shipping or Short-shipping. *A mismatch in the invoiced quantity of goods and the quantity of goods in fact shipped. By over or under-shipping the invoiced quantity of the goods, the buyer or seller (as the case may be) gains excess value when the payment is made.*	▪ Product category ▪ Product description ▪ Unit price ▪ Units
3. Fictitious Trades. *Also known as "ghost shipping" or "phantom shipping". A seller may not ship any goods at all, but simply collude with a buyer to ensure that all shipping and customs documents associated with the trade.*	▪ Transaction date ▪ Quantity ▪ Unit price of goods ▪ Presence of transport document ▪ Validity of transport document
4. Use of Shell or Fictitious Companies. *These companies are incorporated but have no significant assets or operations. Often used as part of opaque transaction structures that obscure the flow of funds and hide the transfer of value from AIs.*	▪ Company name ▪ Beneficial owners ▪ Name of counterparty ▪ Shipper, consignee and notifying party on the transport document ▪ Customer and counterparty due diligence information
5. 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, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services.*	▪ Transaction date ▪ Transactional amount ▪ Product description ▪ Invoice number ▪ Presence of account information of other banks on the invoice ▪ Presence of bank chops on invoice

Typology and indicative description	Information that may be relevant to assessing ML/TF risk
6. Black Market Trades *Also commonly referred to as "black market peso exchange arrangements" (or similar), this usually involves the domestic transfer of funds (that need laundering) to pay for goods on behalf of a foreign importer.* *A typical black market trade may involve, for example:* ▪ *a money launderer selling funds at a discount to a foreign money broker;* ▪ *the money broker integrating these funds into the financial system, often via smaller bank accounts to avoid raising suspicion (also known as "smurfing");* ▪ *the money broker paying for goods on behalf of a foreign buyer; and* ▪ *the foreign buyer selling the goods to repay the money broker.* *In such instances, there may not be any fraudulent documents involved.*	▪ Product description ▪ Product category ▪ High-value equipment and machinery ▪ Counterparty location ▪ Location of counterparty's bank ▪ Customer and counterparty due diligence information ▪ Bank account(s) activities

Part 2 – Suggested Best Practices

Trade Controls	▪ Implementing Trade Controls that provide specific guidance on AML/CFT matters in the context of trade. ▪ Ensuring Trade Controls contain appropriate procedures for handling exception reports and red flags, as well as a procedure for escalating such reports, setting out clear lines of escalation. ▪ Considering ML/TF risks specific to their trade-related activities and identifying the customers and transactions that present higher risk at various stages of relevant trade transactions. ▪ Requiring relevant staff to undertake appropriate CDD (see suggested practices under "CDD Procedures" below) and make use of CDD information to assess whether the trade transactions are commensurate with the customer's background. ▪ Implementing reports and systems (such as exception reports and detection scenarios) that capture the transaction pattern or activities of customers, such as the following examples: ✓ Transactions involving high-risk jurisdictions ✓ Transhipment involving sanctioned countries ▪ Requiring relevant staff to conduct appropriate screening (see suggested practices under "Screening Techniques" below). ▪ Ensuring that red flags are regularly updated and easily accessible to staff.
CDD Procedures	▪ Documenting an internal assessment framework to assess who is a "customer" for the purposes of the AMLO in a given trade transaction or other trade-related scenario. ▪ Assessing customer's trade-based money laundering risk based on their anticipated trade-related activities, upon application for relevant services. Examples of factors for consideration may include types of goods, trade volumes, counterparties and shipment methods. ▪ In addition to the assessment of customer's trade-based money laundering risk upon establishment of the relationship, assessing, on a case-by-case basis or in relation to a particular category of trade transactions, who is the AI's "customer" for the purposes of the AMLO. ▪ Documenting a formal consideration of trade-based money laundering risk in applicable Trade Controls for particular types of trade transactions and categories of customers. ▪ Considering and evidencing the assessment of trade-based money laundering risks related to particular customers and trade transactions. ▪ Obtaining and reviewing underlying trade documentation wherever possible. ▪ Where reasonably practicable, obtaining and using reliable and up-to-date pricing information for relevant commodities and perform price checks on a sampling basis. AIs may have regard to publicly available sources of pricing information for commodity-related transactions. Given the difficulty in obtaining market prices for certain other goods, such as garments and household items, AIs should simply make further enquiries where the pricing of the goods appears to be manifestly unusual, or there are other ML/TF risks, such as red flags. By way of example, the pricing of a t-shirt could be seen as "manifestly unusual" and warrant further enquiries where the invoice states the unit cost is USD100, where the normal unit cost would be in the order of USD5. AIs may wish to consider establishing acceptable price variance thresholds (which could accommodate different thresholds for different types of underlying goods/commodities) and escalation procedures when the thresholds are exceeded.

