Monetary Authority of Singapore

GUIDANCE ON ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM CONTROLS IN TRADE FINANCE AND CORRESPONDENT BANKING

MAS Information Paper

October 2015

Table of Contents

1 INTRODUCTION

1.1 In the National Risk Assessment report published in January 2014, MAS had identified the anti-money laundering and countering the financing of terrorism ("AML/CFT") controls for trade finance and correspondent banking as areas where there could be scope for improvement. Robust controls in these areas enable banks[1] to better prevent and detect the risks associated with trade-based money laundering[2], proliferation financing and other sanctions compliance related issues. This paper aims to provide banks with guidance on the AML/CFT controls in trade finance and correspondent banking activities, assist them in their benchmarking against industry norms and in the implementation of sound risk management practices, and identification of control gaps. The observations were drawn from MAS' on-site inspections and off-site reviews.

1.2 The sharing of sound practices is intended to help banks further strengthen their controls and risk management. The examples in this document are not exhaustive. The guidance 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 trade finance and correspondent banking activities of each bank.

1.3 The contents of this guidance paper do not modify or supersede any applicable laws, regulations and requirements.

[1] For the purpose of this paper, the term, "banks", refers to banks, merchant banks and finance companies.

[2] The term, "trade-based money laundering", has been described by the Financial Action Task Force as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins".

2 TRADE FINANCE

2.1 As a trading and transportation hub, Singapore is vulnerable to money laundering ("ML") risks posed by trade finance. Due to its significant volume and value, trade finance transactions are an attractive medium for money launderers to transfer large values across borders. Trade finance can also be exploited for terrorism and proliferation financing ("TF/PF").

2.2 Significant concerns relating to these ML, TF or PF risks in trade finance (collectively known as "financial crime risks" in this paper) have been highlighted by other supervisory authorities and organisations such as the Financial Action Task Force ("FATF")[3], the Asia/Pacific Group on Money Laundering ("APG")[4] and the Wolfsberg Group[5].

2.3 From 2012 to September 2015, MAS conducted a series of inspections that covered banks' trade finance activities. This guidance paper provides details on pertinent observations arising from MAS' on-site inspections as well as guidance on identifying trade-based financial crime risks and implementing measures to mitigate such risks. Sound practices and areas where further attention is needed are also highlighted in this document.

[3] The FATF is an inter-governmental body established in 1989. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating ML/TF and other related threats to the integrity of the international financial system.

[4] The APG is an autonomous and collaborative international organisation founded in 1997 in Bangkok, Thailand consisting of 41 members including Singapore, and a number of international and regional observers. APG members and observers are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations.

[5] The Wolfsberg Group is an association of thirteen banks that has developed a broad range of standards and a diverse program of activities which address ML risks and other financial crime risks, such as corruption, TF and sanctions.

A Risk Assessment of Trade Finance Business

2.4 Banks typically perform a risk assessment of their trade finance business as part of their overall risk management framework to better understand the financial crime risks they are exposed to as well as to assess whether control measures are in place to mitigate these risks. The trade finance-specific risk assessment could be part of the broader risk assessment performed by banks at the enterprise-wide level in Singapore. Such an assessment allows banks to identify the risk areas in their trade finance activities and determine whether the controls in place are robust. The enterprise-wide risk assessment is intended to enable the bank to better understand its vulnerability to ML/TF risks, including the financial crime risks presented by its trade finance business, and forms the basis for the bank's overall risk-based approach.

Attention Areas

Banks should conduct a comprehensive risk assessment of their trade finance business, taking into account their customer base, geographical locations, products offered, and emerging risks if any, in determining the financial crime risks they are exposed to. Banks should also assess the adequacy of their risk management framework and internal controls to mitigate such risks.

B Due Diligence

2.5 The level of financial crime risks posed by customers and trade finance transactions differs based on their business, geographical locations, and risk profiles. Banks are expected to establish a sufficiently robust due diligence process to ensure that higher risk customers and transactions are subjected to more extensive due diligence measures and closer monitoring of transactions.

2.6 A typical trade finance transaction involves a number of different parties. The parties range from buyer and seller, to their respective agents, bankers and intermediaries. In general, banks should treat an instructing party in a trade finance transaction as their customer and conduct appropriate due diligence measures in accordance with a risk-based approach.

2.7 The due diligence checks that should be conducted by banks depend on the role of the bank in the trade finance transaction. Given that the risk taken on by the bank at each stage of the transaction differs, there would also be a corresponding difference in the type and extent of due diligence measures required. The instructing

party of a bank is determined by the bank's role in the transaction, e.g. for import documentary Letters of Credit ("L/Cs"), the instructing party for the L/C issuing bank is the L/C applicant; for export L/Cs, the instructing party for the L/C advising/confirming bank is the L/C issuing bank or the first advising bank. Banks should establish guidelines to determine the instructing party, and the extent of due diligence measures to be conducted, in a trade finance transaction.

Additional Information to be obtained for Trade Finance Transactions

2.8 In addition to the customer due diligence requirements set out in the MAS Notices to Financial Institutions on Prevention of Money Laundering and Countering the Financing of Terrorism (thereafter referred to as "the Notice")[6], banks are expected to obtain further information to assess the financial crime risks specific to a trade finance transaction.

