AML/CFT INDUSTRY PARTNERSHIP

Best Practices for Countering Trade Based Money Laundering

May 2018

Contents

1. INTRODUCTION

i) In April 2017, the Monetary Authority of Singapore ("MAS") and the Commercial Affairs Department ("CAD") of the Singapore Police Force launched a government-industry partnership to strengthen Singapore's resilience against financial crime.

ii) The Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership ("ACIP") brings together selected industry participants, regulators, law enforcement agencies and other government entities to collaboratively identify, assess and mitigate the key money-laundering, terrorism financing and proliferation financing (ML/TF/PF) risks faced by Singapore. ACIP also enhances the detection and mitigation of trans-national risks arising from Singapore's position as an international financial centre and trade hub.

iii) ACIP comprises a steering group, supported by working groups, which will consider specific risk areas and topics, including trade finance, relevant to money-laundering, terrorism financing and proliferation financing ("ML/TF/PF"). The steering group comprises eight local and foreign banks.

iv) As part of the ACIP initiative, a working group was set up to look into Trade Based Money Laundering ("TBML"). Banks (specifically those with a focus on trade finance business), regulators, law enforcement agencies and professional services organisations were invited to share and contribute to the TBML Working Group.

1.1. BACKGROUND

i) International trade is an attractive medium for money launderers to transfer large values across borders, owing to its significant volume and value. Trade and trade finance transactions can be exploited for ML, TF and PF. As a trade and transportation hub, Singapore is particularly vulnerable to TBML.

ii) Significant concerns relating to ML, TF and PF risks in trade (collectively known as "TBML risks" in this paper) have been highlighted by law enforcement and supervisory authorities, and organisations such as the Financial Action Task Force ("FATF"), the Asia/Pacific Group on Money Laundering ("APG"), the Bankers Association for Finance and Trade ("BAFT") and the Wolfsberg Group.

1.2. OBJECTIVES

i) This paper aims to provide practical guidance to implement the standards stipulated in MAS guidance on Trade Finance and Correspondent Banking published in October 2015[1] and the Wolfsberg Guidelines[2].

ii) The contents of this paper do not modify or supersede any applicable laws, regulations and requirements. They should be applied in a risk-based and proportionate manner, taking into account the risks posed by the customers, and the nature and complexity of the business of each bank.

1.3. METHODOLOGY

i) This Paper outlines the leading practices noted in the market around the identification of Trade Based Money Laundering ("TBML").

ii) Best practices were collated through a series of discussions and written contributions from these members of the Working Group. In addition, the various practical challenges faced by banks were also discussed and considered by the TBML Working Group.

[1] Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking
[2] The Wolfsberg Group, ICC and BAFT - Trade Finance Principles (2017)

1.4. TERMINOLOGY

i) TBML: TBML is the process of disguising the proceeds of crime and moving value or money through the use of trade in an attempt to legitimise their illicit origin[3].

1.5. SCOPE

i) A bank may finance a trade transaction:

a) Using products such as letters of credit, where trade related documents (such as invoices, transport documents) are sent through the bank, which may then be examined by the bank for consistency with the terms of the trade transaction[4]. In such a case, the bank will have information on the transaction as well as the parties involved in the transaction. This is referred to as documentary trade; or

b) Via trade loans, receivables financing or payables financing where a bank may not have access to documentation. This is referred to as open account trade. In such cases, a bank may not receive underlying documentation and may have little information on details of the transaction or parties involved.

ii) This paper provides recommendations on best practices and controls that may be implemented by a bank to combat TBML through documentary trade and high-level guidance on controls for open account trades.

iii) Whilst this Paper focuses on ML/TF/PF risks in a trade finance transaction and TBML controls, a bank needs to ensure that the sanctions risks associated with trade finance are equally and jointly considered. A bank should ensure that the necessary controls to mitigate Sanctions risks associated with such transactions are implemented and monitored.

2. GOVERNANCE AND MANAGEMENT OVERSIGHT

i) This section incorporates key considerations and controls in respect of good governance and management oversight, with focus on the role of senior management.

ii) Governance and management oversight is a wide topic. However, for the purposes of this Paper, guidance is provided on five key areas: Risk Assessment; Roles and Responsibilities; Management Oversight in Trade Finance Business; Independent Assurance and Testing; and Internal Reporting and Role of the Money Laundering Reporting Officer ("MLRO").

2.1. RISK ASSESSMENT

i) The FATF Guidance for a Risk-Based Approach – The Banking Sector (October 2014)[5] indicates that a bank must conduct periodic risk assessments to determine the extent of its vulnerabilities to ML/TF/PF risks. The guidance states that the risk assessment 'forms the basis of a bank's Risk-Based Approach ("RBA")', and the scale and scope of the assessment should be 'commensurate with the nature and size of the financial institutions' businesses'. Depending on the nature of the banking activity, the parameters to consider may be varied. The assessment results should complement information from internal or external sources including national risk assessments[6] and emerging typologies publications in determining possible changes to existing policies, procedures, measures and controls.

[3] FATF: Trade Based Money Laundering (June 2006)
[4] The Wolfsberg Group, ICC and BAFT - Trade Finance Principles (2017)
[5] FATF Guidance for a Risk-Based Approach – the Banking Sector (October 2014)
[6] FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (February 2013)

ii) The MAS Notice 626 and related Guidelines for the Banking Sector (as well as equivalent Notices/Guidelines for other financial industry sectors) set similar expectations on the need for a bank to periodically conduct enterprise-wide risk assessments ("EWRA") to assess such ML/TF/PF vulnerabilities, including for trade finance activities. Such risk assessment should be performed at least every two years.

iii) The risk assessment could be undertaken as part of a bank's AML/CFT EWRA or as a standalone risk assessment for its trade finance business. The risk assessment should have a clearly defined methodology.

iv) The risk assessment should consider both qualitative and quantitative factors. A qualitative assessment should help a bank ascertain whether a bank has implemented sufficient controls to address its regulatory obligations and manage the inherent risk in its trade finance business. Quantitative assessment should assist the bank in determining its inherent risk within the trade finance business. Non-exhaustive examples are provided below in Section 2.1(ix) on data or information the bank may use to measure its inherent risk in a quantitative manner.

v) The risk assessment should consider the following risk components, where relevant to trade finance:

a) Governance and oversight;

b) KYC and CDD;

c) Ongoing monitoring;

d) Name and sanctions screening;

e) Suspicious transactions reporting ("STR");

f) Record keeping and data management; and

g) Staff training.

vi) For each of the areas appended above in Section 2.1(v), the risk assessment should address the following elements:

a) inherent risk;

b) mitigating controls; and

c) residual risk.

vii) To assess its risk exposure, a bank should evaluate and measure risks based, at least, on the following categories:

a) Customers: The customer risk rating methodology should consider risks such as on-boarding channel risks, business and occupation risk, geographic risk, client relationship risk, transparency risk and behavioural and transactional risk. The risk of the products utilized by the client's should also feed into the client risk rating methodology.

b) Products or services: The product risk rating methodology should consider factors such as, but not limited to, product transparency, complexity, third party reliance and risk, speed of settlement, usage of cash or cash equivalent, cross border movement of funds and transaction channels used.

c) Transactions: The bank should consider the effectiveness of its controls to monitor, detect and address any transactions related red-flags and issues. These include, having in place controls to assess the nature of the transactions with regard to the underlying goods or products to the transactions that are financed or intermediated by the bank, source of funds (for example, whether they are from related or otherwise third or unrelated parties), mode of payments (for

example, cycle of payment that seems anomalous, cash payments or through other precious stones and metals).

d) Delivery channels: The bank should consider the effectiveness of its controls to monitor, detect and address any risks from the transaction channels, which may for example, involve third party payments, non-face-to-face relationships or transactions or payment from or to anonymous party.

e) Geography: The bank should consider the effectiveness of its controls to monitor, detect and address any risks posed by the jurisdictions of its customers or flow of the transactions facilitated by the Bank, whether directly or indirectly. This should include, inter alia, having in place controls to assess the typical flows of its customers' transactions, jurisdictions to which the trade transactions have nexus to, and whether the jurisdictions are subject to sanctions, embargos or similar measures issued by, for example, the United Nations, or are known to have a weak AML/CFT regime.

Inherent Risk Assessment:

ix) A non-exhaustive list of quantitative TBML risk factors that a bank may consider include:

a) Number of customers or accounts conducting trade transactions;

b) The value and volume of trade transactions;

c) Number of customers, accounts, value and volume of trade transactions held or conducted by high risk customers;

d) Number of customers or accounts incorporated or have operations in high risk countries or high risk industries conducting trade transactions;

e) Number of customers;

f) The value and volume of trade transactions to or from high risk countries or high risk industries;

g) Number of customers or accounts on-boarded in the last 12 months conducting trade transactions;

h) The value and volume of transactions conducted by customers or accounts on boarded in the last 12 months;

i) Number of customers or accounts transacting in high risk products (product risk is as identified pursuant to the Bank's product risk rating methodology);

j) The value and volume of transactions relate to high risk trade products;

k) Number of alerts raised on unusual transaction pattern related to TBML;

l) Number of STRs raised on suspicion of TBML;

m) Number of correspondent banking relationships in high risk countries; and/or

n) The value and volume of trade transactions with correspondent banking relationships in high risk countries.

