ABS Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism

(13 November 2015)

Introduction

The Association of Banks in Singapore (ABS) issued its first Guidelines, "Prevention of the Misuse of the Singapore Banking System for Drug Trafficking and Money Laundering Purposes", in 1990. It revised the Guidelines in 1994, 2001 and 2009 to reflect the changes in domestic laws and international standards. The Guidelines supplement the Monetary Authority of Singapore (MAS) Notice and accompanying Guidelines on the *Prevention of Money Laundering and Countering the Financing of Terrorism*.

This update continues to consider the MAS' Notice and Guidelines, as well as the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A)* (CDSA), the Financial Action Task Force (FATF) Recommendations and other relevant international best practices.

It addresses the concerns and requirements of investment and commercial banking, private banking, retail banking and trade finance.

The ABS recommends using these Guidelines to preserve, nationally and internationally, the good name of the banking community in Singapore.

These Guidelines apply to all ABS member banks and institutions, as well as the foreign branches and subsidiaries of Singapore-incorporated banks. Where the laws of the foreign jurisdictions differ or conflict with these Guidelines, the foreign branches and subsidiaries shall comply with the more rigorous of the 2 and shall inform the bank's head office accordingly.

These Guidelines are industry best practice meant for all ABS member banks in relation to preventing money laundering (ML) and terrorism financing (TF). Member banks are advised to identify the risks associated with the businesses and services they provide, so that they can adopt suitable mitigating controls.

Table of Contents

1 Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Fundamentals

1.1 Definition of Money Laundering

Money laundering is the process criminals use to try to conceal the true origin and ownership of the proceeds of drug trafficking and other serious crimes listed in the Second Schedule of the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefit) Act (Cap 65A)* (CDSA) so that they appear to have originated from legitimate sources.

Typically, the 3 stages of money laundering (it is not always necessary for one or more of these stages to have occurred in any money-laundering scheme) are:

a. Placement: depositing cash proceeds from illegal activities into the mainstream financial system

   Objective: to get illicit cash into the financial system;

b. Layering: distancing illegal monies from the source by creating complex layers of financial transactions to disguise the audit trail, therefore providing anonymity

   Objective: to make detection as difficult as possible by attempting to break the linkage between the criminal and the proceeds of crime; and

c. Integration: making illegal funds appear legitimate

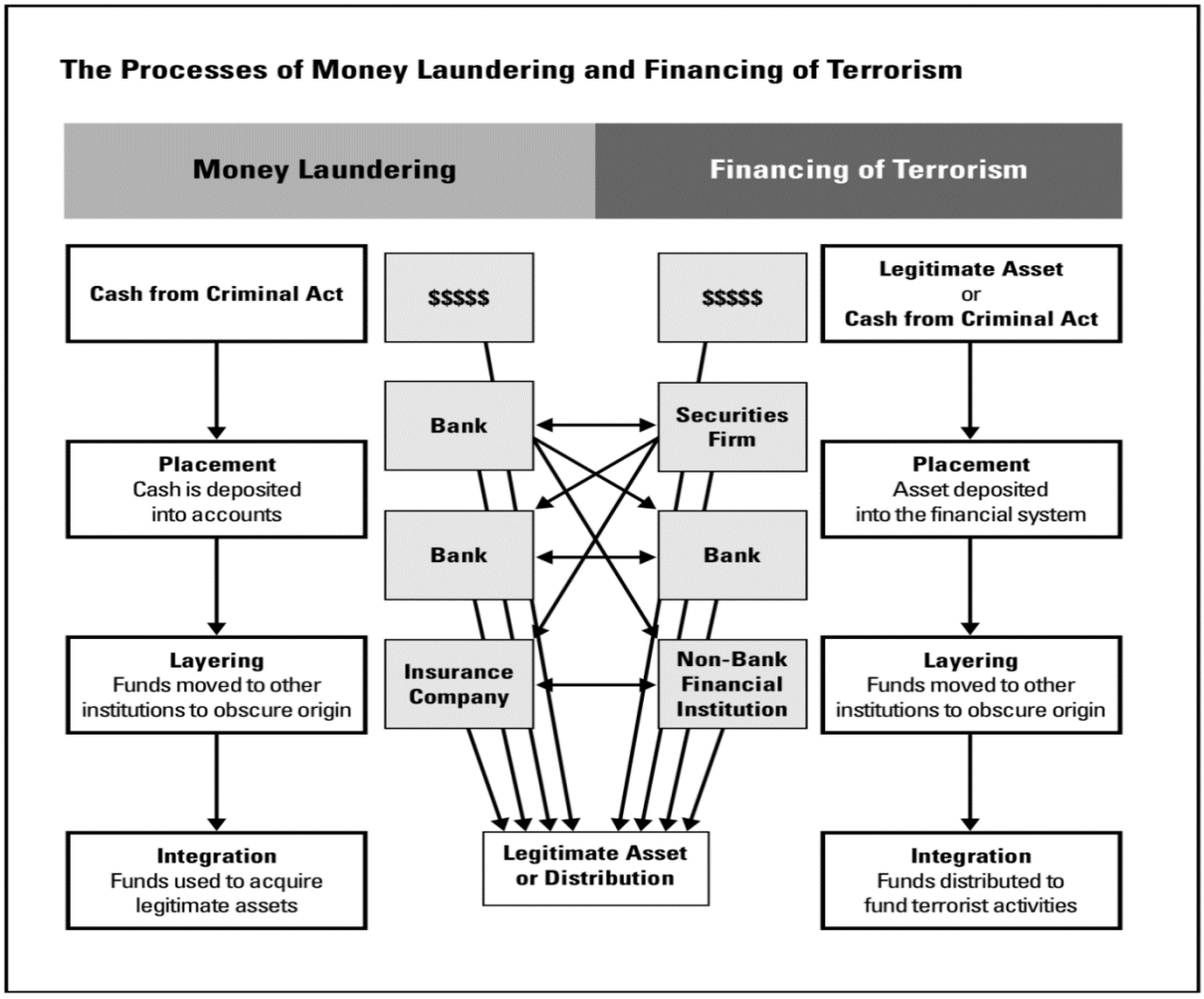
   Objective: to allow the laundered monies to re-enter the economy and appear as if it is from legitimate sources.

Refer to Appendix 1 for examples of placement, layering and integration.

1.2 Definition of Financing of Terrorism

The International Monetary Fund (IMF) defines terrorist financing, or the financing of terrorism, as "the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organisations. Funds may stem from both legal and illicit sources". Such legal sources may include donations or gifts of cash or other assets to organisations such as foundations or charities that in turn are used to support terrorist activities or terrorist organisations.

The techniques used to launder money are similar to those used to conceal the sources of, and uses for, terrorism financing. The diagram below from the World Bank training book shows the similarities between money laundering and terrorism financing.



Source: World Bank Training Book

The stages of money laundering described above may occur at any banking institution, depending on the nature of its products and services. The placement stage mainly affects retail banking as the activities relate to depositing money into bank accounts or buying monetary instruments such as money orders or cheques.

In the layering stages, the launderers or the terrorist financiers may use a series of wire transfers to distance themselves from the funds. Any institution with wire transfer services or remittance services would be at a higher risk of facilitating the layering stage.

In the integration stage, money launderers and terrorist financiers will generally use private banks and investment banks to get monies into the legitimate economy by making medium to long-term investments in ventures such as businesses and real estate.

1.3 Overview of the Singapore AML/CFT Regime

The following is an overview of the AML/CFT legal regime in Singapore and it is important that banks[1] are familiar with, and conduct their business operations, in compliance with the regime.