2.9 Banks should obtain additional information on other relevant parties (such as those set out in paragraph 2.10) to a trade finance transaction, taking into account the bank's role in the transaction. Banks should develop clear procedures on the additional information required under various circumstances for all the relevant parties, including beneficiaries of L/Cs and documentary collections, agents and third parties identified.

2.10 The type and timing of the additional information obtained depend on the bank's role in the transaction and should be in line with a risk-based approach. This also applies to cases where a bank provides credit lines for, or facilitates open account trades (e.g. invoice financing, pre-shipment financing, inventory financing) of its customers. Examples of such additional information are –

(a) trading partners or counterparties of the customer (including buyers, sellers, shippers, consignees, notifying parties, shipping agents, etc.);

(b) nature of the goods traded;

(c) country or countries of origin of the goods (including whether the goods originate from any sanctioned country);

(d) trade cycle;

[6] The applicable MAS Notices include MAS Notice 626, MAS Notice 1014 and MAS Notice 824.

(e) flag of vessel, flag history and name history (to check whether it is related to any country in the list of sanctioned countries);

(f) name and unique identification number (e.g. International Maritime Organisation ("IMO") number) of any vessel proposed to be used (e.g. to better identify if it is ultimately owned by a sanctioned party);

(g) beneficial owner, commercial operator and registered owner of the vessel involved in the transaction to trace the history of former ship owners with focus on country of residence;

(h) port of loading, ports-of-call and port of discharge (including whether the goods originate from, or are sold to any sanctioned country) and the trade routes proposed to be used; and

(i) market prices of goods such as commodities to assess if further information should be obtained where the contract price differs significantly from the market price to mitigate financial crime risk.

2.11 Banks should verify information obtained on a trade finance transaction (e.g. against commercial documents, transport documents, and on a risk-sensitive basis, from independent or public sources) to authenticate the details of the transaction. This should also apply to cases where banks provide credit lines for, or otherwise facilitate, open account trades (e.g. invoice financing, pre-shipment financing, inventory financing) of their customers.

2.12 The following are examples of trade finance transactions and the additional information that banks are encouraged to obtain either at the time of customer on-boarding or at the time of the transaction –

(a) Import (Outward) L/Cs

- The L/C issuing bank should enquire from the L/C applicant the countries with which the applicant trades and the trading routes utilised, the goods traded, and the type and nature of parties the applicant does business with (e.g. customers and suppliers). Where possible, the L/C issuing bank should also enquire about the role and location of third parties (e.g. shipping agents, inspection companies and warehouses) used by the applicant in relation to the business.

(b) Export (Inward) L/Cs

- Where the advising/confirming bank has an ongoing relationship with the L/C issuing bank, the bank may rely on due diligence measures already performed.

- Where the advising/confirming bank does not have an ongoing relationship with the L/C issuing bank, the advising/confirming bank should ensure that it authenticates any L/C received from the L/C issuing bank and that the relevant parties are subjected to the bank's sanctions screening process.

- Where the L/C is issued by an L/C issuing bank in a country considered to present higher financial crime risks or if the nature of the transaction presents higher financial crime risks, the advising/confirming bank should conduct enhanced measures as appropriate.

(c) Bonds/Guarantees

- Banks are reminded to comply with the Notice requirements in relation to the instructing party/applicant as a customer of the bank. The bank should also subject the beneficiary to its sanctions screening process.

(d) Bank-to-Bank Trade Financing

- Financing banks should ensure that due diligence on the borrowing bank has been performed in line with the Notice requirements.

- Banks should also have a robust risk assessment framework to identify higher risk transactions (e.g. by identifying higher risk contracting parties, countries, types of goods and other terms in the L/C). For such higher risk transactions, additional verification measures and AML/sanction checks should be performed (e.g. obtaining certified true copies of underlying commercial and transport documents).

Sound Practices

As part of additional due diligence for trade finance transactions that present higher financial crime risks, some banks perform 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 banks' assessment of the risks posed if irregularities are detected.

Attention Areas

Some banks had a practice of issuing L/Cs with unnamed ports of loading and discharge for commodity traders if the trade routes were not confirmed at the point of L/C application. Banks should establish a process to follow up with customers to obtain supporting documents to identify the ports of loading and discharge, vessels involved, etc. if such information is not provided at L/C issuance.

Additional Information to be obtained for Trade Finance Transactions that present higher financial crime risks

2.13 If, at the initial stage or during the course of any trade finance transaction, a bank becomes aware that the transaction presents higher financial crime risks, the bank is expected to obtain information, in addition to those set out in paragraph 2.9, to assess —

(a) the transaction structure;

(b) the ports of call, including the route of the shipment, ensuring that it appears to be logical with regard to transhipment points and the final destination;

(c) the legitimacy of the payment flows;

(d) the transaction against public sources of specialised data, documents or information (e.g. the International Maritime Bureau) in relation to sea transportation to verify the authenticity of the bills of lading and to confirm that the shipment has taken place; and

(e) whether they are dual-use goods.