Mitigating Controls Assessment:

x) In order to assess the mitigating controls, a bank should maintain an updated inventory of controls mapped to the inherent risks identified. Subsequently, these controls should be tested against policies and

procedures and for their effectiveness to ensure they are adequately mitigating the risks identified through the inherent risk assessment.

Residual Risk Assessment:

xi) Based on the inherent risk rating, the assessment of mitigating controls and effectiveness of controls tested, a bank should determine a residual risk rating.

xii) Upon determining the residual risk rating, the bank should put in place a plan to manage such residual risk and to address any gaps assessed in its controls during the risk assessment exercise.

xiii) The completed risk assessments and supporting information should be well-documented and retained by banks in accordance with the local record keeping requirements stipulated under the relevant Anti-Money Laundering/Combating the Financing of Terrorism ("AML/CFT") Notices and Guidelines.

Best Practices

Inherent Risk Assessment:

The assessment of inherent risk can be conducted by administering questionnaires for qualitative risk factors, and by extracting quantitative data from the relevant bank systems. A bank should be prudent about the threshold for the quantitative risk factors based on its risk appetite and providing risk weights to both the qualitative and quantitative factors.

The information gathered should be populated against the ML/TF inherent risk assessment questionnaire to calculate the Bank's inherent risk. The ML/TF inherent risk assessment questionnaire should cover critical areas of the Bank's business (for example, customers, countries, products, services, transactions and delivery channels) and consider the operational and regulatory risk factors that should be taken into account when assessing the robustness of the TBML programme.

Mitigating Controls Assessment:

To assess the mitigating controls, the bank could create an obligation register based on regulatory expectations and industry best practice. The obligation register should be mapped to policies and procedures, TBML red flags and typologies. Existing controls should be mapped to this register, which will enable identification of control gaps, if any.

The controls that are mapped should be tested for effectiveness. Banks should consider the following while assessing control effectiveness:

1. Review of the Bank's policies and procedures, to identify any gaps between the policies and regulatory requirements;
2. Walkthroughs with the business and operations teams to identify if the policies and procedures are being operationalised effectively; and
3. Sample testing against key control indicators and control sample testing thresholds (the number or percentage of fails a bank is prepared to accept before it could potentially impact the residual risk rating of the process).

The controls in place should be periodically reviewed and tested for effectiveness and whether any change in the inherent risk of the business or residual risk necessitates enhancement of such controls.

2.2. ROLES AND RESPONSIBILITIES

i) The "three lines of defence" model, defined in the Guidelines to MAS Notice 626, is important in assessing, managing and mitigating TBML risks in trade finance. The three lines of defence are:

a) First line of defence: Front office or the business function including relationship management, sales and product team, front office assurance, trade processing function with reporting lines to the front office, and/or trade operations function;

b) Second line of defence: Compliance function which is independent of front office; and

c) Third line of defence: Internal audit or equivalent functions.

Best Practices

A bank should formalise the ownership of policies, procedures and processes between the relevant lines of defence and preferably consider having a RACI (Responsible, Accountable, Consulted, Informed) matrix in place for added clarity on roles and responsibilities. It is good practice to have duly defined roles and responsibilities of each line of defence.

ii) First line of defence:

a) Front office staff should have good knowledge of their customers, including, but not limited to, the customer's business, its trading profile across different geographies, sources of raw materials, manufacturing locations, location of their suppliers and customers, and where appropriate, identify key suppliers and customers, in order to assess the TBML risks posed by these customers and their transactions.

b) When conducting documentary reviews or processing payments, the trade processing or operations team respectively, should not only focus on the operational and credit aspects of the documentation, but also assess whether there are in TBML red flags in the documentation or the transaction.

c) Given the knowledge of the trade processing team of the nature of transactions and industry nuances of products traded, regular information sharing between front office staff and trade processing teams should be encouraged. Such exchange of information will enhance the knowledge and skills of the relevant teams for detection and assessment of TBML risks and red flags.

d) When red-flags are detected by the first line of defence, an internal process should be followed to escalate, assess, and decide as required on the next steps with supporting documentation and rationale or decision.

i) Second line of defence:

a) The Compliance team should have trade finance expertise to review, assess and provide feedback on the TBML red flags identified by the front office and trade processing teams.

b) The Compliance team should perform assurance testing on a regular basis to ensure timely identification of ineffective TBML controls. Compliance testing should focus not only on the trade transactions escalated to Compliance, but also transactions which were not escalated to Compliance or internal Financial Intelligence Unit ("FIU") for investigation.

c) A bank should devise procedures to guide the first line of defence for escalation of suspicious transactions to Compliance or internal FIU.

d) Information on trade transactions or TBML related escalations, controls weaknesses and remedial action plans, together with other issues noted by Compliance should be regularly reported to senior management for effective oversight.

iv) Third line of defence (Internal audit):

a) As the third and last line of defence, internal audit, should conduct a holistic assessment of the Bank's framework to combat TBML, including the assessment of adequacy of policies and procedures and effectiveness of testing of relevant controls. Internal audit should design a TBML focussed test plan and ensure that the staff performing the testing have requisite trade finance and AML/CFT skills.

2.3. MANAGEMENT OVERSIGHT IN TRADE FINANCE

i) Senior management should ensure that:

a) Policies and procedures (along with roles and responsibilities of staff) to manage TBML risks are in place which should be regularly updated to take into account emerging risks;

b) Policies, procedures and processes should be readily accessible, effective and understood by all relevant staff;

c) Relevant skills exist or otherwise are provided to operations and compliance team in order for such team to effectively detect, review, assess and provide feedback or advice on the TBML risks and red-flags.

ii) Senior management may set-up a dedicated forum or committee to oversee and address trade finance related activities and TBML risks. Such a forum or committee may be established locally, regionally or globally depending on the size and complexity of the bank. The second line of defence function should be properly represented in the committee to provide compliance perspectives on the subject matter and highlight potential TBML risks.

iii) Senior management should be provided with regular or periodic reports from all three lines of defence which may be coordinated via the compliance function. Such reports may cover the following:

a) The effectiveness of the implementation of TBML controls, the outcome of the risk assessments and need for controls enhancement;

b) Status of back-logs and aging reports for trade finance customers in respect of CDD periodic review, closure of transactions monitoring and name screening alerts, and closure and reporting of suspicious activity or red-flags detected;

c) Any findings, typologies and threats seen in the trade finance business which require senior management attention, key issues faced in terms of managing TBML risks relating to customers and transactions, and updates on the approach taken to address any material TBML risks identified within the bank; and

d) The effectiveness of the ongoing monitoring programme for managing TBML risks including a periodic assessment of the sufficiency and effectiveness of relevant rules for monitoring trade transactions.

Best Practices

For larger banks, a global or regional trade control forum or committee may be set up, comprising senior management, first and second line of defence representatives, and other relevant departments such as risk management.

The trade control forum or committee may discuss and approve TBML related matters including quality assurance metrics, and escalate significant or material matters for approval to requisite AML/CFT governance committees within the Bank.

There should be a feedback loop from the trade control forum or committee to local country governance committees on decisions made and risks discussed.

For a smaller bank, such a forum or committee may be established at a local level.

In addition to the trade control forum or committee, a bank may decide to form a dedicated trade business and products committee to discuss and approve potential TBML risks on business proposals related to trade products.

2.4. Independent Assurance and Testing

i) A bank should ensure that assurance and testing is performed regularly for continual assessment of the robustness of its TBML controls.

ii) A dedicated function in the second line of defence of a bank should conduct independent assurance and testing of TBML controls. This dedicated function typically sits within the compliance function of a bank.

iii) The assurance and testing should be conducted by experienced staff who understand the trade finance business and TBML risks.

iv) The second line of defence independent assurance and testing should be performed in addition to third line of defence audit and ay self-assessment undertaken by the front and middle office function.

v) Effectiveness of controls and TBML risks and red-flags assessment should be tested through review of the applicable policies and procedures, the soundness of the overall framework as well as testing of samples in key areas where the assurance team concludes as an area of concern. The samples selected for testing purposes should be based on a methodology approved by the Bank which should provide a view on weaknesses in controls and their root-causes.

vi) The independent assurance and testing may cover the following:

a) Effectiveness of the risk-based approach applied in respect of TBML risks and red-flags assessment;

b) Effectiveness of detection of red flags and scenarios applied pre-transaction, during the transaction, at the time of the payment and after the transaction, as well as the quality of the audit trail;

c) Appropriate evaluation of the risk assessment and follow-up on issues identified in the risk assessment; and

d) Completeness and validity of customer, transaction and product due diligence information

Best Practices

Generally, the scope of the assurance programme should include oversight and governance, escalation to senior management of ML/TF/PF risk and compliance issues, compliance with policies and procedures, TBML risk and red-flags detection processes embedded within the trade finance business and operations, TBML control effectiveness, suspicious activity reporting and staff training.