The first money-laundering prosecution in Singapore dates back to 2001. Teo Cheng Kiat, a former employee of Singapore Airlines, pleaded guilty to money laundering, among many other offences. The landscape has changed significantly since then, and authorities have intercepted a record number of money-laundering cases. According to the Commercial Affairs Department of Singapore, 29,082 Suspicious Transaction Reports (STRs) were submitted to the Suspicious Transaction Reporting Office (STRO) in 2014, a 30% increase on 2013.

As Singapore is a member of the Financial Action Task Force (FATF), banks in Singapore should heed the FATF statements released on the MAS website[2] from time to time. Banks are required to take appropriate actions and due diligence measures, as recommended by the FATF with respect to the named jurisdictions.

2 *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A)* (CDSA)

2.1 Predicate Offences

A predicate offence is an offence the proceeds of which may become the subject of a money laundering offence. Over time, legislation globally has broadened the definition of predicate offences to cover any serious crime, including terrorism financing activity and tax crimes. Money laundering predicate offences in Singapore are listed in the CDSA.

2.2 The CDSA defines 4 distinct predicate offences. An offence is committed under the CDSA when a person:

a. (i) conceals or disguises any property which (in whole or in part whether directly or indirectly) represents his/her benefits from drug trafficking or from criminal conduct; or (ii) converts or transfers that property or removes it from Singapore;

b. who, knowing or having reasonable grounds to believe, that any property (in whole or in part, directly or indirectly) represents another person's benefits from drug trafficking or criminal conduct, acquires that property without consideration;

c. knowingly assists a person to commit the first offence to avoid the prosecution of a money laundering offence or to avoid the enforcement of a confiscation order under the CDSA. The concept "knowingly" under this section implies both a subjective and an objective element; and/or

d. when a person enters into an arrangement, knowing or having reasonable grounds to believe that by the arrangement (a) the retention or control by or on behalf of another for that other person's benefits of Drug Trafficking or Criminal Conduct is

[1] Throughout these Guidelines, "Banks" will, where applicable, refer to banks licensed under the *Banking Act* and merchant banks licensed under the *Monetary Authority of Singapore Act*.

[2] www.mas.gov.sg/Regulations-and-Financial-Stability/Anti–Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti–Money-Laundering-and-Countering-the-Financing-of-Terrorism/AMLCFT-Announcements.aspx.

facilitated (whether by concealment, removal from Singapore, transfer to nominees or otherwise); or (b) that other person's benefits from Drug Trafficking or Criminal Conduct are (i) used to secure funds that are placed at that other person's disposal, directly or indirectly; or (ii) are used for that other person's benefit to acquire property by way of investment or otherwise and knowingly or having reasonable grounds to believe that the other person carries on/has carried on Drug Trafficking or engages/has engaged in Criminal Conduct and has benefited from these criminal activities.

2.3 Tipping-Off Offence

Tipping-off is the act of providing confidential information or advance notice on an investigation to another person, generally the customer, or somebody close to them, which is likely to prejudice the investigation. It is important to note that this includes situations where a disclosure is in the process of being made. It is vital that banking professionals understand, and manage their customers accordingly, to avoid being caught under this section of the law.

Under the CDSA, the tipping-off offence is covered as follows:

a. Disclosure Relating to Authorised Officer's Investigation & Lodging of STRs

Any person who:

i) knows or has reasonable grounds to suspect that an Authorised Officer is acting, or is proposing to act, in connection with an investigation which is being, or is about to be, conducted under or for the purposes of the CDSA; or

ii) knows or has reasonable grounds to suspect that a disclosure has been or is being made to an Authorised Officer under the CDSA; and

iii) discloses to any other person information or any matter which is likely to prejudice the investigation, or proposed investigation, or any investigation which might be conducted following the disclosure,

shall be guilty of an offence.

b. Disclosure Relating to Production Order or Search Warrant

i) Where, in relation to an investigation into Drug Trafficking or Criminal Conduct, as the case may be, an order under Section 30 (Production Order) has been made or has been applied for and has not been refused or a warrant under Section 34 (Search Warrant) has been issued, a person who, knowing or suspecting that the investigation is taking place, makes any disclosure which is likely to prejudice the investigation shall be guilty of an offence.

Under the CDSA, the penalty for tipping-off is a fine not exceeding S$30,000 or a jail term not exceeding 3 years or both.

2.4 Complying with Court Orders

A court order is an official proclamation by a judge (or panel of judges) that defines the legal relationships between the parties to a hearing, a trial, an appeal or other court proceedings. A court order must be signed by a judge; some jurisdictions may require it to be notarised.

The CDSA defines 5 distinct types of court orders. These are:

a. Production Order

All banks must comply with a production order issued by the High Court under Section 31(1) of the CDSA within a reasonable period, but not less than 7 days[3], as the order may specify.

Penalty: Production order

A person who fails to comply with a production order shall be liable on conviction to:

i) a fine up to S$10,000; or

ii) imprisonment up to 2 years; or

iii) both.

b. Search Warrant

All banks must comply with a search warrant the court issues under the CDSA.

Penalty: Search warrant

A person who hinders or obstructs an Authorised Officer in executing a search warrant shall be guilty of an offence and shall be liable on conviction to:

i) a fine up to S$10,000; or

ii) imprisonment up to 2 years; or

iii) both.

c. Restraint Order

d. Charging Order

e. Confiscation Order

Besides a production order and a search warrant, banks must also comply with a restraint order, charging order and confiscation order. A person who fails to comply with such court orders may be charged with contempt of court.

2.5 Record Keeping

All banks must retain all Financial Transaction Documents (FTDs) for the Minimum Retention Period (MRP) of 5 years.

A FTD includes any document relating to:

a. account opening/closing

[3] The period of time shall be reckoned in accordance with Order 3 of the Rules of Court (*Supreme Court of Judicature Act*).

b. operation of accounts;

c. safe deposit boxes;

d. wire transfers;

e. loan applications; and

f. records of customer identification.

Failure to retain these FTDs for the MRP is an offence punishable with a fine not exceeding S$10,000. In addition, where a bank is required by law to release an original FTD before the end of the MRP applicable to the document, the institution shall retain a copy of the document until the period has ended or the original is returned, whichever occurs first; failing which it is also liable to a fine not exceeding S$10,000.

Apart from the above documents required under the CDSA, the MAS also requires banks to retain:

a. CDD documents and information relating to:

   i) business relations;

   ii) wire transfers;

   iii) transactions undertaken without an account being opened;

   iv) account files;

   v) business correspondence; and

   vi) any analysis undertaken.

b. data, documents and information needed to explain and reconstruct transactions

for at least 5 years following the termination of such business relations or completion of such transactions. Under the MAS Act, a bank which fails to maintain CDD information as required under MAS Notice 626[4] shall be guilty of an offence and liable on conviction to a fine not exceeding $1 million, and to a further fine of $100,000 for every day during which the offence continues after conviction.

2.6 Extra-Territoriality

The CDSA, according to section 3(5), applies to any property situated in Singapore and elsewhere. This means that any person who launders property, even if the property is situated overseas, can be liable for a money laundering offence under the CDSA.

[4]Throughout these Guidelines, all references to MAS Notice 626 as it applies to banks will, where applicable, also include references to the corresponding MAS Notice 1014 as it applies to merchant banks.

2.7 Cross-Border Movements of Physical Currency and Bearer Negotiable Instruments

Part VIA of the CDSA aims to impose measures for disclosing information about movements of physical currency and bearer negotiable instruments into and out of Singapore for the purposes of detecting, investigating and prosecuting Drug Trafficking Offences and Serious Offences (Criminal Conduct). Please refer to Appendix 3 – ABS Guidelines on the New Cross-Border Currency/Bearer Negotiable Instruments Reporting Regime.

3 Countering the Financing of Terrorism Laws

3.1 The *Terrorism (Suppression of Financing) Act (Cap 325)* (TSOFA)

On 23 September 2013, the TSOFA was amended to implement changes to the anti-terrorism financing regime. The amendments consolidated the provisions in the United Nations (Anti-Terrorism Measures) Regulations and the TSOFA.