In addition, the bank should conduct site visits and meetings with the instructing party, where appropriate.

Invoice Financing

2.14 Banks regularly grant invoice financing facilities as part of their trade finance business. For such invoice financing facilities, banks may accept summaries of invoice details from selected customers in lieu of the actual invoices and shipping documents.

2.15 Subsequent to providing invoice financing services to their customers, banks should follow up with customers to obtain commercial invoices and transport documents for the verification of the genuineness of the trades. Such verification checks are typically performed by a function independent of the front office. Banks should have a formal process in place to perform post-financing validation checks to ensure that the information provided by the customers in the summaries of invoices match the details in the actual trade documents.

2.16 Banks which implement validation checks on a sampling basis should ensure that their sampling methodology is robust. A risk-based approach to the sampling methodology should be applied such that higher risk profile customers and transactions are targeted, and that the frequency of checks and number of samples chosen are commensurate with the risks identified. Sample checks should also include some lower risk accounts. The lack of checks exposes banks to risks since errors in the information submitted by customers, such as invoice value, names of vessels and shipping companies/agents etc. would remain undetected. The checks are particularly important as the effectiveness of the bank's AML/CFT sanctions screening depends on the accuracy of such information. Such checks also serve to deter customers from submitting false or inaccurate information in the invoice summaries.

2.17 When granting invoice financing facilities, banks had, in the past, generally taken into consideration only the credit quality of the customers. However, awareness of financial crime risks in this regard has increased in recent times. To mitigate financial crime and other legal, regulatory and reputational risks, other considerations should include the bank's knowledge of the customer and its business activities, account conduct, the customer's reputation in the industry as well as the customer's governance structure and control culture, amongst others.

Attention Areas

(a) Post-financing, banks should follow up with their invoice financing customers to obtain commercial invoices and transport documents to perform verification checks to ensure that the trades are genuine.

(b) Banks should formalise a process to perform post-financing validation checks on inaccuracies in the invoice summaries which would otherwise remain undetected.

(c) For the approval of invoice financing facilities, other considerations besides the credit quality of the customers should be formalised in the bank's policies, even if they are taken into consideration in practice.

Dual-Use Goods

2.18 Dual-use goods are goods, software and technology normally used for civilian purposes but which may have military applications, or may contribute to the proliferation of weapons of mass destruction.[7] Interpretation of "dual-use" requires a degree of technical knowledge that checkers of L/Cs may not always possess. In addition, the description of the goods may appear in the documents using a wording which does not allow the identification of such goods as "dual-use". Without the necessary technical qualifications and knowledge across a wide range of products and goods, the ability of a bank to understand the varying applications of dual-use goods will be limited. However, banks may refer to sources of information that may be relevant to assessing the risk that particular goods may be "dual-use", or otherwise subject to restrictions on their movement (e.g. Strategic Goods Control List from Singapore Customs[8] and European Commission's TARIC database[9]).

2.19 It is important that banks ensure that staff are aware of the risks of dual-use goods and the common types of goods with dual use, and are capable of identifying red flags which suggest that dual-use goods may be supplied for illicit purposes. References to public sources of information and other guidance should be provided to staff and formalised in the bank's policies and procedures to ensure that dual-use goods in trade finance transactions can be identified whenever possible. Such transactions should be highlighted and escalated as part of the bank's due diligence process.

[7] Definition retrieved from http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/

[8] For more information and details on the Strategic Goods Control List, please refer to the following link - http://www.customs.gov.sg/stgc/leftNav/str/Overview.html

[9] For more information and details with regard to the European Commission's TARIC database, please refer to the following link - http://ec.europa.eu/taxation_customs/dds2/taric/taric_consultation.jsp?Lang=en

C Sanctions Controls

Screening

2.20 Sanctions screening is a major component of transactional due diligence to ensure that banks are not dealing with sanctioned individuals or entities. Banks perform name screening on the key parties to each transaction. Besides screening the parties to the transaction, such as the seller of the goods, banks should also screen the vessel used to transport the underlying goods, the shipping company, any agents or third parties present in the transaction, and know the ports of call of the vessel for the particular transaction flow (origin port, destination port) where possible. It is also a good practice for banks to find out the recent voyage history of the vessel. If the vessel had docked at embargoed countries during its previous voyages, it could be a trigger for banks to conduct further checks as the transaction could involve dealings with sanctioned entities or embargoed goods.

2.21 Banks should be aware of any adverse developments pertaining to some parties (e.g. addition to list of designated individuals/entities) present in the trade finance transaction, between the inception of the trade finance transaction and submission of trade documents since there could be significant time difference during this period. Furthermore, banks are expected to perform sanctions screening both at the inception of the trade finance transaction and at the point of submission of the trade finance documents as some of the transactional details, e.g. vessel used to transport the cargo, ports of call, may not be known at trade inception and hence would not have been screened at that stage.

Sound Practices

(a) Many banks perform name screening on a transactional level. Transactional information is typically keyed into systems to enable detection of sanctioned customer names, ports and vessels.

(b) For other relevant information not keyed into systems, some banks perform manual name screening or manual compliance checks against the bank's sanctions lists.