Specialist teams may be formed within the first and second lines of defence to perform ongoing independent assurance testing:

(i) First line of defence may be represented by staff from the trade controls team; and,
(ii) Second line of defence should be represented by staff from the compliance testing team.

The samples selected for testing should include both transactions and alerts escalated to compliance, and transactions or alerts which were resolved within the first line of defence and not escalated to compliance or the internal financial intelligence unit ("FIU").

2.5. Internal Reporting and Role of Compliance Officer or MLRO

i) The MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism and the related Guidelines require a designated AML/CFT compliance officer or MLRO charged with second line of defence responsibilities and oversight.

ii) In the trade finance context, the AML/CFT compliance officer or MLRO role (or their responsible delegates) is expected to undertake duties mentioned in this Paper under Sections on Roles and Responsibilities and Independent Assurance and Testing, as well as, inter alia, undertake the following responsibilities:

a) Coordinate with relevant departments in the first line of defence to draft and implement policies and procedures, to ensure effective execution of controls and ongoing monitoring;

b) Train relevant trade processing or other specialised staff in trade finance business or products, to assess escalated red-flags or issues, transactions related risks or suspicious transactions and trade activities;

c) Consider the red flags and risks to conduct detailed review, as required, in assessing whether a STR should be filed and/or advise whether the transaction should be aborted;

d) Based on the information obtained and the final STR determination, work with relevant functions to re-assess and recommend adjustment to the customer's risk profile and updates to customer and product due diligence records;

e) Provide TBML specific training, sourced internally or externally. This should include relevant staff across all three lines of defence, and in particular, specialised staff handling day-to-day trade finance and compliance matters;

f) Participate in related business governance forums and committees to discuss TBML matters; and

g) Ensure regular reporting to senior management and Board members on TBML risk events or matters.

Best Practices
Roles and responsibilities of the AML/CFT compliance officer or MLRO (and their responsible delegates) in managing TBML risks should be documented and the incumbent of such role should be adequately supported by the Board and senior management in the performance of their duties.

3. Due Diligence

i) Customer Due Diligence ("CDD") is particularly important for a bank to manage and monitor the risks associated with customers on an ongoing basis, throughout the customer life-cycle with the bank.

ii) When conducting CDD for trade customers, both borrowing and non-borrowing, the bank should thoroughly understand its customer's business model prior to on-boarding. The bank should obtain additional know your customer ("KYC') information to assess the TBML risks associated with the customer.

iii) For trade finance customers, including non-borrowing ones, the bank should establish supplemental questions to the KYC or account opening form, to obtain information on the business of the customer, purpose of the trade activities, the intended parties and countries that the customer intends to transact with, the typical volume and value or price of goods to be transacted, the typical use of such goods, whether the customer will be trading with goods subject to embargo and export or import controls, whether any of the goods traded by the customer will ultimately be transported or transhipped to a sanctioned country even if the shipment is unloaded at a different port of destination, the customary payment terms with the buyer or seller (as applicable), the parties that will making or receiving the payment (when the details are known), the customary agents, shippers, freight-forwarders or insurers used by the customer (if already known), known counterparties at the time of opening of the account, and the reasons if there are related parties involved in the transaction. If required, the front office staff may conduct site visits to and meetings with the customer to confirm the details provided by the customer.

iv) This information mentioned in the preceding paragraph above should be obtained prior to on-boarding a customer to profile the customer and its expected transactions. Where there is deviation from this information at the time of the transaction or the delivery or issuance of trade documentation, the Bank should investigate the same as part of its red-flags assessment.

v) All CDD or KYC information available should be refreshed during periodic review or when there are significant changes to the customer's business and operations, so that changes to the customer profile or known trading patterns of the customer are captured.

3.1. Policies and Procedures

i) Banks should develop policies and procedures to assess and mitigate the risks of trade-based money laundering. These policies and procedures should enable banks to identify customers and transactions that pose the highest financial crime risk, and should set out well-defined processes with clear lines of responsibility for assessing and mitigating risks[7].

ii) In addition to the identification and verification measures required pursuant to the relevant MAS Notices, a bank's policies and procedures should define:

a) Enhanced CDD measures so that higher risk customers and transactions are appropriately assessed; and

[7] FCA Thematic Review - Banks' control of financial crime risks in trade finance

b) Additional KYC information[8] which should be obtained about the customer, including, their principal counterparties, the countries where these counterparties are located, the goods or services that are typically exchanged, the expected annual transaction volume and flows.

iii) The policies and procedures should be presented to senior management or relevant committees and be regularly updated to remain consistent with regulatory requirements, industry guidelines and typologies to take into account emerging risks. Instances when the policies and procedures should be refreshed include:

a) Regulatory requirements and/or guidance are amended or revised;

b) Best practices or guidance from industry bodies or standard setting agencies such as FATF, ICC, Wolfsberg and BAFT is issued;

c) Lessons learnt based from internal control failures, findings from assurance and testing and risk assessment or typologies ascertained from STR filings; and

d) Feedback is provided by law enforcement agencies, regulators, internal audit or external auditors.

3.2. IDENTIFYING THE CUSTOMER FOR THE APPLICATION OF DUE DILIGENCE MEASURES

i) Generally, full CDD should be conducted on at least one party in a trade finance transaction. The exact role of the bank in that trade transaction determines who is considered the customer. The bank should clearly establish the identity of the customer, typically the party instructing the bank, and the contracting party with the Bank.

ii) For avoidance of doubt, pursuant to Section 6 of MAS Notice 626, CDD should be performed on the customer before establishing the business relationship and / or permitting the trade finance transaction.

iii) Minimum standards are provided herein on who should be considered the customer of a bank for CDD purposes. Depending on the role of the Bank and the Bank's risk based approach:

Letters of Credit ("LC")	
Where the Bank is the issuing bank	a) The applicant of the letters of credit is deemed to be the customer.
Where the Bank is the advising bank	b) The issuing bank (of the letters of credit) is deemed to be the customer.
Where the Bank is the second advising bank and not the confirming bank	c) The first advising bank is deemed to be customer and CDD or enhanced CDD must be performed on the first advising bank.
Where the Bank is the second advising bank and the confirming bank	d) The issuing bank is deemed to be the customer and CDD must be performed on the issuing bank. In such a case, the issuing bank is the primary obligor and has nominated the Bank as the confirming bank.
Where the Bank is the transferring bank	e) The issuing bank is deemed to be the customer and CDD must be performed on the issuing bank.
Where the beneficiary of an export (Master) LC instructs the bank to issue a new LC (Slave LC)	f) The beneficiary becomes the Intermediary and the Applicant of the Slave LC. CDD must be performed on the Intermediary. CDD is not required on the Beneficiary of the back-to-back LC.
Where there is back-to-back letters of credit, and the Bank is acting as the advising bank,	g) The issuing bank of the export letters of credit (or the Master letters of credit) is deemed to be the customer and CDD must be performed on the issuing bank).
Where the Bank is the confirming bank	h) The issuing bank is deemed to be the customer and CDD must be performed on such issuing bank. In addition, if the LC does not call for or allow confirmation, and the Bank adds a silent

[8] Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking

	confirmation, the Bank is establishing a relationship with the beneficiary by receiving instruction from the beneficiary. Accordingly, CDD should also be performed on the beneficiary.
Where the Bank is the remitting bank (sending export bills and documents under letters of credit for collection) and no financing is involved	i) The issuing bank is deemed to be the customer and CDD must be performed on the issuing bank.
Where the Bank is the negotiating or re-negotiating or paying or accepting bank	j) The issuing bank is deemed to be the customer and CDD must be performed on the issuing bank. In addition, if the Bank negotiates the letters of credit due to discrepancies, the Bank is establishing a relationship with the beneficiary by receiving instruction from the beneficiary. Accordingly, CDD should also be performed on the beneficiary.
Where the Bank is not the nominated bank and does not provide financing, but remits the beneficiary's documents to a nominated or confirming bank for the purposes of negotiation or renegotiation or paying or accepting	k) The beneficiary is deemed to be the customer and CDD must be performed on the beneficiary. In such a case, the Bank is performing a service for and on behalf of the beneficiary.

Documentary Collections ("DC")	
Where the Bank is the collecting bank	l) The drawee is deemed to be the customer and CDD must be performed on the drawee.
Where the Bank is the remitting bank	m) The drawer is deemed to be the customer and CDD must be performed on the drawer.
Where the Bank is the remitting bank and the documents are routed to the bank through the drawer's bank	n) The drawer's bank is deemed to be the customer and CDD must be performed on the drawer's bank.