The TSOFA defines 4 types of offences relating to terrorism financing.

a. Providing or collecting property for terrorist acts

Every person who directly or indirectly, wilfully and without lawful excuse, provides or collects property:

i) with the intention that the property be used; or

ii) knowing or having reasonable grounds to believe that the property will be used,

in whole or in part, in order to commit any terrorist act, shall be guilty of an offence.

b. Providing property and services for terrorism purposes

Every person who directly or indirectly, collects property, provides or invites a person to provide, or makes available property or financial or other related services:

i) intending that they be used, or knowing or having reasonable grounds to believe that they will be used, in whole or in part, for the purpose of facilitating or carrying out any terrorist act, or for benefiting any person who is facilitating or carrying out such an activity; or

ii) knowing or having reasonable grounds to believe that, in whole or in part, they will be used by or will benefit any terrorist or terrorist entity,

shall be guilty of an offence.

c. Using or possessing property for terrorism purposes

Every person who:

i) uses property, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out any terrorist act; or

ii) possesses property intending that it be used or knowing or having reasonable grounds to believe that it will be used, directly or indirectly, in whole or in part, for the purpose of facilitating or carrying out a terrorist act,

shall be guilty of an offence.

d. Dealing with property of terrorists

No person in Singapore and no citizen of Singapore outside Singapore shall:

i) deal, directly or indirectly, in any property that he knows or has reasonable grounds to believe is owned or controlled by or on behalf of any terrorist or terrorist entity, including funds derived or generated from property owned or controlled, directly or indirectly, by any terrorist or terrorist entity;

ii) enter into or facilitate, directly or indirectly, any financial transaction related to a dealing in property referred to in paragraph (i); or

iii) provide any financial services or any other related services in respect of any property referred to in paragraph (i) to, or for the benefit of, or on the direction or order of, any terrorist or terrorist entity.

Any person who contravenes this prohibition shall be guilty of an offence.

If a person acts reasonably in taking, or omitting to take, measures to comply with Section 6 of the TSOFA, he shall not be liable in any civil proceedings arising from having taken or omitted to take the measures, if he took all reasonable steps to satisfy himself that the relevant property was owned or controlled by or on behalf of any terrorist or terrorist entity.

A person who commits a terrorism financing offence, if found guilty, shall be liable on conviction:

a. in the case of an individual, to a fine up to S$500,000 or to imprisonment up to 10 years, or both; or

b. in any other case, to a fine not exceeding S$1 million.

Disclosures relating to a police officer's investigation will constitute a tipping-off offence.

Any person who:

a. knows or has reasonable grounds to suspect that:

   i) a police officer is acting or is proposing to act, in connection with an investigation which is being, or is about to be, conducted under or for the purposes of the TSOFA; or

   ii) a disclosure or report has been or is being made under Sections 8, 9 or 10,

b. discloses to any other person information or any other matter which is likely to prejudice that investigation or proposed investigation, or any investigation which might be conducted following the disclosure or report,

   shall be guilty of an offence and shall be liable on conviction to a fine up to S$30,000 or to imprisonment up to 3 years or both.

It is a defence in proceedings under Section 10B(1) or (2) for a person to prove that he did not know and had no reasonable grounds to suspect that the disclosure was likely to be prejudicial in the way described in the relevant section.

3.2 Reporting Obligations

Disclosure of Information Relating to Property of Terrorists

Every person in Singapore and every citizen of Singapore outside Singapore who:

a. has possession, custody or control of any property belonging to any terrorist or terrorist entity; or

b. has information about any transaction or proposed transaction in respect of any property belonging to any terrorist or terrorist entity,

shall immediately inform the Commissioner of Police of that fact or information.

The Commissioner of Police may require such person to furnish such further information or particulars as the Commissioner may think fit. Any person who contravenes the above regulations shall be guilty of an offence.

It shall be a defence for a person to prove that he had a reasonable excuse for not informing the Commissioner of Police.

Disclosure of Information about Acts of Terrorism Financing

Every person in Singapore who has information which he knows or believes may be of material assistance:

a. in preventing the commission by another person of a terrorism financing offence, or in securing the apprehension, prosecution or conviction of another person, in Singapore, for an offence involving the commission, preparation or instigation of a terrorism financing offence; and

b. who fails to disclose the information immediately to a police officer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding 5 years or to both.

It shall be a defence for a person charged with such an offence to prove that he had a reasonable excuse for not making the disclosure.

3.3 Penalties

A person who fails to disclose under Section 8 or Section 10(1) of the TSOFA shall be liable, on conviction, to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding 5 years or to both.

3.4 Court Orders

Section 11 of TSOFA allows the Attorney General to apply for a search warrant, seizure warrant, forfeiture order or restraint order against terrorist property. Banks must comply with such orders.

Failure to comply with a restraint order is a criminal offence punishable on conviction with a fine not exceeding S$50,000 or a term of imprisonment not exceeding 5 years or both.

3.5 Statutory Protection

No criminal or civil proceedings shall be taken against a person for any disclosure made in good faith under Section 8(1) or 8(2), or Section 10 of TSOFA.

The identity of a person making a disclosure or report pursuant to Sections 8, 9 or 10 of the TSOFA cannot be revealed in any civil or criminal proceedings, subject to the power of the court to permit inquiry and require disclosure under certain circumstances.

A bank to which a direction is issued (e.g. MAS Notices) or which is bound by any regulations (e.g. MAS Regulations) made by the MAS for the purposes of discharging or facilitating the discharge of any obligation binding on Singapore by virtue of a decision of the Security Council of the United Nations shall comply with the direction or regulations notwithstanding any other duty imposed on the bank by any rule of law, written law or contract.

A bank shall not, in carrying out any act in compliance with any direction or regulations made under Section 27A(1) of the MAS Act, be treated as being in breach of any such rule of law, written law or contract.

4 Risk Assessment and Risk-Based Approach

4.1 Overview

The Singapore Government ran a nationwide exercise in 2013 to enhance and deepen the collective understanding of the ML/TF risks in the country. The results of the assessment were published in the *Singapore National Money Laundering and Terrorist Financing Risk Assessment Report* (NRA)[5] in 2014.

Banks are also required to carry out an Enterprise Risk Assessment (ERA) to identify and assess their ML/TF risks at all levels. The MAS Notice 626 allows banks to adopt a risk-based approach (RBA) when assessing their ML/TF risks.

The ABS recognises a diverse range of banks operate in Singapore. They differ in size, nature of business, and products and services offered. As a result, banks are advised to consider their ML/TF risks in light of their business activities, operating environment and customers when developing an ERA framework.

Banks shall identify, assess and understand their ML/TF risks. They should consider the following factors in their ERAs.

a. Customers (especially high-risk customers);

b. Countries or jurisdictions customers are from or in;

c. Countries or jurisdictions the bank operates in;

d. Products, services, transactions and delivery channels (especially those newly developed with new technologies, and that funds transfers);

e. Internal audit and regulatory findings;

f. Volume and size of transactions;

g. Investigations and suspicious transaction reporting; and

h. Training and communications.

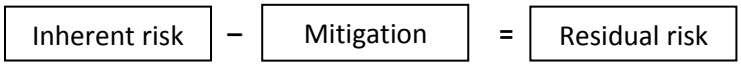
Banks should complement this information with information obtained from relevant internal and external sources, such as heads of businesses, relationship managers, national risk assessments, control lists issued by inter-governmental international organisations and national governments,

[5] Based on the NRA, Singapore's inherent ML/TF risks are high. Despite having a very low crime rate due to Singapore's tough enforcement of its strong laws, the country's role as an international transport hub and financial centre (with a significant foreign population) makes it a potential transit point for illicit funds for offences committed overseas. Singapore is exposed to money-laundering threats arising from foreign predicate offences (Singapore being used as a conduit to money launder foreign criminal proceeds). The main conduits are banks, remittance agents, shell companies and individual money mules. Similarly, due to Singapore's regional neighbours, there is a risk terrorism financing occurs. See www.mof.gov.sg/portals/0/data/cmsresource/Press%20Release/2013/Singapore%20NRA%20Report.pdf.