(c) Some banks conduct additional checks for transactions where there are screening hits against vessel names, discrepancies or ambiguity in trade documents, transhipments or the use of multiple ports. These additional checks include location checks of vessels (such as the last known port and destination) against third party independent sources. This additional information helps the banks in their assessment of potential suspicious transactions.

Attention Areas

(a) Banks should have formalised guidelines on the parties that require screening. This would ensure that bank staff performing screening checks are aware which parties have to be screened and there are no cases where certain parties in a trade finance transaction are omitted.

(b) If banks obtain additional information from their customers (e.g. the customer's trading partners), screening of these trading partners should be performed. Screening of parties named in trade documents should also be performed in all instances.

2.22 In invoice financing, customers which are permitted to submit summaries of invoices usually provide certain transactional information, including the commercial invoice number, currency, amount, issue date, maturity date and buyer/seller names of each transaction. The invoice financing banks should require customers to provide the full set of transactional information in the summaries on a pre-financing basis as far as possible. Other transactional information present in commercial invoices and transport documents which banks should require customers to provide include names of vessels, shipping companies/agents, ports of loading and discharge, and description of goods. This is to ensure that the banks minimally screen the full set of transactional information to satisfy themselves that they have not directly or indirectly financed a trade finance transaction with or for the benefit of a designated person/entity. Policies and procedures should provide guidance to staff on the type of transactional information required to be obtained for invoice financing.

Attention Areas

In accepting summaries of invoices, banks should ensure that the summaries contain the relevant information required to conduct the necessary review/sanctions screening at the pre-financing stage. Transactional information present in commercial invoices and transport documents should be subject to review and sanctions screening.

Audit Trail

2.23 Banks maintain audit trails of the sanctions screening performed for trade finance transactions. Such audit trails are important as they allow banks to ascertain that the requisite screenings are comprehensively and adequately performed and also allow for effective second-level post-transaction reviews. Banks are also expected to have adequate documentation of the review process for resolving

screening hits, including justifications and reasons for closing off screening hits as false hits.

Attention Areas

Banks should ensure that documentation of the review process for screening hits is maintained and accessible. Justifications for closing off screening hits as false hits should be properly documented to facilitate second-level post transaction reviews, and audits.

D Trade-Based Money Laundering Controls

Assessment of Deviations from Market Prices

2.24 Checks on the reasonableness of invoice prices of goods/commodities against prevailing market prices (referred to as "price checks") are not only useful to mitigate credit risks; they also serve to identify potential fraud and ML/TF activities arising from over/under-invoicing of transactions.

2.25 Banks should perform price checks, particularly where market prices are available, minimally on a sampling basis. Policies and procedures should be clearly set up to guide staff in performing such checks, including establishing the level of acceptable price variance, and escalation procedures when significant differences in prices are identified.

2.26 Banks could consider setting different thresholds for different types of underlying goods/commodities. There should also be periodic assessments of whether the thresholds continue to be reasonable based on prevailing market prices for the goods/commodities.

2.27 Price checks should be performed by functions independent of front office so as to enhance the effectiveness of the checks and minimise conflicts of interest.

2.28 There should be guidelines in place for the selection of reference prices for the purpose of performing price checks.

Sound Practices

A bank has implemented an in-house system to detect differences between transacted and market prices which facilitated its assessment of price deviations.

Attention Areas

Banks should put in place policies and procedures to guide staff in their assessments and checks on transactional prices for deviations. In addition, banks should set out the escalation procedures to manage transactions where significant differences in prices are identified.

Related Party Transactions

2.29 There are inherently higher risks of fraud and financial crime associated with the financing of transactions between a customer and its related parties.

2.30 Some banks recognise this risk and require related party transactions to be escalated for further scrutiny. Banks could consider implementing additional safeguards to mitigate the risks arising from related party transactions, e.g. requiring documentary evidence to verify the authenticity of these related party transactions.

2.31 Banks' front office would obtain information about a customer's business and its present and future trading profile, including information on the customer's related parties, and where applicable, the typical related party transactions that occur in the course of the customer's business. However, such information may not be made available to the middle or back offices for additional due diligence, such as checks on the rationale for the trade flows and pricing, to be performed on the individual transactions.

2.32 The middle office/back office staff processing the trade finance transactions would be better informed when identifying related party transactions if there is effective sharing of information between the front office, which would have collected information on their customers' related entities as part of the customer on-boarding and regular review process, and the control or operations units processing the trade transactions.

Attention Areas

(a) Banks should put in place policies and procedures to guide staff in identifying related party transactions of customers.

(b) Besides efforts to identify related party transactions in practice, there should be a formal process in place to identify related party transactions and to trigger relevant follow-up actions to ascertain the authenticity of such transactions.

(c) Middle/back office staff should perform additional due diligence when processing related party transactions, to minimise fraud and financial crime risks.

Underlying Goods Financed

2.33 Banks should formalise processes to identify unusual transaction patterns that are inconsistent with the customers' profiles for further reviews and investigations. In addition to checking for inconsistencies in customers' trading patterns, banks are encouraged to check the descriptions of goods stated in the trade documents, particularly for descriptions which are unclear or worded in a foreign language. Banks should, on a best effort basis, determine whether the underlying goods financed are embargoed goods and there should be special attention paid to dual-use goods.