Bank guarantee, Bond or standby Letters of Credit	
Where the Bank's guarantee, bond or standby letters of credit is requested by a party which is not a financial institution	o) The applicant or the party on the bank has guaranteed (the party whose name appears on the guarantee), is deemed to be the customer and CDD or enhanced CDD must be performed on the applicant or the party on the bank guarantee. Where the applicant and the party on the bank guarantee are different, CDD should be performed on both entities. CDD is not required on the Beneficiary.
Where the Bank's guarantee, bond or standby letters of credit is issued pursuant to a counter-guarantee from a financial institution	p) The financial institution is deemed to be the customer and CDD or enhanced CDD must be performed on the financial institution. In such a case, the beneficiary of the guarantee or the customer's customer is not the party on whom CDD should be performed.

Bank to Bank reimbursement	
For export letters of credit, where the Bank is nominated as the reimbursing bank to honour a claim from the claiming bank	q) The issuing bank is deemed to be the customer and CDD must be performed on the issuer. The claiming bank is not the party on whom CDD should be performed on.
For irrevocable reimbursement undertaking, where the Bank receives a request from the issuing bank to issue the undertaking	r) CDD must be performed on the LC issuing bank as the Customer.

Refinancing and Rediscounting	
Where a pre-arrangement on financing has	s) The borrowing bank is deemed to be the customer

been made between the Bank and the borrowing bank	and CDD must be performed on the borrowing bank.

Trade Finance Transaction	
For sell down of transaction banking assets and contingents, where the Bank is offloading risk of its customers to another risk participating bank or insurer or development organisation	t) The risk participating bank or insurer or development organisation is deemed to be the customer and CDD must be performed on these parties. This is considered as a separate transaction to the underlying trade transaction or financing provided by the Bank.
For purchase of transaction banking assets and contingents, where the bank is the risk participating bank	u) The obligor bank (or the party from whom it is buying the assets and contingents) is deemed to be the customer and CDD must be performed on the obligor bank. In addition, CDD will also have to be performed on the underlying customers preferably prior to acquisition of the assets and contingents.

3.3. EFFECTIVE INFORMATION SHARING

i) A bank should ensure that there is a mechanism or feedback loop in place for effective information sharing (on an as-needed basis) for functions involved in the trade finance business or transactions. The information could assist in providing the relevant staff a holistic view of the customer, and identify any risks or red-flags in the customer's transactions or where there are deviations from the established pattern of transactions.

vi) Such information mentioned could include details of the customer's business and trading activity which is consistent with the profile of the customer, trading profile or pattern which is customary to the customer, the usual parties involved in the transactions and destination and flows of the same, the expected volume or value of the transactions, and the typical trade cycle for the type of goods the customer transacts.

4. TRANSACTIONS SURVEILLANCE

i) Transaction surveillance should be conducted by the Bank via:

a) Its automated transaction monitoring system;

b) Transaction review of the trade documentation and other transaction related information that comes to the attention of the Bank; and

c) Name or sanctions screening of the customer and all related parties to a transaction as well as screening of the payments or swift messages related to a trade finance transaction.

ii) A bank should conduct pre-transaction, in-progress and post-transaction reviews to identify TBML risks and red flags. The bank should also seek to detect any unusual or potentially suspicious features within a trade finance transaction or a series of transactions.

iii) Other than relying on the transaction monitoring system, a bank should put in place measures to assess a transaction before permitting the transaction, during the transaction or when documents are delivered, and at the time of payment or completion of the transaction. Risk-based post-transaction reviews and periodic customer reviews are an additional measure the bank may take to build an effective control environment.

Best Practices

Examples of additional measures that a bank could consider for review of trade finance transactions to assess TBML risk are:

i) Obtain more information and understanding from the instructing party in relation to the frequency of the transactions;
ii) Conduct checks into the verification of shipments after the Uniform Customs and Practice for Documentary Credits ("UCP") operation is over, to identify spurious transactions where buyers and sellers act in collusion. This can be done by sampling transactions, across a cross section of the bank's trade clients;
iii) Conduct checks into the verification of shipments after the Uniform Customs and Practice for Documentary Credits ("UCP") operation is over, to identify spurious transactions where buyers and sellers act in collusion. This can be done by sampling transactions, across a cross section of the bank's trade clients;
iv) Conduct site visits and meetings with the instructing party (for example, include planned and unplanned site visits);
v) Question if the goods are not typically exported from a particular country (for example, sugar from Bangladesh);
vi) Incorporate additional measures for high risk goods and services. While there is no definite list of 'high risk goods and services' for money laundering, such goods generally have a high value that is difficult, if not impossible, to ascertain independently and may fall into the following categories:
    a. Gold and platinum jewellery;
    b. Precious stones (such as diamonds, emerald);
    c. Branded luxury goods and items;
    d. Commodities (such as crude oil, gas, coal, sugar)
    e. Computer equipment or components (such as memory chips); and
    f. Art

4.1. TBML Red Flags

i) A bank should consider in its transaction review process the TBML red flags published by regulatory and industry bodies such as the MAS[9] and BAFT[10]. A bank should also include red flags and typologies identified internally from analysis of its internal alerts, STRs or from public sources. A robust transaction review process depends on the ability of the relevant staff to identify TBML risks and red flags.

ii) Banks should document and maintain a list of red flags and case studies that would apply specifically to their trade finance business. The relevant staff should be trained on the use of such checklists as well as the manner in which the red flags should be assessed, documented, escalated or closed.

iii) When a trade finance transaction is being reviewed by the trade processing team or the team assessing TBML red flags, there must be an established protocol in place within the bank for such teams to have access to all relevant information, and to request additional information.

iv) A bank should consider an escalation matrix for the operations team to escalate trade finance transactions to a centralised unit, typically sitting within the compliance function, for a holistic assessment to determine how to address TBML red flags. All information collected from both front office and operations should be provided to this centralised unit during escalation for discussion.

[9] Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking
[10] BAFT: Combating Trade Based Money Laundering: Rethinking the Approach (August 2017)

v) The assessment of red flags should be documented in the CDD profile or elsewhere for future reference. Refer to Case Studies 1, 2 and 3 for practical examples where such a feedback loop identified red flags which might have otherwise not been highlighted.

vi) Outlined below are some of the risk indicators for letters of credit transaction which could be uncovered either before or after the transaction is executed[11].

Activity or information connected with the letters of credit	Pre or Post[12] Checks
Parties	Pre
Deal Structures • Beyond capacity or substance of customer • Improbable goods, origins, quantities, destination • Unusual complexity or unconventional use of financial products • Transhipment through one or more jurisdictions with no apparent economic reason	Pre or Post
Goods • Blatant anomalies value versus quantity • Totally out of line with customer's known business	Pre or Post
Countries • On the financial institution's high risk list • Any attempt to disguise or circumvent countries involved in actual trade	Pre or Post
Payment Instructions • Illogical • Last minute changes • Third party or party unrelated to the transaction remits the payment	Pre or Post
Repayment arrangements • Third parties are funding or part funding the letters of credit value (just in time account credits to settlement account)	Post
LC patterns • Constantly amended or extended • Routinely cancelled or unutilized	Post
LC Counterparties • Connected applicant/beneficiary • Applicant documentation controls payment	Pre or Post
Discrepancies in documents • Goods descriptions differ significantly • Especially invoice vs shipping doc • Unexplained third parties	Pre or Post
Discrepancies waived • Advance waivers provided • Absence of required transport document • Significantly overdrawn LC	Pre or Post

4.2. Documentary Review

i) Given the susceptibility of trade to fraud, money laundering and proliferation financing, banks should undertake robust checking of trade transaction documents.

ii) TBML reviews should be conducted as follows:

a) At the point of issuance or advising;

b) When amendments occur during the transaction, or when documents are received;

[11] Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017
[12] Post checks refers to checks performed after a trade is complete, but prior to the transfer of securities or cash.

c) At the time of payment; and

d) At the completion of the transaction.

iii) Guidance should be provided to the relevant staff to ensure that TBML reviews are performed in a timely, structured and consistent manner. The TBML risks and red flag reviews should not be limited to a mere "tick box" exercise, and compliance function should be consulted where necessary. This guidance should be supported by subject matter training (Refer to Section 6).

iv) The TBML review should be performed by staff who are experienced in trade finance and who have a good understanding of TBML red flags. Any red flags or potentially suspicious activity should be assessed against documents provided and the profile of the customer. Clarification may be sought from the relationship manager or front office teams. When clarification must be sought from the customer, staff should take due care to not tip off the customer on a potential STR filing. Depending on the bank's internal procedures, and where necessary, such concerns should be escalated to the Compliance teams, to determine whether the transaction is suspicious and filing of an STR is warranted (Refer to Case Study 4).

v) Examples of checks that should be conducted by banks based on the documents obtained include (non-exhaustive):

a) Vessel: Vessel checks[13] to identify whether the vessel travelled to the respective ports as detailed in the relevant documents (for example, Bill of Lading, Invoices). A bank should also make reasonable effort to check that the cargo is loaded and discharged at the declared destinations.[14]

b) Price: A bank should make reasonable effort to assess whether the price of goods in a transaction is not false, misleading or there is an obvious misstatement in price. A bank should make further enquiries where the pricing of the goods appears to be manifestly unusual and make escalations as necessary, using the established escalation protocol for TBML.

c) Invoice: A bank should have controls and processes to detect if the same invoice has been submitted for financing more than once within the same organization. The Bank should review if the customer's business activities support the invoices.

d) Description of goods: A bank should have procedures to identify dual use goods[15], where applicable. Such procedures may include obtaining clarity when there is general or vague wording in the description of goods (for example, metal, electronic, chemicals) which presents challenges in reasonable identification of the nature of the goods. A bank should implement procedures, when goods are identified as potentially of dual use, to escalate these cases to the AML/CFT Compliance staff and relevant management staff.

vi) A bank should leverage industry utilities and tools where available and adopt a risk-based approach in managing its TBML risks, focusing more on transactions where potential red flags are identified. Examples of such utilities and tools include International Maritime Bureau (IMB), Lloyd's List Intelligence (LLI) and Sea Searcher.