AML/CFT mutual evaluation and follow-up reports by the FATF or associated assessment bodies, as well as typologies.[6]

Banks should consider the results of Singapore's NRA Report in their enterprise-wide ML/TF risk assessment process. As the NRA Report is specific to the ML/TF risks in Singapore, banks should not simply project their results to their global presence without taking into account the ML/TF risks in other jurisdictions.

The consolidated assessment of a bank's ML/TF risks shall take into account its branches and subsidiaries, to allow the bank to assess its ML/TF risks holistically. Each bank should consider all relevant risk factors that contribute to its overall ML/TF risks, and institute appropriate mitigating controls using an RBA, to reduce the residual ML/TF risks to an acceptable level.



The scale and scope of ERAs should match the nature and complexity of each bank's business. The ERA should include all risk and compliance functions and all relevant stakeholders such as business functional heads and risk and compliance functions. The risk assessment should be documented, and approved by each bank's senior management and anti–money laundering governance committee (or equivalent).

Where the bank is a branch or subsidiary of a bank incorporated outside Singapore, the local senior management of the branch or subsidiary is responsible for reviewing and approving the risk assessment of the Singapore bank entity. The approved risk assessment should be current, and readily available for sharing with the MAS on request.

Each bank may conduct a consolidated ERA across businesses and legal entities within the financial group. However, each entity should be able to demonstrate to the MAS or its own auditors that its inherent ML/TF risks and mitigation measures adequately reflect the consolidated assessment, and controls have been strengthened where necessary.

Each bank should review its risk assessment at least once every 2 years, or when a material trigger event occurs, whichever is earlier. A material trigger event might alter the bank's ML/TF risks, and the bank should promptly update its risk assessment following such an event to assess the need for additional monitoring and control measures.

[6] www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf.

5 New Products, Practices and Technologies

5.1 Overview

Banks usually perform a "new product assessment" covering the risks (including credit, market, operational, liquidity, legal, regulatory and reputational risks) and controls before introducing new products, practices or technologies. Banks should also assess ML/TF risks prior to launching new products, practices and technologies.

Where the ML/TF risks of a new product, practice or technology are assessed to be material, banks should update their enterprise-wide risk assessment.

Where a system or operational enhancement does not have any ML/TF risk implications, for example a system that allows customers to print their statement, banks may choose not to perform a ML/TF risk assessment.

Where a new product, practice or technology does not involve moving funds or assets, the ML/TF risks could be lower, and may not affect the enterprise-wide risk assessment.

Each bank's local senior management and heads of businesses, risk and compliance is responsible for reviewing and approving the development and use of new products, practices and technologies, even if such roll-outs are global initiatives.

6 Customer Due Diligence

6.1 Risk-Based Approach

Risk-based approach (RBA) refers to the process that drives a dynamic framework for addressing risk. The RBA should strengthen controls where banks have identified high-risk concerns. The RBA would guide the customer due diligence (CDD) assessment and it should highlight high-risk concerns when evaluating the ML/TF risk of a new customer. MAS Notice 626 paragraph 4 provides an overarching regulatory expectation in the approach.

6.2 Customer Defined

Banks should refer to the MAS Notice for the definition of a customer. In addition, banks should screen names and adopt an RBA when performing due diligence on guarantors given that they will be the next source of repayment if a customer is not able to meet their obligations.

6.3 Customer Risk Assessment

Banks generally assess the ML/TF risk of a customer at the CDD stage and assign a score or risk rating. Once banks onboard a customer, they should use an RBA to review their transactional behaviour and activities, and update the customer's risk assessment

6.4 Know Your Customer

Know your customer (KYC) commonly refers to the process of understanding a customer.

MAS Notice 626 and the accompanying Guidelines apply to a wide range of banks including retail banks, private banks and investment banks, which have vastly different business products, services, processes and clientele.

Accordingly, while the MAS Notice and Guidelines outline minimum standards to guide banks on the requirements they must meet, how they do so may differ from bank to bank according to the size, nature and complexity of each bank's operations and business in Singapore. As a result, banks are advised to formulate CDD policies and procedures that suit their business operations.

Banks should note that under MAS Notice 626 paragraph 6.2, prior to establishing business relations or undertaking any transaction without opening an account, where a bank has reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct as defined in the CDSA, or are property related to the facilitation or carrying out of any terrorism financing offence as defined in TSOFA, the bank shall:

a. not establish business relations with, or undertake a transaction for, the customer; and

b. file a Suspicious Transaction Report (STR)[7], and send a copy to the MAS for information.

There are no set standards for undertaking CDD. Apart from the Guidelines to MAS Notice 626, banks may also take guidance from a Basel Committee Paper published in January 2014[8], which refers to an effective structure between the first line of defence and the second line of defence for capturing and assessing the required information of the customer and, if necessary, driving any escalation process. The KYC process is a key control in the AML/CFT framework and drives the other ML/TF controls such as monitoring and surveillance.

All banks must know their customers and understand the purpose of their accounts. This means that each bank must be able to establish the identity and some basic background information on their customers. Each bank must establish its own KYC program, tailored to suit the size, nature and complexity of its operations and business in Singapore.

Where a bank is unable to complete verification after factoring in the delayed verification allowed under paragraph 6.34 of the MAS Notice, the bank shall terminate or not commence the business relationship, and determine whether to file an STR. The bank's management should be kept informed of such occurrences.

Banks should institute policies, procedures and controls to mitigate the ML/TF risks arising from deferring the completion of verification, including:

a. having appropriate limits on the financial services available to the customer;

b. limiting the number, type and value of transactions that can be undertaken (e.g. limiting the amount of funds that can be deposited or not allowing withdrawals); and

c. closely monitoring procedures until verification is complete.

---

[7] Please note in particular Section 48 of the CDSA on tipping-off.

[8] www.bis.org/publ/bcbs275.pdf.

6.5 Customer Identification Program

The Customer Identification Program (CIP) sets the standards for what information should be gathered on the customer for identification and verification purposes. The program is generally driven by the regulatory requirements in the country in which the bank is operating, as well as the business risks associated with the bank's activities.

When banks in Singapore set up their CIP program, they should take into account the requirements of MAS Notice 626 paragraph 6. Completion of CDD measures entails obtaining customer information, screening the customer (including their connected parties, beneficial owners and natural persons appointed to act on their behalf) and verifying customer information.

Given the different nationalities of bank customers and that not all 5 customer identification information fields required under MAS Notice 626 may be available from a single customer identification document, banks should require customers to provide the necessary information using various identification documents.

Banks should identify and verify the identities of connected parties and beneficial owners as required under MAS Notice 626. They may apply an RBA based on an assessment of the ML/TF risks in each case.

In verifying the identity of a natural person appointed to act on a customer's behalf, where banks encounter genuine difficulties in obtaining proof of his residential address due to valid reasons, a business address may be used in situations where the assessed ML/TF risks are not high. Such assessments must be clearly articulated and documented.

6.6 Customer Due Diligence

The type of CDD assessment may depend on the type of customer, (e.g. whether retail or corporate) and many other factors. It is not limited to screening only politically exposed persons, and sanctions screening for name, adverse news and business assessment.

The assessment should highlight any high-risk concerns from an ML/TF perspective that would require enhanced due diligence.