	▪ Ensuring trade processing staff keep up–to-date with emerging trade-based money laundering risks (see also under "Expertise, Awareness and Training" below). ▪ Requiring processing teams to escalate suspicions for investigation as soon as possible, having regard to internal escalation procedures.
Screening Techniques	▪ Identifying and screening all relevant parties to a transaction and other information contained within trade documents against applicable sanctions lists. ▪ Screening for and recording in relevant systems information on all relevant fields to a transaction, such as, for example: ✓ Counterparty name(s) and location(s) ✓ Counterparty bank(s), their capacity in the transaction, and location(s) ✓ Customer name(s) including individuals and companies ✓ Carrier / charter / agent ✓ Consignee ✓ Country of origin ✓ Description of goods / commodities ✓ Freight forwarders and shipping companies ✓ Originating and recipient entities of the goods (ie importer and exporter) ✓ Shipper, consignee and notification party on transport documents ✓ Shipping route (such as the port of loading, port of discharge, port of transhipment, etc.) ✓ Vessel name(s) ✓ Flag of vessel ▪ Investigating hits before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and clearly documenting the rationale for any decisions made. ▪ Using reliable third party data sources where appropriate to verify the information given in trade documentation, such as L/Cs and bills for collection, and in circumstances where credit lines are provided, or otherwise facilitated through open account trades, such as invoice financing, pre-shipment financing, inventory financing. ▪ Appropriately prioritising the review of certain types of potential matches following analysis of previous sanctions alerts. ▪ Validating key information where possible, such as shipping container numbers. ▪ Using manual screening and review procedures to supplement any automated screening as part of trade processing procedures. ▪ Ensuring new or amended information about a transaction is captured and screened. ▪ Re-screening for potential sanctions matches when appropriate – for example, at the key stages of a transaction.[12]

[12] Members may refer to The Wolfsberg Trade Finance Principles (2011) publication, or other industry or regulatory guidance, as appropriate.

Expertise, Training and Awareness	▪ Employing staff involved in CDD, screening and review in relation to trade transactions (such as 'Level 1' trade processors) with good knowledge of international trade and customers' expected activities and a sound understanding of trade-based money laundering risks. ▪ Employing staff responsible for reviewing escalated transactions with substantial knowledge of trade-based money laundering risks. ▪ Making available detailed guidance for relevant staff on what constitutes a potentially suspicious transaction, including indicative lists of red flags. ▪ Providing tailored training that raises staff awareness and understanding of trade-based money laundering and sanctions risks. Such training utilises appropriate guidance from regulators and industry bodies like the HKMA, Wolfsberg Group, APG, etc. ▪ Making use of relevant FATF, regulatory and industry publications to raise awareness of emerging risks amongst relevant staff. This may include relevant international publications.
Assurance	▪ Ensuring regular, periodic quality assurance work is conducted by suitably qualified and experienced staff who assess the judgments made in relation to trade-based money laundering risk and potentially suspicious transactions. ▪ Where possible, conducting a review to ensure that all red flag controls at the pre-processing stage are working effectively. ▪ Expertise in trade-based money laundering also being held in a department outside of the trade finance business (e.g. compliance) so that independent decisions can be made in relation to further investigations.
Dual-use Goods	▪ Implementing policies and procedures that are appropriate in relation to dual-use goods, having regard to the nature and scale of the AI's trade-related activities. ▪ As part of any such policies and procedures that are implemented, referring to the "Dual-use Goods List" maintained under the Import and Export (Strategic Commodities) Regulations made under the Import and Export Ordinance (Cap. 60).

Part 3 – Suggested Red Flags

The following is a non-exhaustive list of red flags that could highlight trade-based money laundering. These should be considered for implementation by individual AIs on a risk-based approach, having regard to the nature and scale of their business and particular scenarios.

In relation to suggested red flags that refer to particular percentages or other thresholds, each AI should consider the most appropriate percentages or other threshold that addresses the relevant trade-based money laundering risk, based on the AI's internal risk assessment for that product type, transaction or customer.

A Customer Red Flags

(a) Uncommon transaction structure or overly complex transaction structure without a clear and legitimate commercial purpose or some reasonable justification.

(b) The transaction is not commensurate with known customer profile, structure or business strategy. In a trade-based money laundering 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 customer has no experience in the goods in question, or the size or frequency of the shipments appear inconsistent with the scale of the customer's regular business activities (e.g. a sudden surge in transaction size).

(c) The customer significantly deviates from their historical pattern of trade activity (i.e. in terms of value, frequency or merchandise) with dubious pricing of goods and services.

(d) The customer or parties have suspicious addresses. For example different transacting businesses may share the same address or the businesses only provide a registered agent's address.

(e) The customer reacts aggressively to know your customer questions or tries to force the AI to take CDD shortcuts by citing time pressures.

(f) The customer refuses any form of contact or communication with the AI, without a valid reason for that refusal.

(g) The customer is overly keen to waive discrepancies.

(h) The customer offers to pay unusually high fees to the AI.

(i) The bank is approached by a previously unknown party whose identity is not clear, who seems evasive about its identity or connections, or whose references are not convincing, or payment instructions are changed at the last minute.