2.34 Banks should ensure that there are effective channels for information obtained by the front office during the customer on-boarding and ongoing review processes, which should include information on typical goods the customer deals in, to be shared with the middle and back office staff. This is to facilitate checks on the underlying goods by the middle and back office staff in their day-to-day processing of transactions.

2.35 The front office should also regularly review customer transactions for inconsistencies with the customers' profiles.

Controls over Multiple Financing of Invoices

2.36 When invoice financing facilities are granted, banks should ensure that there are proper processes and controls in place to detect if customers have submitted the same invoice for financing more than once.

Sound Practices

A few banks have enhanced systems to detect duplicate/multiple entries of the same invoice number that was keyed in for processing.

E Transaction Monitoring & Filing of Suspicious Transaction Reports

2.37 Banks should ensure that their transaction monitoring processes and systems are robust to enable suspicious transactions to be flagged, investigated and escalated. Regular compliance checks, especially on transactions that were not escalated, should be performed for quality assurance purposes.

2.38 Most cases of trade finance transactions escalated to Compliance and Management for attention were in relation to potential breach of sanctions related to PF. There were generally fewer cases of trade finance transactions escalated or further investigated due to potential ML concerns. Consequentially, fewer Suspicious Transaction Reports ("STRs") were filed on trade finance transactions in relation to suspicion of ML. Banks should ensure that transactions suspected of being used for ML purposes are duly investigated and promptly escalated to the Compliance function or senior management. If there are grounds to suspect that a customer is using trade finance to launder money, finance terrorism or facilitate PF, STRs must be promptly filed. The bank should also minimally subject the customer account to enhanced monitoring and consider rejecting the transaction.

Sound Practices

For suspicious transactions with insufficient grounds to be rejected, banks subject the customer to enhanced monitoring.

F Policies and Procedures & Training

2.39 Most banks have controls and procedures in place to address the risk of dealing with sanctioned parties and vessels for trade finance transactions. Given the increasing propensity for trade to be used as a channel to launder illicit funds, policies and procedures which detail the various money laundering methods that could be employed by criminals in trade finance transactions, including the red flag indicators mentioned in para 2.41, would be beneficial in raising the level of staff awareness. These policies and procedures should define the responsibilities for different functional areas of the bank to ensure that the relevant parties understand

their AML/CFT responsibilities when processing trade finance transactions. This could include formalised guidelines on the circumstances under which a transaction should be escalated to Compliance and senior management and/or subjected to closer monitoring.

2.40 Banks should regularly review the need to allocate more resources towards training to raise the awareness of staff to the financial crime risks associated with trade finance and the measures to mitigate such risks. Case studies and relevant industry publications could be included in the training to highlight high risk areas that require more attention from staff or common typologies.

Sound Practices

The Compliance function of a bank conducts regular interviews with selected front office employees to ascertain if staff have a good understanding of the due diligence requirements, the financial crime risks associated with trade finance transactions, and the bank's mitigating measures.

Attention Areas

(a) Banks should have more specific guidance, policies and procedures in place to address the overall risks of trade-based money laundering.

(b) There should also be adequate and specific training conducted by banks on the financial crime risks prevalent in the trade finance business for all relevant staff.

G Potential Red Flags

2.41 Banks should pay attention to the following red flags when processing trade finance transactions of their customers as they could be indicative of a transaction being used for financial crime purposes. These examples are not exhaustive, and the presence of a single red flag indicator does not mean that the transaction is illegal. A confluence of multiple indicators would nonetheless suggest that the transaction is suspicious, and appropriate due diligence measures, including STR filing, should be adopted by the bank.

Transactions with Higher Financial Crime Risk Elements

- The commodity is shipped to, through or from a jurisdiction designated (e.g. by the FATF or United Nations) as "higher risk" for financial crime activities
- The type of commodity shipped is designated as "higher risk" for financial crime activities[10]
- Potentially higher risk activities, including activities/goods that may be subject to export/import restrictions

Inconsistencies and Transactions Which Do Not Make Economic Sense

- Underlying goods, size of transaction, value of transaction, counterparties involved in the transaction, are inconsistent with the customer's usual business pattern, or deviate from the customer's business strategy.
- Mis-declaration of value (e.g. over-valuation) of goods
- The method of payment[11] or financing[12] appears inconsistent with the risk characteristics of the transaction
- Unexplained, unnecessary or last minute changes to a specific transaction or payment instructions
- Unusual payment terms, where payments and interest rates substantially deviate from expected market practice or prevailing rates
- Tenor of the financing is not in line with the nature of the underlying commodity financed, which could be a perishable good
- Transaction does not make economic sense
- Goods are inconsistent with the country of import/export

[10] For example, high-value, low-volume goods (e.g. certain IT and electronic products), which have high turnover rates and present valuation difficulties.
[11] For example, (i) the use of an advance payment for a shipment from a new supplier in a high-risk country, or (ii) direct payment through open accounts from banks to overseas suppliers on trade credit application of the domestic trader.
[12] For example, use of factoring companies to finance trade transactions between related companies.