When dealing with an unfamiliar or new customer, the bank should exercise caution and if the customer is assessed to be of a higher ML/TF risk, more information should be obtained to better understand the customer, their connected parties, beneficial owners, and natural persons appointed to act on their behalf.

Banks should be mindful when undertaking transactions for customers who are non-account holders. Two or more transactions undertaken by non-account holders may be related or linked if they involve the same sender or recipient. Such transactions may be entered separately to deliberately restructure an otherwise single transaction to circumvent the respective transaction and wire transfer thresholds of S$20,000 or S$1,500 to avoid CDD measures.

Apart from the 5 customer identification information fields that banks must obtain under MAS Notice 626, banks should also request each customer's telephone number. Banks should refer to Appendix A in the Guidelines to MAS Notice 626 on CDD information to be obtained for different types of customers.

Banks should ensure that CDD documents are current. If the bank becomes aware of material changes to a customer's information (e.g. change in nationality), and such changes are not reflected

in the CDD documents (even though they are within the validity period), updated CDD documents should be obtained from the customer.

Any bank staff may certify CDD documents to be true copies or confirm that he has sighted the original documents. Where a customer is unable to produce original identification documents for valid reasons, banks may apply an RBA and accept copies of identification documents (e.g. certificate of incorporation and board of directors' resolution) certified by an authorized person (e.g. company secretary) assessed to be independent. Banks should not accept certification of identification documents by a company director as he is not considered to be independent.

Banks may, using an RBA, accept electronic copies of certified true copies of CDD documents (e.g. a syndication loan arrangement[9]). To verify the authenticity of electronic CDD documents, such as proof of address (e.g. for credit card applications), banks may perform validation checks such as sending correspondence to a customer's address to test for returned mail.

CDD documents that are not in English should have the key clauses translated to facilitate the bank's KYC process. Such clauses should identify the customer, their connected parties, beneficial owners, and natural persons appointed to act on their behalf, and the purpose of the account, to allow assessment of the money laundering risks. For example, key clauses in the Memorandum and Articles of Association of a corporate customer in a foreign language should at least be sufficiently translated into English to show whether the customer is allowed to issue bearer shares. Similarly, key clauses in a company search document in a foreign language should be sufficiently translated to facilitate the identification of the customer's connected parties and beneficial owners.

Banks should obtain documentary proof that the appointed natural person is authorised to act on a customer's behalf. Such a document could be a board resolution authorising a person to act on behalf of a corporate customer, or a power of attorney authorising a person to act on behalf of an individual customer.

Under MAS Notice 626 paragraph 6.10, a bank has to identify and verify the identity of natural persons who act on a customer's behalf in establishing business relations. In the case of dealers (or staff members) of a bank or financial institution counterparty (customer) who executes trades on behalf of the counterparty but cannot move funds, such dealers (or staff members) can be treated like employees of the counterparty. There is no need to perform CDD on these dealers (or staff members). However, banks are expected to obtain periodic updates of the list of such dealers (or staff members) acting on behalf of their customers for risk management and control purposes.

6.7 Screening

MAS Notice paragraphs 6.39–6.42 set out the expectations of the standards in customer screening for banks operating in Singapore. Screening is fundamental to managing ML/TF risks and enhances sanctions compliance.

Banks are expected to have adequate systems, procedures and processes to screen any parties who are sanctioned or suspected to be involved with money laundering, terrorism financing or proliferation activities. Banks should document the results of screenings and assessments of potential matches.

---

[9] Refer to the respective ABS Anti–Money Laundering Principles sections in this document for more information.

It is important that screening tools be appropriately calibrated to capture name permutations and abbreviated or misspelt names. For sanctions screening, banks are encouraged to set lower thresholds. A 99% or 100% match setting would be unacceptable as banks risk not picking up sanctions hits. Banks should perform periodic back testing with different calibration levels to see if the screening throws up accounts with sanctioned parties, or those with adverse information.

As part of continuous monitoring, each bank shall maintain CDD information of its customers (and their connected parties, beneficial owners and natural persons appointed to act on their behalf) in its customer database for periodic name screening. This enables the bank to check for any incremental adverse news (including sanctions) associated with its customer base, for timely responses.

Banks must also screen all wire transfer originators and beneficiaries to check for the possibility of ML/TF and hits against sanctions lists (refer to Section 10 for more information on wire transfers). For transactions where the assessed ML/TF risks are lower such as where payments are only facilitated for account holders of banks in Singapore (e.g. local FAST/GIRO payments), banks need not conduct real-time screening of the originators and beneficiaries when processing these transactions.

If a bank has a positive hit against a sanctions list, it should stop all action on the account, assess if it is required to freeze the funds or other assets of the designated person or entity without delay and prior notice, and consider filing an STR. It should also consider re-assessing the risk rating of the customer and whether to terminate the business relationship.

6.8 Simplified Due Diligence

A bank need not inquire on the existence of beneficial owners in relation to a customer that has been assessed to be of low risk and for which it has no doubt on the veracity of CDD information, if the customer is:-

a. a Singapore Government entity;

b. a foreign government entity;

c. an entity listed on the Singapore Exchange;

d. an entity listed on a stock exchange outside of Singapore that is subject to:-

    i) regulatory disclosure requirements; and

    ii) requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, laws or other enforceable means);

e. a financial institution set out in Appendix 1 of MAS Notice 626;

f. a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF; or

g. An investment vehicle where the managers are financial institutions:-

    i) set out in Appendix 1 of MAS Notice 626; or

ii) incorporated or established outside Singapore but are subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

Where the bank has not made an inquiry on the existence of a beneficial owner in relation to a customer corresponding to (f) or (g)(ii) above, it should document the basis for its determination that the requirements under (f) or (g)(ii) have been met.

For Singapore Government entities, banks are not required to verify the identity of natural person(s) appointed to act on the customer's behalf as stated under paragraph 6.12 of MAS Notice 626. However, banks must obtain information to confirm that it is a Singapore Government entity.

Banks should, however, continue to monitor the relationships for which SDD were conducted including updating customer identification information, periodic screening of names and transactions in the transaction monitoring surveillance systems. Banks must scrutinise the transactions to ensure they are consistent with the bank's knowledge of the customer, their business and risk profile and, where appropriate, source of funds. Banks should pay special attention to all complex and/or unusually large transactions and unusual patterns of transactions that do not make economic, commercial or legal sense. Banks must support and document any assessment of low risk.

6.9 Enhanced Due Diligence

Enhanced due diligence (EDD) refers to the additional documents and/or reviews that are required to assess the risks associated with a customer following a high-risk concern identified in the CDD assessment. Such additional documents and/or reviews may also be triggered by other controls in the AML/CFT framework, such as alerts from transaction monitoring and inquiries from relevant authorities. Depending on the business segment of the bank, the EDD assessment may differ. EDD in private banking may differ from that in investment banking, commercial banking and retail banking. For more information, refer to the sector-specific ABS Anti–Money Laundering Principles in this document.

EDD measures relating to tax crimes may include checking for signs that funds are not proceeds from serious tax crimes, and establishing that complex structures are not being used to launder proceeds from serious tax crimes.

Banks should consider EDD measures for customers who live in and/or source funds from countries identified as having inadequate anti–money laundering standards or that represent a high risk for crime and corruption. Similarly, EDD measures may be warranted for customers who engage in sectors or business activities known to be susceptible to money laundering.

[PBIG – paragraph 3-2 and Wolfsberg PB Guidelines – paragraph 2.2]

6.10 Beneficial Ownership

MAS Notice 626 paragraph 2.1 defines the beneficial owner as the natural person who ultimately owns or controls a customer, or the natural person on whose behalf a transaction is conducted or business relations are established. It includes any person who exercises effective control over a legal person or legal arrangement.

MAS Notice 626 paragraphs 6.13–6.17 set the key regulatory expectations for identifying and verifying the beneficial owner.