[13] Sources to perform these checks include: Vessel finder , Lloyd's list
[14] Using tools such as International Maritime Bureau.
[15] Dual use goods are items are goods, software and technology that can be used for both civilian and military applications. (Definition retrieved from http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-usecontrols/)

Best Practices

As part of additional due diligence for trade transactions with potential red flags and those deemed high risk, a bank may perform additional checks against independent sources and databases. These checks indicate the flag of the vessels used and also the previous names of the vessel, if any, and facilitate the assessment of the risks posed if irregularities are detected.

Post-financing and using a risk-based approach, a bank should follow up with their invoice financing customers to obtain commercial invoices and transport documents. This will enable the Bank to perform verification checks and ensure that the trades are genuine.

Where anomalies regarding customer's trade-related activities are identified at any stage, a bank should obtain further information to assess whether there may be a legitimate explanation to allay the concern. If there is a reasonable and legitimate explanation for the anomaly, the TBML risk may be mitigated. The Bank should maintain good quality records of the explanation and the decision to accept the same as being reasonable and legitimate.

4.3. Sanctions Screening and Payment Message Screening

i) A bank should have a clearly defined screening policy, including sanctions screening, specific to trade finance. Based on the screening requirements, the bank should define critical data elements or "fields" that should be screened.

ii) As part of processing documentary and other trade products, the bank receives unstructured data contained in documents. This data should be assessed for viability of manual sanctions screening, especially where the data concerns entity names, individual names or geographical locations (cities, ports, countries, regions). The bank should establish a standardised form for the mandatory names which should be retrieved from the trade transaction documents for screening purposes.

iii) The following list includes some examples (non-exhaustive) of entities that could be screened:

a) Counterparty name(s) and location(s);

b) Counterparty bank(s) and location(s);

c) Customer name(s) and aliases including individuals and companies;

d) Carrier, charter, agent, freight forwarders, shipping companies;

e) Consignee;

f) Country of origin;

g) Origin of goods or commodities;

h) Originating and recipient entities of the goods (that is, importer and exporter) or shipper, consignee and notification party on transport documents; intermediaries engaged as part of the transaction;

i) Shipping route (such as the port of loading, port of discharge, port of transhipment);

j) Vessel name(s);

k) Flag of vessel;

l) Vessel IMO number;

m) Insurer;

n) Beneficial owners of vessel; and/or

o) Registered owners of vessel.

List Management:

iv) In addition to the screening guidance in the MAS Guidelines to Notice 626, screening lists (for sanctioned entities, individuals and countries) could include internal lists containing entities that are:

a) Not sanctioned but identified to be front companies for sanctioned companies;

b) Previously exited by the Bank for ML/TF/PF-related issues; or

c) Where appropriate, deemed to pose higher TBML risks.

vii) A bank could also add non-sanctioned countries, which it deems as high risk, to this list, in order to scrutinise transactions involving these countries.

Screening Process:

viii) At the time of receiving instructions to process a trade transaction, screening should be performed on relevant parties and entities whose information is available to the Bank.

ix) A bank should endeavour to identify all relevant parties and transportation carriers to the extent possible, not just at inception, but throughout the transaction, so that screening can be performed at various stages of the transaction (for example, in the case of letters of credit, screening should be done during issuance, amendment, receipt of documents and payment or settlement).

x) Entities that are not provided for in the SWIFT messages, and not automatically passed through the message filtering system for screening, should be manually screened.

xi) Clearance of screening hits should be subject to "four-eye" checks. Hits that are deemed unusual should be escalated to the compliance function for review. The rationale for discounting the screening hits should be appropriately documented and recorded for audit purposes.

Best Practices

Information contained in trade documentation should be screened against applicable lists or information provided by the authorities.

Hits should be investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and rationale should be clearly documented for any decision made.

New or amended information in relation to a transaction should be captured and screened in a timely manner.

4.4. Post Event Transaction Monitoring – Trends and Patterns Analysis

i) While screening and documentary review can identify anomalies for individual transactions, they do not enable banks to identify unusual trends and patterns in customer trades. Through comparison with historical transactions, transactions monitoring or surveillance systems can flag transactions for further

investigation based on certain pre-defined rules and, where data and systems are able to support this, identify deviations from past behaviour.

ii) Although -specific monitoring systems do not currently exist, banks could leverage monitoring systems developed to for cash accounts to monitor transfers between trade accounts in a similar fashion.

iii) Due to the range of variations inherent in normal trading patterns, it should be recognised that it is difficult to employ standard patterning techniques in transaction monitoring processes or systems for trade transactions.

Best Practices

As part of the review process for trade transactions, transaction monitoring analysts should conduct a holistic review of trade transactions. As the bank's existing transaction monitoring systems might only detect transaction movements and payments carried out through the customer's corporate account, the analyst should work with relevant units, including trade finance units, to determine if there may be any TBML related red-flags. Refer to Case Study 5 for an example of such a holistic review.

A bank may deploy technology solutions for back testing of transaction data to detect any TBML risks or red flags which may have not been captured during a manual review process.

5. Suspicious Transaction Reporting

i) A bank should ensure that transactions suspected of being used for ML/TF/PF purposes are duly investigated and promptly escalated to the compliance function and senior management. Records of the escalation, the review and rationale for the decision and the action taken should be kept for all stages of the escalation process up to and including the decision at compliance or other independent senior management level whether or not to file an STR.

ii) All STRs should be filed in a timely manner, and where necessary, the bank should contact the Suspicious Transaction Reporting Office or relevant authorities to follow-up on the information.

iii) When a bank is assessing whether to file an STR, it should, at a minimum:

a) Review trade finance documents, for example, bills of lading and commercial invoices;

b) Conduct company verifications and media searches;

c) Conduct client account activity reviews;

d) Review existing CDD information and, where required, obtain information from relationship management teams who should further reach out to customers (where necessary);

e) Review the results of any available screening and monitoring processes; and

f) Re-assess the customer risk and make adjustment to the risk rating, if appropriate.

Best Practices
Regular compliance checks, especially on transactions that were not escalated, should be performed for quality assurance purposes. Details of an escalation, the review and rationale for the decision and action taken should be accurately recorded for all stages of the escalation process up to and including the decision at the compliance function and/or senior independent level whether or not to file a STR.

6. TRAINING AND AWARENESS[16]

i) A bank should provide its staff with relevant, specific and targeted training to detect and prevent TBML risks and to heighten the risk awareness and competence of such relevant staff to mitigate ML/TF/PF risks and compliance with regulatory requirements.

ii) A bank should provide training and disseminate information to all relevant staff to highlight significant regulatory changes and new risks and typologies noted for managing TBML risks.

iii) In order to raise the awareness of TBML risks and the measures to mitigate such risks, a bank's AML/CFT framework should provide guidance and relevant training on a regular basis to staff involved in relationship management and transaction processing, operations as well as to other relevant staff, who are involved in trade transactions. Case studies and relevant industry publications should be included in the training to highlight common typologies or risk areas that require more attention from staff. In addition to regular training, a bank could increase staff awareness of current risks through sharing relevant typologies and relevant industry publications.

iv) Training should be refreshed periodically, as determined by the Bank's risk assessment. Training should align with the Bank's policies and procedures and should consider the circumstances which are unique to the Bank, for example products offered, operational locations, and customer types.

[16] List of MAS 626 Red Flags
MAS Information Paper October 2015 – Guidance on Anti-Money Laundering & Countering The Financing of Terrorism Controls in Trade Finance & Correspondent Banking
The Wolfsberg Group, ICC & BAFT Trade Finance Principles
HKMA – Guidance Paper on Combating Trade-based Money Laundering
FATF Typologies - APG Typology Report on Trade Based Money Laundering

Best Practices

A bank should consider TBML risks and conduct periodic training for staff to identify the transactions that present the higher risk of ML/TF/PF at various stages of a transaction.