- Transport document shows transhipment through one or more jurisdictions for no apparent economic reason

Related Party/Third Party Transactions

- Transaction is between or involves related parties
- Same address used for different transacting parties, usage of registered agent's address, or other address inconsistencies
- Unexplained or unnecessary parties to the transaction and who appear evasive about their identity on further enquiries
- Transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction
- Payment or payment requests of proceeds to a third party unrelated to customer

Transactions with Unexplained/ Frequent Documentary Changes

- Transaction involves the use of repeatedly amended or frequently extended L/Cs without legitimate commercial reasons
- Significant amendments in L/C without reasonable justification; including changes to beneficiary or stated location of payment
- Non-standard clauses or phrases (e.g. L/C is unconditional, divisible and assignable, transactions requiring proof of product, transferable and assignable without being used) included in L/C
- Unauthorised amendments or indications of tampering to trade documents

Transactions with Multiple Discrepancies/ Missing Information

- Receipt of L/C as an unauthenticated SWIFT or untested telex message
- Discrepancies in country of beneficiary's account and beneficiary's stated location/ business operations
- Physical trade-related documents appear fraudulent or altered
- Variances between the description of the goods on the transport document and the invoice
- Discrepancies between the value of the invoice and current market value of the product
- The quantity of the goods exceeds the known capacity of the shipping container or tanker capacity
- Abnormal weights for the goods compared to the quantity of goods
- Inappropriately sized or non-typical type of vessel used to transport the goods

- Absence of documentation or refusal to provide documents to prove shipment of goods
- Bill of lading describes containerised cargo but no container numbers are evidenced

Usage of Front/ Shell Companies and Complex Structures in Transactions

- Transaction involves the use of front (or shell) companies
- Attempts made to circumvent/disguise countries involved in the trade
- Unnecessarily complex transaction structure possibly designed to obscure the true nature of the transaction
- Multiple intermediaries used for a transaction
- Series of cross border transactions in the same goods between related companies

Other Red Flag Indicators

- Future dated bill of lading
- Unusual triggers for payment (e.g. before goods are shipped, no documentation required, etc.)
- Customer shares the same address as a sanctioned entity
- Inability or reluctance to provide clear answers to queries from the bank in relation to the nature as well as the commercial and technical aspects of the transaction
- Dual-use goods used in a transaction, which could also be coupled with additional red flags such as military or government buyers, unusual shipping route, reluctance on part of customer or purchasing agent to offer information on end use of the item, product is not in line with the buyer's business, or product is incompatible with the technical level of the country to which it is shipped to.

3 CORRESPONDENT BANKING

3.1 Correspondent banking relationships expose banks to inherently higher ML/TF risks, largely because, when executing the instructions of respondent financial institutions ("FIs"), banks have limited information available regarding the nature or purposes of the underlying transactions.

A Due Diligence on Respondent FIs

3.2 Banks that undertake correspondent banking activities typically conduct an assessment of the ML/TF risks associated with such activities. Such an assessment helps the bank to identify, assess and understand the risks associated with providing correspondent banking services so that the bank can apply appropriate due diligence and risk mitigation measures. The bank's assessment of the ML/TF risks specific to correspondent banking could be a part of its enterprise-wide risk assessment.

3.3 Generally, banks perform due diligence measures on respondent FIs in accordance with the Notice. These measures include gathering adequate information about the respondent FI, determining from available sources the reputation of the respondent FI and the quality of supervision over the respondent FI, and assessing the respondent FI's AML/CFT controls.

Attention Areas

Due diligence measures on respondent FIs may be performed centrally, for instance by Head Office ("HO") or a hub location. Despite such arrangements, banks are still responsible for assessing the ML/TF risks they are exposed to through such correspondent banking relationships. At a minimum, banks should assess that the due diligence measures performed by HO or another entity within the group are adequate and meet the requirements of the Notice. Banks should also refer to paragraph 4-6(b)(i) and (ii) of the Guidelines to the Notice when performing assessment of the ML/TF risks of countries and jurisdictions.

Assessing the Suitability of the Respondent FI

3.4 As part of a robust information gathering process, banks obtain information on the respondent FI and its management, including the shareholding structure, beneficial owners, directors and senior management of the respondent FIs. Using a risk-based approach, banks make inquiries and perform due diligence checks on the beneficial owners, connected parties and senior management of these respondent

FIs. Due diligence checks performed include name screening to identify sanctioned parties and Politically Exposed Persons ("PEP"). Banks' policies and procedures establish the type of information to be obtained as part of the bank's due diligence measures.

3.5 Banks' assessments typically take into account the respondent FI's reputation and the quality of supervision over the respondent FI. Banks could rely on information from the FATF mutual evaluation reports and statements on countries or jurisdictions as either being subject to countermeasures or having strategic AML/CFT deficiencies, and mutual evaluation reports by FATF-style regional bodies. Banks may also refer to publicly available information from competent national authorities and any restrictive measures imposed on a country, particularly prohibitions on providing correspondent banking or other similar services. In this regard, correspondent banks should pay particular attention when establishing or continuing relationships with respondent FIs located in jurisdictions that are subject to FATF countermeasures, or have strategic AML/CFT deficiencies, or have been identified as being "non-cooperative" in the fight against ML and TF.