Where the customer is a legal arrangement, banks should identify and verify the identities of the persons who have effective control or ultimate ownership of the arrangement (e.g. settlors, trustees and protectors). In cases with beneficiaries, banks should identify and verify the beneficiaries' identities before making any distributions to them.

For example, the Guidelines to MAS Notice 626 indicate a shareholding threshold of 25% for the determination of beneficial ownership in a legal person or legal arrangement. Banks are reminded that a natural person who does not meet the shareholding threshold, but who has effective control over the customer (e.g. through exercising significant influence), is considered a beneficial owner under the MAS Notice.

While banks may adopt the practice of obtaining an undertaking or declaration from customers to identify beneficial owners, such an undertaking or declaration does not absolve banks from the need to take reasonable measures to identify and verify the beneficial owners through independent documentary evidence (e.g. company search documents, certificate of incumbency, letter of undertaking from the nominated shareholder).

A similar approach could be taken to obtain declaration and clarification when the customer has a more complex ownership structure, such as a trust, a personal investment company or an entity with multiple layers of control. Banks must obtain adequate information to assess the plausibility of the reason for the complex ownership structure (usually tax planning or estate planning).

For individual accounts of natural persons, banks should take reasonable steps to establish that the account owner is also the beneficial owner. Banks must reasonably establish that a third party is not influencing the account holder, either for monetary returns or through intimidation. It must establish that the mandated authorised signatory or Power of Attorney holder is not the beneficial owner and establish that the source of wealth and funds is consistent with the account holder's declared wealth and occupation. Banks should refer to the ABS Guidelines on "Reduced Mental Capacities" and identify red flags to help staff recognise such situations.

6.11 Politically Exposed Person

Under MAS Notice 626, a politically exposed person (PEP) is defined as a natural person who is or has been entrusted with prominent public functions, whether domestically, in a foreign country or in an international organisation. A list of prominent public functions is provided in the MAS Notice and it includes among other things "senior civil or public servants" and "senior executives of state-owned corporations".

Local "senior civil or public servants" include:

a. Parliamentary Secretary;

b. Permanent Secretary;

c. Deputy Secretary; and

d. Head and Deputy Head(s) of a statutory board, government agency or public authority.

Local "senior executives of state-owned corporations" include Chairman, Chief Executive and Deputy Chief Executive(s) of state-owned corporations (including government-linked corporations).

For appointments that fall outside the above list, banks should adopt risk assessments to determine the appropriate level of CDD, referring to the seniority, prominence and importance of the customer's role and appointment relative to the list.

Recommended guidance on a PEP and former PEP

When assessing whether a customer is a PEP, banks should consider:

a. an individual who is or held a prominent public function which includes the roles held by a head of state, a head of government, government ministers, senior civil or public servants, senior judicial or military officials, senior executive of state-owned corporations, senior political party officials, members of the legislature and senior management of international organisations. This will also include family members and close associates of a PEP; and

b. a middle ranking or more junior official of any of the above categories would generally not be considered a PE P.

In relation to the due diligence of a former PEP, FATF Recommendation 12 provides guidance as follows:

a. the handling of a customer who is no longer in a prominent public position should be based on an assessment of risk and not on prescribed time limits. Possible risk factors include the level of (informal) influence the individual could still exercise and the seniority of the position the individual held as a PEP and whether the individual's previous and current function are linked; and

b. banks should not simply prescribe a time limit for removing such status after the PEP ceases holding office. Instead, banks should calibrate their assessment

and due diligence by determining when a former PEP's influence diminishes or becomes less vulnerable to corruption after the individual steps down from their prominent public function.

Banks are reminded of the need for the approval process for onboarding PEPs (and other higher AML risk customers). Banks must ensure that appropriately designated senior management personnel approve higher risk customers to ensure compliance with the AML/CFT Notice. The risk of onboarding the PEP (and other higher anti–money laundering risk customers) must be made known to the relevant line(s) of business.

Banks should have a list of unacceptable customers and customer categories, which they should update periodically. Banks may wish to visit the links below for information on jurisdictions that restrict PEPs or public officials holding foreign bank accounts.

a. www.ey.com/Publication/vwLUAssets/EY-Legal-Alert-30-December-2014-Eng/$FILE/EY-Legal-Alert-30-December-2014-Eng.pdf.

b. www.transparency.org/files/content/corruptionqas/287_Foreign_exchange_controls_and_assets_declarations.pdf.

c. www.kenyaembassy.com/pdfs/The%20Constitution%20of%20Kenya.pdf.

d. http://unpan1.un.org/intradoc/groups/public/documents/aapam/unpan038432.pdf.

e. www.business-anti-corruption.com/country-profiles/the-americas/venezuela/initiatives/public-anti-corruption-initiatives.aspx.

In addition, Transparency International's corruption index may help with assessing vulnerability to corruption. Banks may also refer to the *Wolfsberg Anti-Corruption Guidance 2011*, which applies generally to the financial services industry.

6.12 Source of Wealth and Source of Funds of PEPs

Paragraph 8.3 (b) of MAS Notice 626 requires banks to establish, by appropriate and reasonable means, the sources of wealth and funds of a customer or beneficial owner.

The source of wealth relates to how the customer acquired the wealth and banks should obtain an indication of the size of the customer would be expected to have. The source of funds refers to the origin of the funds or assets that are the subject of the relationship with the bank. Banks should ensure that these funds and/or assets are not proceeds of crime, including those arising from tax evasion.

Banks should continue to rely on their respective AML/CFT questionnaires and procedures to obtain information about the source of wealth and/or funds of their customers or beneficial owners.

Given the public profile and media coverage of PEPs, public domain information is useful for determining a PEP's source of wealth and/or funds. Banks, however, need to be satisfied the information source is credible before relying on it.

In the case of a domestic or an international organisation PEP, where the PEP individual does not have control and voting powers over the customer (e.g. children of a PEP or a PEP as an independent

director of an entity) or where the PEP individual is not the source of funds or wealth, banks shall adopt an RBA to determine the applicability and/or extent of EDD measures.

6.13 Ongoing Monitoring

As part of ongoing monitoring, banks may adopt an RBA to update CDD information after a periodic review or trigger event for a high-risk customer, and after a trigger event for non–high risk customers.

Where practical, taking an RBA, banks should periodically ask customers to confirm that the CDD information (e.g. a certificate of incumbency or a register of directors or shareholders) is still valid. Banks should obtain updated CDD documents when relevant customer information changes (e.g. change in directors, shareholders or authorised persons).

Banks should consider drawing up scenarios and parameters for monitoring transactions that may be linked, such as transactions involving the same customers as either the originators and/or beneficiaries. Banks should centrally monitor transactions carried out by the same customers across different business lines within the bank for a holistic review.

Parameters and thresholds should be set and refined to ensure that they are appropriate for detecting unusual bank-wide customers' transactions. The effectiveness and efficiency of these transaction monitoring parameters and thresholds should be periodically assessed by personnel independent of business users. Identifiable transaction trends should be incorporated into the banks' AML/CFT risk assessment framework to strengthen the banks' defences against money laundering, terrorism financing and proliferation financing. These may also be shared with appropriate personnel, including front office and compliance staff members.

Where it is not practical to set up relevant parameters and thresholds to monitor bank-wide transactions, banks should at least set up these measures within each business unit. This allows prompt sharing of any suspicious transactions of a common customer across business units, and provides a more holistic assessment of the ML/TF risks the customer poses.

Alerts and hits generated by transaction monitoring systems should be dealt with and the justification documented. Banks should institute controls to ensure that such alerts and potential hits are duly and promptly processed.

To comply with the revised MAS Notice 626 which took effect from 24 May 2015, banks need to carry out a remediation exercise to retrospectively revisit CDD information for customers which they have onboarded before the above date. An RBA should be considered when prioritising the CDD remediation exercise so that higher risk customers are reviewed first.