For TBML training, a bank should identify all relevant staff who are involved in trade finance transaction. These should include front and middle office, such as trade product specialists, relationship managers, trade operations, AML advisors and CDD specialists.

A bank should retain copies of the training materials and attendance records for trainings that were delivered. This will enable the bank to review and update the training materials with new information, including new typologies and trends in TBML.

In addition to TBML typologies published in regulatory and industry papers, a bank should develop their own TBML typologies and case studies from STRs filed by them. The red flags should be modified, as applicable, to reflect the Singapore trade environment, or the Bank's own experience with trade transactions, or intelligence received from the group or other credible sources.

Besides regular training, TBML training should be conducted when there are new trade-related product offerings or modifications to existing trade-related products by the bank. This training should include a discussion of the new or modified product offerings and how the bank may be able to identify TBML red flags specific to this product. The training should be delivered to all staff involved in the review and processing of the new or modified product.

AML/CFT compliance teams, when discussing a new or modified trade-related product offering with the Trade Product Specialists or Relationship Manager, should assess the ML/TF/PF risks and level of risk awareness of the front office on TBML risk.

7. Record Keeping

i) It is important that a bank retains adequate records to demonstrate that controls are operating effectively. Such records are imperative to carry out effective compliance monitoring or quality assurance testing and to demonstrate to regulators that TBML risks are being managed effectively.

ii) A bank should, at a minimum, ensure that all records pertaining to trade transactions are kept in accordance with MAS Notice 626 requirements.

iii) A bank should maintain an audit trail for addressing any TBML risks and red flags that may arise at any stage of the transaction. This audit trail should include the basis of their decision and approvals obtained.

iv) In the case of closing a hit as a false alert, a bank should document the process taken to assess the TBML risks triggered and the rationale for closing the alert. Additional information collected for the purpose of the review, including any correspondence with the client, should be filed together with all the records pertaining to the transaction. Such audit trails are important as they allow the Bank to ascertain that the requisite surveillance is comprehensively and adequately performed. It also enables effective second-level post transaction reviews.

Best Practices
A bank should ensure that documentation of the review process for surveillance hits is maintained and easily accessible. Justifications for closing off alerts as false hits should be clearly documented in detail to facilitate post transaction review and audits. A bank should ensure proper documentation and record keeping of both the initial CDD assessment and any updated information. This should include customer and transactional information, any decisions made, and the rationale for the decision.

8. Open Account Trade Considerations

i) The majority of world trade finance transactions are carried out under "Open Account" terms. In such terms, the buyer and seller agree to the terms of the contract, goods are delivered to the buyer and a clean or "netting"[17] payment through the banking system closes the transaction.

ii) Under such Open Account terms, unless a bank is providing credit facilities, the Bank's involvement will be limited to the clean payment and it might not be aware of the underlying reason for the payment.

iii) As the bank has limited visibility of the transaction, it might not be able to carry out financial crime risk checks other than the standard AML and sanctions screening on the clean or netting payment[18].

iv) Despite the challenges faced due to lack of information or documentation, a bank should look out for, inter alia, the following red flags, where possible:

a) The customer engages in transactions that are inconsistent with the customer's business strategy (for example, a steel company starts dealing in paper products) or make no economic sense;

b) The customer deviates significantly from its historical pattern of trade activity (that is, in terms of markets, monetary value, frequency of transactions or volume);

c) Transacting parties appear to be affiliated, conduct business out of a residential address, or same business address or provide only a registered agent's address; or

d) The customer conducts business in jurisdictions that are bordering sanctioned countries or are at higher risk for TBML.

v) Where a bank is able to obtain underlying documentation from its customers, the bank should assess TBML risks and red flags as stipulated in this Paper.

[17] Netting refers to offsetting the value of multiple payments due to be exchanged between two or more parties.
[18] The Wolfsberg Group, ICC and BAFT - Trade Finance Principles (2017)

9. BEST PRACTICES

i. Risk Assessment

Inherent Risk Assessment:

The assessment of inherent risk can be conducted by administering questionnaires for qualitative risk factors, and by extracting quantitative data from the relevant bank systems. A bank should be prudent about the threshold for the quantitative risk factors based on its risk appetite and providing risk weights to both the qualitative and quantitative factors.

The information gathered should be populated against the ML/TF inherent risk assessment questionnaire to calculate the Bank's inherent risk. The ML/TF inherent risk assessment questionnaire should cover critical areas of the Bank's business (for example, customers, countries, products, services, transactions and delivery channels) and consider the operational and regulatory risk factors that should be taken into account when assessing the robustness of the TBML programme.

Mitigating Controls Assessment:

To assess the mitigating controls, the Bank should create a register of regulatory requirements or obligations, including known regulatory expectations and applicable industry best practice. The bank's policies and procedures, TBML red flags, controls which have been implemented and typologies should be mapped against the said register. This exercise should lead towards identification of control gaps, if any.

The controls that are mapped should be tested for effectiveness. Banks should consider the following while assessing control effectiveness:

1. Review of the Bank's policies and procedures, to identify any gaps between the policies and regulatory requirements;
2. Walkthroughs with the business and operations teams to identify if the policies and procedures are being operationalised effectively; and
3. Sample testing against key control indicators and control sample testing thresholds.

The controls in place should be periodically reviewed and tested for effectiveness and whether any change in the inherent risk of the business or residual risk necessitates enhancement of such controls.

ii. Roles and Responsibilities

A bank should formalise the ownership of policies, procedures and processes between the relevant lines of defence and preferably consider having a RACI (Responsible, Accountable, Consulted, Informed) matrix in place for added clarity on roles and responsibilities. It is good practice to have the process architecture documented with clarity in the ownership and duly defined roles and responsibilities of each line of defence.

iii. Management Oversight in Trade Finance

For larger banks, a global or regional trade control forum or committee may be set up, comprising senior management, first and second line of defence representatives, and other relevant departments such as risk management.

The trade control forum or committee may discuss and approve TBML related matters including quality assurance metrics, and escalate significant or material matters for approval to requisite AML/CFT governance committees within the Bank.

There should be a feedback loop from the trade control forum or committee to local country governance committees on decisions made and risks discussed.

For a smaller bank, such forum or committee may be established at a local level.

In addition to the trade control forum or committee, a bank may decide to form a dedicated trade business and products committee to discuss and approve potential TBML risks on business proposals related to trade products.

iv. Independent Assurance and Testing

Generally, the scope of the assurance programme should include oversight and governance, escalation to senior management of ML/TF/PF risk and compliance issues, compliance with policies and procedures, TBML risk and red-flags detection processes embedded within the trade finance business and operations, TBML control effectiveness, suspicious activity reporting and staff training.

Specialist teams may be formed within the first and second lines of defence to perform ongoing independent assurance testing:

(i) First line of defence may be represented by staff from the trade controls team; and,
(ii) Second line of defence should be represented by staff from the compliance testing team.

The samples selected for testing purpose should include the transactions or customers escalated to compliance and transactions or customers alerts which were resolved within the first line of defence and not escalated to compliance or internal financial intelligence unit ("FIU") (if any).

v. Internal Reporting and Roles of Compliance or MLRO

Roles and responsibilities of the AML/CFT compliance officer or MLRO (and their responsible delegates) in managing TBML risks should be documented and the incumbent of such role should be adequately supported by the Board and senior management in the performance of their duties.

vi. Transactions Surveillance

Examples of additional measures that a bank could consider for review of trade finance transactions to assess TBML risk are:

i) Obtain more information and understanding from the instructing party in relation to the frequency of the transactions;
ii) Conduct checks into the verification of shipments after the Uniform Customs and Practice for Documentary Credits ("UCP") operation is over, to identify spurious transactions where buyers and sellers act in collusion. This can be done by sampling transactions, across a cross section of the Bank's trade clients;
iii) Conduct site visits and meetings with the instructing party (for example, include planned and unplanned site visits);
iv) Question if the goods are not typically exported from a particular country (for example, sugar from Bangladesh);
v) Incorporate additional measures for high risk goods and services. While there is no definite list of 'high risk goods and services' for money laundering, they can generally be represented by goods that have a high value that is difficult, if not impossible, to ascertain independently and may fall into the following categories:
    a. Gold and platinum jewellery;
    b. Precious stones (such as diamonds, emerald);
    c. Branded luxury goods and items;
    d. Commodities (such as crude oil, gas, coal, sugar)
    e. Computer equipment or components (such as memory chips); and
    f. Art

vii. Documentary Review

As part of additional due diligence for trade transactions with potential red flags and those deemed high risk, a bank may perform additional checks against independent sources and databases. These checks indicate the flag of the vessels used and also the previous names of the vessel, if any, and facilitate the assessment of the risks posed if irregularities are detected.