3.6 In assessing respondent FIs' controls in regard to their ML/TF risk management, some banks relied on their respondent FIs' responses to the Wolfsberg Questionnaire, which has been designed to provide an overview of a bank's AML/CFT policies and practices. While this is one possible source for banks to understand the AML/CFT policies and controls of their respondent FIs, banks are expected to perform their own internal assessment on whether their respondent FIs have adequate controls against financial crime.

3.7 Banks' assessments should typically include discussions with the respondent FIs' senior management and Compliance functions on their AML/CFT awareness, risk management and compliance, and policies and procedures to combat ML/TF risks. It may also be useful to have discussions with the home regulators on the AML/CFT regulations and controls in respondent FIs' countries, and the standards of compliance by these respondent FIs. Where risks are assessed to be higher, the due diligence measures could also include a review of respondent FIs' policies and procedures, so as to better understand the ML/TF risks and compliance frameworks of the respondent FIs. Banks should ensure that these due diligence measures are not limited to completing "check boxes" in questionnaires and encompass qualitative assessments of the ML/TF risks posed by the respondent FI.

Sound Practices

In assessing the respondent FI's reputation and the quality of supervision over respondent FIs, some banks have adopted the following measures:

(a) Evaluate and perform a risk assessment of global regulators. The factors considered as part of the risk assessment include whether the regulator had put in place AML/CFT regulations and supervision in line with FATF standards, and the corruption index within the country, among others.

(b) Perform enhanced due diligence measures for respondent FIs located in jurisdictions that have strategic AML/CFT deficiencies or have been identified as "non-cooperative" in the fight against ML and TF.

Attention Areas

(a) Banks should identify and perform name screening on the respondent FI's beneficial owners, senior management and officers such as the Chief Executive Officer, the Chief Financial Officer and Chief Risk Officer to determine whether the respondent FI has connections to sanctioned parties or PEPs.

(b) On the quality of supervision over respondent FIs, some banks need to better document their assessment on the reputation of the respondent FIs and the quality of supervision over the respondent FIs.

(c) A review of the respondent FI's responses to the AML/CFT questionnaire should be performed and the outcome of such a review should be factored into the assessment of the respondent FI's ML/TF risk rating. Banks should also follow up with respondent FIs that do not reply to such questionnaires.

(d) Banks should not base their assessment of the adequacy of AML/CFT controls of the respondent FI on the AML/CFT questionnaire completed by the respondent FI without further due diligence to establish the quality of the respondent FI's AML/CFT controls. Such due diligence could include a more detailed discussion of AML/CFT controls with senior management and the Compliance function of the respondent FI, to assess its AML/CFT awareness, risk management and compliance with international standards.

Due Diligence in relation to "Nested" Correspondent Banking Relationships

3.8 Due diligence in relation to "nested" correspondent banking relationships[13] needs to be robust. Such downstream clearing relationships operated by the respondent FI for other FIs with weaker AML/CFT controls, could present higher ML/TF risks, if the transactions flow through the correspondent bank. Banks should ensure that appropriate enquires are made on "nested" relationships, including carrying out visits to and discussions with the respondent FI and ensuring that the respondent FI has conducted adequate due diligence on such relationships. In this regard, banks should institute more due diligence measures when establishing and continuing correspondent banking accounts where there are "nested" relationships. More attention should be accorded to new relationships and respondent FIs domiciled in high risk jurisdictions.

Sound Practices

(a) Some banks have a committee consisting of front office, risk and compliance representatives for reviewing due diligence measures performed on respondent FI clients.

(b) Some banks' due diligence measures include site visits or calls to understand the respondent FI's AML/CFT controls, customer base and whether nested banking relationships are involved.

Attention Areas

(a) Banks should put in place a process to identify "nested" correspondent banking relationships and set out policies and procedures for assessing such "nested" relationships.

(b) Banks should consider assessing the AML/CFT controls of downstream correspondent clearers and request the list of downstream correspondent clearers to which their respondent FIs provide downstream clearing services, and perform enhanced due diligence through screening checks on these downstream respondent FIs. These requirements should be formally updated in the banks' policies and procedures to ensure a consistent assessment of such downstream clearing relationships.

[13] Nested correspondent banking refers to the use of a bank's correspondent relationship by a number of respondent FIs (also known as "correspondent clearers") through their relationships with the bank's direct respondent FI to conduct transactions and obtain access to other financial services.

Prohibition against Establishing Correspondent Banking Relationships with Shell FIs

3.9 Correspondent banks should not enter into or continue a correspondent banking relationship with a shell FI, which is a FI incorporated in a jurisdiction in which it has no physical presence or which is unaffiliated with a regulated financial group. A correspondent bank should also satisfy itself that its respondent FI does not permit the latter's accounts to be used by shell FIs.