7 Reliance on Third Parties

7.1 Reliance on Third Parties Versus Outsourcing Arrangements

Reliance on third parties occurs when the CDD is based on the AML/CFT policies, procedures and controls of the third party and not the bank's own AML/CFT policies, procedures and controls. In contrast, under an outsourcing arrangement, the service provider will perform the CDD based on the bank's own AML/CFT policies, procedures and controls.

7.2 Syndicated Facility Transaction

Where the bank's assessment of the customer's ML/TF risk is higher than the lead arranger's assessment, the bank should perform its own CDD and apply its own requirements. This allows banks to apply controls that are more stringent and monitoring of the customer meets their own AML/CFT risk and control framework.

Banks are reminded that even though third parties perform CDD measures, banks are responsible for ensuring that the measures are adequate and meet Singapore's regulatory requirements. Banks are encouraged to perform sample checks to assess whether third party CDD is satisfactory, as the bank is ultimately responsible for complying with local AML/CFT regulatory requirements.

8 Correspondent Banking

8.1 Overview

This section on Correspondent Banking guides banks on the AML/CFT controls banks should consider when providing correspondent banking services. Correspondent banking activities present inherently higher money laundering and financing of terrorism risks given that correspondent banks may not have full visibility of the nature and/or purpose of the underlying transactions when executing instructions from a respondent bank or financial institution (collectively referred to as "respondent bank" hereafter). Banks should also refer to the *MAS Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking* issued on 22 October 2015.[10]

8.2 Correspondent Account

Often referred to as a nostro or vostro account, a correspondent bank account is established by a (respondent) bank with a (correspondent) bank for the latter to assist in receiving deposits, making payments or handling other financial transactions. In other words, a correspondent bank is the bank that is providing the correspondent banking services, while the respondent bank is the bank using these account services, whether foreign or domestic.

A respondent bank would usually open a correspondent bank account in a foreign country to facilitate its transactions in that country's currency. Similarly, domestic correspondent bank accounts may be opened to facilitate transactions in the local currency.

---

[10] www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Guidance%20on%20AML%20CFT%20Controls%20in%20Trade%20Finance%20and%20Correspondent%20Banking.pdf.

8.3 Correspondent Banking Services

Correspondent banking refers to a bank that provides a demand deposit, current or other liability account to another bank in an account relationship. Correspondent banking (and similar) services would generally include, but are not limited to:

a. cash management;
b. international funds transfers;
c. cheque clearing;
d. payable through accounts;
e. pouch activities;
f. bulk cash activities;
g. third-party payments; and
h. trade finance services, such as:
    i) advising;
    ii) confirming; and
    iii) negotiating.

Please note that foreign exchange and money market transactions do not fall within the scope of "similar services".

Given the nature of correspondent banking services, banks are not always able to identify the beneficial owner(s) in a transaction. For this reason, banks should perform appropriate CDD measures on respondent banks when they act as intermediaries of these beneficial owner(s), to check that their AML/CFT regimes are as stringent as Singapore's or are also subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

Under MAS Notice 626, banks in Singapore shall perform the following measures, in addition to CDD measures, when providing correspondent banking or other similar services:

a. Assess the suitability of the respondent bank by:
    i) gathering adequate information about the respondent bank to understand fully the nature of the respondent bank's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
    ii) determining the reputation of the respondent bank and the quality of supervision over the respondent bank from available information sources, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and
    iii) assessing the respondent bank's AML/CFT controls to make sure that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which it operates;
b. Clearly understand and document the respective AML/CFT responsibilities of each bank; and
c. Obtain approval from the bank's senior management before providing correspondent banking or similar services to the respondent bank.

As part of due diligence, banks may consider visiting or contacting the respondent banks to assess their AML/CFT risk awareness, controls and compliance culture. Banks may find it useful to visit the respondent banks' supervisory authority to gain a better understanding of their AML/CFT supervision and standards of compliance by the respondent banks. Banks should document call reports of such due diligence visits or contacts.

If banks are satisfied that the respondent banks' AML/CFT policies and procedures meet the FATF and Singapore AML/CFT standards, they may continue to rely on the KYC performed by the respondent banks. Otherwise, if banks are not able to mitigate the higher ML/TF risk, they should consider not establishing or continuing any correspondent banking relationship.

Banks are also reminded to ensure that proper and complete sanctions screening systems are in place for screening requested incoming and outgoing funds transfers as part of correspondent banking services. This will facilitate the detection of any undesirable transactions for appropriate follow-up actions (please refer to paragraph 6.7 for examples of required actions).

Separately, in a SWIFT Relationship Management Application (RMA) situation, banks should adopt an RBA in performing KYC on the respective financial institution's management. For example, where the SWIFT RMA relationship involves only non-authenticated and/or non–payment related messages with a bank or financial institution supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, then a lower level of due diligence may be applied.

8.4 Due Diligence Considerations

The due diligence program should include appropriate, specific, risk-based procedures and controls designed to ensure that the correspondent bank is able to detect and report suspicious money laundering activity conducted through the account opened for the respondent bank.

The initial due diligence program should try to determine the:

a. nature and/or markets and type of anticipated activities of the respondent bank;
b. respondent bank's ownership structure, and the character and integrity of the management structure;
c. respondent bank's reputation and quality of supervision; and
d. strength of its AML controls, having regard to the regulatory regime and jurisdiction where it operates.

The above would drive the need for further assessment of the respondent bank, depending on the risk appetite of the correspondent bank, i.e. determining the high-risk customers. When assessing a higher risk customer, the correspondent bank should consider other measures, including a more thorough due diligence assessment of the respondent's AML/CFT framework and underlying controls, a more in-depth understanding of the respondent's customer base, and a review of the high-risk indicators, such as using shell banks (prohibited under MAS Notice 626), payable through account services and numbered accounts.

Below are examples of high-risk indicators:

a. Payable through account (PTA)

i) *What is a PTA?*
A PTA is also known as a pass-through account or pass-by account. It is a sub-account established for the customer of the respondent bank under the correspondent account of the respondent bank.

ii) *Why does a PTA bring about heightened ML/TF risks?*
A PTA allows the customer of the respondent bank to have direct access to the account instead of going through the respondent to transact on their behalf. Hence, the correspondent bank may not have access to information about the third parties accessing the account. The operational aspects of

such accounts make them vulnerable to abuse as the account holder can have numerous users and the correspondent bank may not have full oversight of the instructing party (customer of the respondent bank).

b. Offshore banking licence

i) *What is an offshore banking licence?*
Banks that operate under an offshore banking licence are prohibited from conducting activities with the residents of the licensing jurisdiction or in their local currency. However, they will have the authority to deal with citizens of other countries.

ii) *Why does such a licence bring about heightened ML/TF risks?*
There is a risk that the local government or enforcing authority has less incentive to have appropriate oversight of the offshore banking institutions. Therefore, there could be a risk of lesser AML/CFT controls over such business activities by the respondent bank. It is important then for the correspondent bank to understand the AML regime of the respondent bank operating under such a licence when reviewing this high-risk indicator.

c. Shell bank

i) *What is a Shell Bank?*
A shell bank is a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

ii) *Why does such a bank bring about a heightened ML/TF risk?*
Such banks are generally unregulated and have no incentive to have any AML/CFT controls in place; therefore a correspondent bank needs to ensure that its respondent customers have prohibition policies for such banks. Please note that banks in Singapore are not allowed to open any account or undertake any transaction with or for shell banks, whether directly or indirectly.

8.5 Ongoing Due Diligence Considerations

The due diligence program for correspondent banking must be updated periodically. The frequency of updates and the extent of CDD can be based on an RBA where the frequency should increase and enhanced CDD be performed for higher ML/TF risk customers

Banks should have 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 financial institutions and may be related to money laundering and/or terrorism financing.