Post-financing and using a risk-based approach, a bank should follow up with their invoice financing customers to obtain commercial invoices and transport documents. This will enable the Bank to perform verification checks and ensure that the trades are genuine.

Where anomalies regarding customer's trade-related activities are identified at any stage, a bank should obtain further information to assess whether there may be a legitimate explanation to allay the concern. If there is a reasonable and legitimate explanation for the anomaly, the TBML risk may be mitigated. The Bank should maintain good quality records of the explanation and the decision to accept the same as being reasonable and legitimate.

viii. Sanctions Screening and Payments

Information contained in trade documentation should be screened against applicable lists or information provided by the authorities.

Hits should be investigated before proceeding with a transaction (for example, obtaining confirmation from third parties that an entity is not sanctioned), and rationale should be clearly documented for any decision made.

New or amended information in relation to a transaction should be captured and screened in a timely manner.

ix. Post-Event Transaction Monitoring- Trend & Pattern Analysis

As part of the review process for trade transactions, transaction monitoring analysts should conduct a holistic review of trade transactions. As the Bank's existing transaction monitoring systems might only detect transaction movements and payments carried out through the customer's corporate account, the analyst should work with relevant units, including Trade Finance units, to determine if there may be any TBML related red-flags. Refer to Case Study 5 for an example of such a holistic review.

A bank may deploy technology solutions for back testing of transaction data to detect any TBML risks or red flags which may have not been captured during a manual review process.

x. Suspicious Transaction Reporting

Regular compliance checks, especially on transactions that were not escalated, should be performed for quality assurance purposes.

Details of an escalation, the review and rationale for the decision and action taken should be accurately recorded for all stages of the escalation process up to and including the decision at the compliance function and/or senior independent level whether or not to file a STR.

xi. Training and Awareness

A bank should consider TBML risks and conduct periodic training for staff to identify the transactions that present the higher risk of ML/TF/PF at various stages of a transaction.

For TBML training, a bank should identify all relevant staff who are involved in trade finance transaction. These should include front and middle office including trade product specialists, relationship managers, trade operations, AML advisors and CDD specialists.

A bank should retain copies of the training materials and attendance records for trainings that were delivered. This will enable the Bank to review and update the training materials with new information, including new typologies and trends in TBML.

In addition to TBML typologies published in regulatory and industry papers, a bank should develop their own TBML typologies and case studies from STRs filed by them. The red flags should be modified, as applicable, to reflect the Singapore trade environment, or the Bank's own experience with trade transactions, or intelligence received from the group.

Besides regular training, TBML training should be conducted when there are new trade-related product offerings or modifications to existing trade-related products by the Bank. This training should include a discussion of the new or modified product offerings and how the Bank may be able to identify TBML red flags specific to this product. The training should be delivered to all staff involved in the review and processing of the new or modified product.

AML/CFT compliance teams, when discussing a new or modified trade-related product offering with the Trade Product Specialists or Relationship Manager, should assess the ML/TF/PF risks and level of risk awareness of the front office on TBML risk.

xii. Record Keeping

A bank should ensure that documentation of the review process for surveillance hits is maintained and easily accessible. Justifications for closing off alerts as false hits should be clearly documented in detail to facilitate post transaction review and audits.

A bank should ensure proper documentation and record keeping of both the initial CDD assessment and any updated information. This should include customer and transactional information, any decisions made, and the rationale for the decision.

10. APPENDIX

A. GLOSSARY

Acronyms	Description
ACIP	Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
APG	Asia/Pacific Group on Money Laundering
BAFT	Bankers Association of Finance and Trade
CAD	Commercial Affairs Department
CDD	Client Due Diligence
CFT	Combatting the Financing of Terrorism
DC	Documentary Collections
EDD	Enhanced Due Diligence
EU	European Union
EWRA	Enterprise Wide Risk Assessment
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIU	Financial Intelligence Unit
HKAB	Hong Kong Association of Bankers
HKMA	Hong Kong Monetary Authority
ICC	International Chamber of Commerce
LC	Letter of Credit
IMO	International Maritime Organization
IT	Information Technology
MAS	Monetary Authority of Singapore
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NTP	National Trading Platform
OFAC	Office of Foreign Assets Control
RBA	Risk Based Approach
SBLC	Standby Letters of Credit
STR	Suspicious Transaction Reports
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBML	Trade Based Money Laundering
TF	Terrorist Financing
TM	Transaction Monitoring
UCP	Uniform Customs and Practice
VAS	Value Added Services

B. CASE STUDIES

i) The following case studies are intended to provide a practical flavour of the red flags to consider while reviewing trade transactions. Note that the amounts and values of currencies cited may have been changed from the original.

Case Study 1
Red flags: • Payments from client's buyers received prior to financing • Unable to reconcile and validate source of funds
Best practices: • Transaction monitoring to flag historical transactions based on rules and typologies • Periodic review of customer and understanding of customer profile
A routine sampling check of the client's transactions revealed that certain payments from the client's buyers were often received prior to the Financial Institution's financing. Upon clarification, the client responded that the sampled repayments in-question had been remitted in the past. The company did not appear cognizant that the requisition of FI financing without an underlying trade obligation outstanding represented a breach of the Financial Institutions lending condition. In addition, there was lack of clarity on the fact that, given the payments had already been received, how and where were the Financial Institutions funds being applied. As a result, there existed the risk of "double financing" since the bank loans were disbursed on credit exposure that had been repaid / liquidated. Certain payments were not remitted by the approved buyers, as intended. The client explained that the payments were settled though netting-off against other transactions and remittances from other non-approved buyers. The Financial Institution was unable to effectively reconcile and validate the source of funds.

Case Study 2
Red flags: • Use of possibly an offshore company to receive and remit funds relating to the transactions • Balance funds were withdrawn from the company's account via cheques after each transactions • Parties involved in the transaction could not be identified on the shipping company's website
Best practices: • Sample/periodic checks conducted on the trade transactions and underlying trade documents • Validation of trade documents against third party platforms (e.g. International Maritime Bureau)
The client was in general wholesale trade of seafood. It had three directors, who were also equal shareholders, one East Asian national and two Southeast Asians. The suppliers were from East Asia and buyers were from East Asia and other parts of Southeast Asia. *During the account review of the client it was noted that the account contained primarily incoming remittances from Company A (East Asia incorporated company dealing in seafood) and outgoing remittances to Company B (also an East Asia incorporated company dealing in seafood). The bank accounts of Company B and Company C were opened in banks located in East Asia. The amount of incoming remittance typically exceeded the amount of outgoing remittances; which the customer explained to be their profit margin. Balance funds were withdrawn via cheques periodically.* *The Director who was the East Asian National was stated as the person with the industry experience and network. Given that the transactions involved counterparties with no Southeast Asia nexus, the purpose of incorporating an offshore company in Southeast Asia to perform these business transactions was questionable. The customer was able to provide invoices and shipping documents upon request. As the shipping company used offered tracking services online, the bill of lading number was checked on its website and noted that every piece of available information matched, thereby suggesting that the sampled transactions were backed by actual business activities. However, as the parties involved in the transaction were not revealed on the shipping company's website, the financial institution was concerned about the possibility that the bill of lading was being doctored to make use of information available on genuine bill of ladings. The financial institution proceeded to check with the International Maritime Bureau and was informed that according to the shipping company, the details of the parties involved in the transactions did not match. This confirmed the suspicions that the bill of ladings provided were forged.*

Case Study 3
Red flags: • Transactions involve the use of front/shell companies • Trade counterparties involved appear to be engaged in different business activities • "Return" of funds from suppliers and the lack of supporting information to support the flow of funds
Best practices: • Periodic review of customer and understanding of customer profile • Due diligence performed on counterparties' nature of business and business address • Transaction monitoring to flag historical transactions based on rules and typologies • Perform price checks on the reasonableness of goods/commodities traded against market price
A routine review of the client's trade transactions revealed that generally, there was no meaningful information (i.e. lack of corporate website) on the named counterparties from which the funds were received. The absence of corporate websites for the identified counterparties raised the concern as to whether the companies were "shell entities" and hence, triggered further concerns on their source of wealth and sources of funds. It also raised potential issue(s) as to whether there were genuine sell-side trade transactions or whether the inward funds represented merely pass-through cash flows. *Additionally, the client had received suspected U-Turn of funds from one of its suppliers. The client's explanation for this was that the identified supplier was also one of the buyers and hence, the perceived "return" of funds were actual payments for cargoes delivered. The Financial Institution was unable to validate the client's explanation.* *Separately, one of the client's counterparties was identified as a newly incorporated company with a USD1/- paid-up capital. The office address appeared residential-like, as opposed to a commercial premise. The absence of a physical business operating premise raised suspicions whether it was an operating or shell company as well as its source of wealth and funds generation.* *A review of the accompanying trade-related documents. For example, commercial invoices, raised several other risk concerns such as counterparties appearing to be in a different lines of business, shared the same address and the veracity of the prices.*

Case Study 4
Red flags: • Trade counterparty involved appears to be engaged in a different business activity • Discrepancy in the port of loading stated on the Bill of Lading and on IMB • Shipment routes involved a sanctioned country
Best practices: • Periodic review of customer and understanding of customer profile • Due diligence performed on counterparty' nature of business and shipping agent's location • Validation of trade routes against third party platforms (e.g. International Maritime Bureau)
During a post-transactional review, the Financial Institution had requested for further information on one of the client's oil trading counterparties. According to the client, the relationship with the identified counterparty was established approximately 1 year ago. To corroborate the relationship, the client had provided trade documents that evidenced the supply of oil from the counterparty. However, in one of the transactions, while the Bill of Lading ("B/L") indicated that the base oil was shipped from Middle East, the IMB search indicated that the port of loading was Middle East. The B/L was signed-off by a certain shipping agency, which was located in Middle East. Further checks revealed that the counterparty's business activities were reflected as "toys and games" as opposed to oil trading. It was questionable and suspicious that the client had engaged this counterparty as a business partner for the supply of oil.