B Due Diligence on Group Relationships

3.10 The inherent risks of correspondent banking exist even when the service is offered to a bank's own overseas branches, subsidiaries and affiliates, as they may engage in business with customer types that pose varying levels of financial crime risks and may operate in a jurisdiction that is of higher risk for financial crime. In addition, the level of AML/CFT controls, and the corresponding risk profile, could differ among the group entities.

3.11 Correspondent banks are required to carry out adequate due diligence on each of the respondent FIs, even though they may be a branch, subsidiary or affiliate of the parent bank, on which due diligence had been done. Banks are required to take into account the potential ML/TF risks inherent in each respondent FI and the AML/CFT controls in place. This serves to combat the risk of illicit or terrorist funds flowing through the correspondent bank. All such relationships must be approved by senior management.

Attention Areas

Banks should perform due diligence measures on branches and subsidiaries within the group.

C Ongoing Monitoring of Respondent FIs

3.12 Banks perform ongoing monitoring of correspondent banking relationships for all respondent FIs. The ongoing due diligence process includes the performance of periodic due diligence reviews, sanctions screening, adverse news monitoring and transaction monitoring.

Ongoing Monitoring and Periodic Due Diligence Reviews

3.13 Periodic due diligence reviews should be performed for all respondent FIs to determine if the respondent FIs, their connected persons (such as new or existing executive directors), senior management and authorised signatories have been listed as PEPs, sanctioned persons or persons involved in or suspected of being involved in criminal activities since the initial due diligence was performed during the on-boarding process.

3.14 Banks adopt a risk-based approach, usually based on the risk rating assigned to each respondent FI, in determining the due diligence information to be reviewed and updated on a regular basis. For instance, correspondent banking relationships that pose higher risks are subject to annual reviews and closer account monitoring. Some banks, as part of ongoing monitoring and periodic due diligence reviews, review customers' actual transaction activities vis-à-vis expected and past transactions, in respect of volumes, values, frequency and nature of transactions. For banks to perform such reviews, banks need to enquire and understand the projected account activity of its respondent banks so as to better monitor the transactions of the correspondent banking accounts.

Sound Practices

During the periodic due diligence review of respondent FIs, a bank analyses transactions over the last three months to assess if the transaction patterns are consistent with the respondent FI's profile and projected account activity. Another bank analyses and compares expected volume of transactions with the actual volume of transactions over the past 12 to 24 months to detect any suspicious activities during the annual due diligence review.

Attention Areas

Banks should perform ongoing monitoring and periodic due diligence reviews of respondent FIs subsequent to customer on-boarding. Such periodic reviews should also include a review of the respondent FI's account activity.

Name Screening and Adverse News Monitoring

3.15 The ongoing due diligence process, particularly in regard to monitoring for adverse news and screening of respondent FIs, needs improvement. This process enables banks to monitor the reputation of respondent FIs and consider if the adverse information would be sufficient cause to perform a review on the relationship

and if a higher risk rating should be assigned to the respondent FI. Audit trails of due diligence measures, including any screening performed, should be maintained.

Attention Areas

Banks should take into account adverse news on respondent FIs in the public domain and assess if such news would result in a change in the ML/TF risk rating assigned to the respondent FIs and a corresponding change in the required level of due diligence and ongoing monitoring required.

Transaction Monitoring

3.16 Correspondent banks should put in place appropriate transaction monitoring policies and procedures to be able to detect any activity that is not consistent with the purpose of the services provided to the respondent FI or which is not in line with the usual or expected activities of the respondent FI. As part of transaction monitoring, banks should monitor flow of funds to sanctioned entities and countries, to safeguard themselves from being used as a conduit for financial crime. Transaction monitoring should be conducted for both AML and CFT purposes and banks should consider the scenarios, parameters and thresholds used for the monitoring of correspondent banking activities, taking into account that these activities pose different risks compared to other activities of the bank. Banks should conduct sanctions screening to ensure that the correspondent banking accounts are not used for transactions with or payments to sanctioned parties.

Attention Areas

(a) Transaction monitoring systems and reports to detect unusual or suspicious pattern of activities that are inconsistent with the purpose of the services provided to or the expected activities of the respondent FIs should be implemented and made available to staff for ongoing monitoring purposes.

(b) Banks should ensure that their transaction monitoring systems are able to detect unusual transaction patterns and also take into account detection scenarios and thresholds specific to the banks' correspondent banking activities.

4 CONCLUSION

4.1 It is vital that banks establish and maintain robust AML/CFT risk management systems and controls to manage and mitigate the financial crime risks arising from trade finance and correspondent banking relationships. It is imperative that senior management set the right tone at the top and inculcate an appropriate risk and compliance culture amongst its staff, across all levels and functions, to ensure effective implementation of a strong AML/CFT framework.

4.2 Banks are expected to periodically review their policies and processes taking into account changes in the operating environments and regulatory developments. Banks should also devote attention to raising the effectiveness of their AML/CFT controls through adequate systems, processes, staff expertise and training.

4.3 For Singapore to maintain her reputation as a clean and trusted commercial, trading and transportation hub, banks must ensure that their AML/CFT controls remain effective and are commensurate with the size, nature and complexity of their business.