B Documentary Red Flags

(a) 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 of the goods shipped.

(b) Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped.

(c) There are substantial discrepancies in merchandise descriptions, e.g. quantities, weights.

(d) Obvious over or underpricing of goods (that is, significant discrepancies appear between the value of the goods reported on the invoice and the known fair market value of the goods). In a trade context, where goods are highly overvalued, the importer could be moving funds out of their country. Conversely, where the goods are highly undervalued, the exporter could be moving funds out of its country.

(e) Obvious misrepresentation of the quantity of goods shipped. The contract value is unusually high for a party.

(f) Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

(g) The transaction involves the use of repeatedly amended or frequently extended L/C.

(h) The documents show excessively amended terms.

(i) The documents contain non-standard clauses or phrases or have other unusual characteristics.

(j) There are dubious unauthorised alterations or amendments to the documents.

(k) The beneficiary or applicant refuses to provide documents to prove shipment of goods (indicates possible phantom shipping or multiple invoicing).

(l) There are other dubious indicators such as unusual codes, markings or stamps on the monetary instruments (e.g. drafts or bills of exchange, or future dated bills of lading, and transaction under L/C without proper transport document or document evidencing shipment / delivery of goods).

(m) There are indications that the descriptions of the goods are coded or disguised.

(n) The customer requests (a) an L/C without calling for a 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.

(o) The transaction is without transport documents evidencing movement of goods.

(p) The bill of lading describes containerised cargo but without container numbers or with sequential container numbers.

(q) There are indications that documents have been re-used.

(r) There are indications of double invoicing.

(s) The invoice shows "Other/Undefined" charges as an unreasonably high percentage of total transaction value.[13]

(t) A documentary credit if overdrawn by more than an unreasonably high percentage of the original value

(u) The goods in respect of a documentary credit are over shipped by an unreasonably high percentage of the original quantity.

(v) An L/C is dated later than its date of presentation.

(w) The description of goods on the transport documents (if any) cannot be linked to the document terms and / or the actual invoice.

(x) The customer re-submits a document rejected earlier as a result of financial crime risk concerns.

(y) The non-negotiable bill of lading is consigned 'to be advised between applicant and beneficiary' (consignment should be to a named party).

(z) The customer makes a trade-related claim on a stand-by L/C before or a short period of time after its issuance.

(aa) 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 Red Flags

(a) The transaction structure is designed to conceal information or make it difficult for AIs to obtain certain information or the true nature of the transaction. This may include indications that a shipment is structured to disguise proliferation risks.

[13] The percentage that constitutes "unreasonably high" should be determined by the AI in accordance with the criteria set out in the introduction to this part.

(b) The transaction involves round-tripping or circular transactions.

(c) The transaction involves an uncommon or complicated movement of goods and/or third parties without an obvious purpose.

(d) The method of payment appears inconsistent with the risk characteristics of the transaction.

(e) The shipment does not make economic sense, takes an uneconomical shipping route, or the shipping route is unclear.

(f) The mode or method of shipping is unclear.

(g) The customer has unusually frequent round dollar transactions.

(h) The transaction involves the use of front or shell companies without a clear and legitimate commercial purpose or some reasonable justification.

(i) The transaction involves sanctioned entities.

(j) The transaction route involves high-risk jurisdictions or the trade transaction otherwise involves high risk jurisdictions.

(k) The commodity is trans-shipped through one or more jurisdictions for no apparent economic or other logistical reason.

(l) The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction, or other indications of possible black market peso exchange arrangements.

(m) The transaction involves an unusually high number of intermediaries, too many or unnecessary parties, or transferable letters of credit.

(n) 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.

(o) Documents such as an L/C received through unverified channels such as unauthenticated SWIFT message.

D Commodity Red Flags

(a) The type of commodity being shipped is designated as “high risk” for trade-based money laundering activities (e.g. precious metals and stones).

(b) The type of commodity being shipped appears inconsistent with the exporter or importer’s regular business activities.

(c) The commodity is shipped to (or from) a jurisdiction designated as “high risk” for ML/TF activities.

(d) Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity’s fair market value.

(e) The commodity includes dual-use goods.

E Vulnerable Goods Red Flags

The transaction involves goods vulnerable to trade-based money laundering, such as:

(a) gems;

(b) jewellery;

(c) cigarettes and other tobacco products;

(d) consumer electronics and home appliances;

(e) telephone cards and other stored value cards;

(f) precious metals;

(g) military goods and war material (these include items such as arms, ammunition, bombs, missiles, sensor integration equipment, armoured vehicles, electronic

equipment, laser systems, flying objects, tear gases and other irritants, certain components used for the production of arms and software developed for the use of war materials); or

(h) obvious dual-use goods, having regard to the “Dual-use Goods List” maintained under the Import and Export (Strategic Commodities) Regulations made under the Import and Export Ordinance (Cap. 60).