Case Study 5
Red flags: • Discrepancy in the value of goods stated in the invoice and airway bill
Best practices: • Incorporation of High Risk goods in the transaction surveillance system
An incoming remittance was flagged by the Bank's automated filtering system. The buyer had remitted the funds to the seller (customer) for the purchase of monitoring software for the vessel. This was in line with the business profile of customer. The buyer specializes in the installation, servicing, voyage repairs, retrofit, conversions and dry docking activities associated with all classes of Ocean going vessels. *Investigations showed that the value of goods declared on the airway bill was USD 88,000 which was significantly lower than the value of goods stated on the invoice (USD 1,660,000). Upon further clarification, the seller explained that the buyer had requested them to declare the value of goods in such a manner. The discrepancy noted and the explanation provided by the seller are both questionable.*

Case Study 6
Red flags: • Multiple flow-through transactions through the account within a month • Transactions do not make economic sense • Incomplete information on counterparties on the trade documents
Best practices: • Transaction monitoring to flag historical transactions based on rules and typologies • Review of trade documents to identify discrepancy in counterparties' information • Filing of STR upon identification of suspicious indicators

Company A is in the business of trading metals minerals and energy products. Within a month, its bank account in Southeast Asia received and transferred large amounts of funds to various corporate entities in Southeast Asia and overseas. This triggered a review by the Financial Institution. Upon examination of supporting documents provided for these trade transactions, they appeared to be dubious as they either did not contain the names of the transacting parties or had incomplete information such as addresses. It appears that Company A is a conduit used to facilitate the transfer of funds through purported trade transactions. As such, a STR was filed with the Suspicious Transactions Reporting Office.

The following suspicious indicators were raised:

i) Corporate account appears to be temporary depository account used to conduct flow-through transactions which did not make economic sense;
ii) Anomalies in transactions that did not correspond with the usual transaction pattern; and
iii) When queried on the transactions, trade documents were provided as supporting documents and they contained missing or incomplete information.

Case Study 7

Red flags:

- Complex transaction flow with the involvement of multiple parties in the transaction when the goods was ultimately sold to a party that operates in the same country as the seller
- Unit price of goods is below the initial purchase price and market price
- Illogical payment flow for the transaction of goods between Coal Supplier A, Company B and Company C

Best practices:

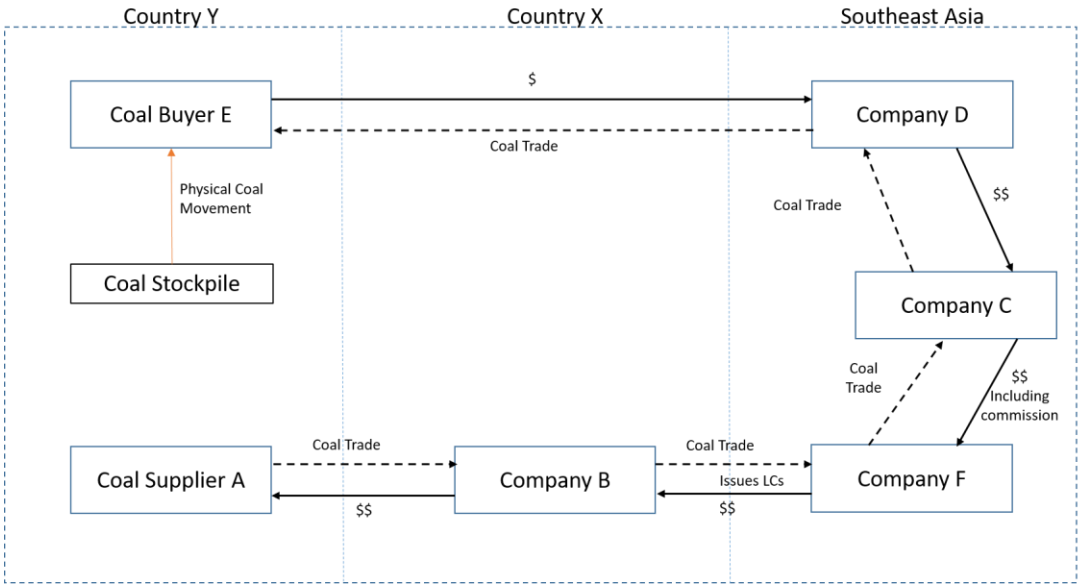
- Review of trade documents to identify discrepancy in information provided
- Understanding of the client profile
- Transaction surveillance and documentary review to identify TBML red flags

Coal supplier A in Country Y sold coal through various intermediaries in Country X and Southeast Asia to ultimate coal buyer E situated in the same country, Country Y. Company B bought the coal from the coal supplier and sold it to Company C, coal broker, who then sold the coal to Company D. Company D, which also purchases coal from several other companies, sold the coal to the ultimate buyer E in Country Y at prices lower than the initial purchase price and significantly below the market price. The coal traded was not exported to Companies B, C or D, and remained in Country Y. Company D will arrange for transportation to collect coal from the stockpile in Country Y and deliver to ultimate buyer E in the same country.

Funds arising from the coal purchase were transferred from ultimate buyer E in Country Y to Company D and C's bank accounts in Southeast Asia. Instead of engaging the banks, Company C engaged a non-financial institution, Company F, to obtain financing for the coal purchase from Company B. Company F issued Letters of Credit on behalf of Company C to Company B. In return, Company C pays commission to Company F prior to the issuance of the Letters of Credit. Funds in relation to these coal purchases were then transferred from Company F to Company B's bank account in Country X, and ultimately to coal supplier A in Country Y.

The following suspicious indicators were raised:

i) The shipments do not make economic sense;
ii) When queried on the flow-through transactions, trade documents were provided as supporting documents and they contained significant discrepancies;
iii) Subjects engaged in circuitous routing of shipments and/or circuitous routing of financial transactions; and
iv) Subjects involved in shipment of goods inconsistent with normal geographic trade patterns.



C. Disclaimer

1. This report is intended to be a tool-kit and reference material for the relevant financial [and non-financial] sector regulated for AML/CFT in Singapore. No part of this report may be reproduced or used for any other purposes, unless written consent have been obtained from MAS, CAD and Association of Banks in Singapore.

2. The cases studies cited within have been extracted from a variety of sources. Due care has been taken to avoid inclusion of any information that might reveal or point to the identity of a specific bank or customer. It should not be assumed, inferred or concluded that any criminal conduct has been established or actions taken against any persons mentioned in the case study.

D. TBML Working Group Members and Other Contributors

Firm	Representative
Banks	
United Overseas Bank Limited	Victor Ngo (Co-Chair)
United Overseas Bank Limited	Lim Siew Lee
United Overseas Bank Limited	Chan Kai Wai
United Overseas Bank Limited	Steven Tan
Standard Chartered Bank	Willem Toren (Co-Chair)
Standard Chartered Bank	Rosalind Lazar
Standard Chartered Bank	Nellie Tan
Standard Chartered Bank	Albert Teoh
The Hongkong and Shanghai Banking Corporation Limited	Beaver Chua
The Hongkong and Shanghai Banking Corporation Limited	Shawn Tan
The Hongkong and Shanghai Banking Corporation Limited	Chen Jee Meng
Citibank N.A.	Rashmi Dubier
Citibank N.A.	Chaw Chin Siang
Citibank N.A.	Khor Boon Keng
Citibank N.A.	Ashlynn Siau
BNP Paribas	Linda Woon
JP Morgan Singapore	Grace Ho
MUFG	Angie Chiong
MUFG	Adeline Loke
Professional Services	
Deloitte	Radish Singh
Deloitte	Kalyani Vasan
Deloitte	Ankur Shukla
Deloitte	Emily Lim
Government	
Monetary Authority of Singapore	
Commercial Affairs Department, Singapore Police Force	
Singapore Customs	