9 Wire Transfer

9.1 Overview

Where a name screening check produces a positive hit, banks should have a protocol for the investigation and escalation of the hit, as well as the determination on whether to proceed with the wire transfer. The proposed action would require the concurrence of an independent reviewer. Banks should adopt the 4 eyes principle and put in place an approval matrix and escalation route.

9.2 Responsibility of the Ordering Institution

For joint accounts, the ordering institution shall provide all the joint account holders' information to the beneficiary institution. Where there are space constraints in the SWIFT message, the ordering institution may indicate in the wire transfer message that the originator information provided relates to a joint account holder to allow the beneficiary institution to request additional information as necessary.

9.3 Responsibility of Beneficiary Institution

Where an incoming wire transfer is not accompanied by complete originator information, a beneficiary institution should request the information from the ordering institution (e.g. when it is indicated in field 72 that the ordering party is a joint account holder). Banks should consider rejecting incoming wire transfers or terminating business relations with overseas ordering institutions that fail to provide adequate originator information. Banks should be mindful of any legal and regulatory requirements that may be imposed on overseas ordering institutions in relation to cross-border wire transfers.

Where it is against the laws or regulations of the country of the ordering institution to provide the required information, the bank should assess the AML/CFT regulatory requirements in the ordering bank's jurisdiction, and the AML/CFT risk arising from the incomplete information. Once the assessment is complete and the proposed action determined, an independent reviewer must concur with the proposed action.

For money transfers such as those executed through Visa Direct and MasterCard MoneySend, a bank may not be able to screen the name of the originator, given the unavailability of such information. However, banks should, at a minimum, perform due diligence on the service providers.

9.4 Responsibility of the Intermediary Institution

The intermediary institution is not required to verify the identities of wire transfer beneficiaries given that these beneficiaries are not their customers. However, the intermediary institution is required to identify and screen all wire transfer originator and beneficiary information.

10 Suspicious Transaction Reporting

10.1 Overview

A Suspicious Transaction Report (STR) is made when a person knows or has reason to suspect that property is directly or indirectly linked to criminal conduct, and the knowledge or suspicion arose during the course of the person's trade, profession, business or employment. The "transaction" usually refers to a financial transaction. Such reports are lodged with the Suspicious Transaction Reporting Office (STRO) of the Commercial Affairs Department.

It is important to note that a physical transaction need not have occurred for a report to be required, leading many people to adopt the term "Suspicious Activity Report" (SAR) rather than STR.

Reporting a suspicious transactions under the CDSA is mandatory and failure to do so is a crime punishable with a fine up to S$20,000. Reporting can be done via a general disclosure under Section 39(1) of the CDSA or a specific disclosure under Sections 43(3) or 44(3).

A person who knows or has reasonable grounds to suspect that any property:

a. in whole or in part, directly or indirectly, represents the proceeds of;

b. was used in connection with; or

a. is intended to be used in connection with,

any act which may constitute drug trafficking or criminal conduct and the information or matter on which the knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, he shall disclose the knowledge or suspicion or the information or matter to an Authorised Officer as soon as is reasonably practicable after it comes to his attention.

Section 39(6) provides an exception to the general rule of disclosure to the Authorised Officer, stating that such disclosure "shall not be treated as a breach of any restriction upon the disclosure imposed by law, contract or rules of professional conduct and he shall not be liable for any loss arising out of the disclosure". Therefore "banking secrecy" would not undermine whistle-blowing actions against customers under the CDSA, although the statutory protection provided by Section 39(6) only extends to disclosures relating to drug trafficking and criminal conduct.

Banks should have policies and procedures for exceptional or extraordinary cases, including an escalation process, timing and action plan. Where a transaction is known to be part of an ongoing investigation by the relevant authorities, the bank should initially notify the STRO by telephone or email, and follow up according to STRO directions.

A bank should consider filing an STR if it receives any adverse news about a customer in relation to financial crimes. Filing an STR could facilitate a more effective investigation by the authorities, and prompt the bank to take preventive measures against the customer.

11 Proliferation Financing

11.1 Overview

According to FATF, "proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling and use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations".[11]

In the course of preventing ML/TF, banks should expand their scope to incorporate policies, procedures and controls to combat proliferation financing. These should consider the indicators of proliferation financing.

[11] www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf.

12 Sanctions

12.1 Overview

The MAS has issued regulations, announcements and a notice on sanctions that banks in Singapore must observe.

12.2 Sanctions and Freezing of Assets Regulations

The ABS notes that the MAS issues, pursuant to its powers under Section 27A(1)(b) of the MAS Act, regulations on sanctions and freezing of assets, which are available on the MAS' website.[12]

12.3 Notice on Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions

Banks in Singapore are banned from conducting transactions or business relationships with, or for the benefit of, a designated person[13], whether directly or indirectly. Any dealings must be approved by the MAS.

Banks should sign up for relevant email notifications from the MAS' website so that they are updated on the MAS' regulations on sanctions and freezing of assets, AML/CFT announcements and notices on prohibited transactions. They should promptly incorporate any changes into their ML/TF policies, procedures and controls. In respect of sanctions monitoring, the ABS recommends that:

a. banks assess their risk profiles and establish appropriate systems and controls to ensure they comply with sanctions requirements. These controls may include prohibiting transactions for or on behalf of a person or persons, and/or undertaking more due diligence to screen a person or persons in respect of sanctions requirements;

b. banks assess the risks of transactions or business relationship with people located in countries or jurisdictions sanctioned under a United Nation Security Council Resolution (UNSCR) as may be adopted by the FATF and the MAS, where appropriate;

c. banks assess which countries carry the highest risks and analyse transactions from countries or jurisdictions known to be a source of terrorism financing, particularly new business from such jurisdictions and when receiving inward payments for existing customers or inter-bank transactions;

---

[12] www.mas.gov.sg/Regulations-and-Financial-Stability/Anti–Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Targeted-Financial-Sanctions.aspx.

[13] A "designated person" under the Notice on Prohibition on Transactions with the Iranian Government and with Iranian Financial Institutions refers to

a. the Government of Iran;

b. the Central Bank of Iran, also known as Bank Markazi Jomhouri Islami Iran;

c. a financial institution in Iran;

d. a branch or subsidiary of a person or entity falling within subparagraph (b) or (c); or

e. a person or entity (whether corporate or unincorporate) owned or controlled, directly or indirectly, by any person falling within subparagraph (a), (b), (c) or (d).

d. transactions with counterparties located in countries or jurisdictions that are no longer identified as being sanctioned may still require higher-than-normal attention, particularly if FATF has identified that such countries or jurisdictions pose substantial ML/TF risks;

e. banks should, where relevant, acquire information on sanctioned countries and persons from available sources. For example, banks may obtain information from any domestic sanctions or blacklists issued by authorities, the consolidated list of the UNSCRs, financial sanctions in the European Union Office, HM Treasury (United Kingdom) lists, and the Office of Foreign Assets Control (OFAC) of the United States Department of Treasury; and

f. banks obtain available national and international information to check against their customer databases and records, as well as to monitor transactions.

13 Compliance, Audit, Employee Hiring and Training

13.1 Compliance

The key elements in paragraphs 13.2 to 13.7 below should help banks address key obligations and responsibilities in the fight against ML/TF.

13.2 Group Policy

A bank incorporated in Singapore shall develop and implement a group AML/CFT policy that considers its ML/TF risks, the size, nature and complexity of its business and operations both in Singapore and overseas, and communicate these to all employees in the financial group. It shall introduce safeguards to protect the confidentiality and use of any information that is shared within the financial group, abiding by the laws of Singapore and the jurisdictions where its branches and subsidiaries are located.

13.3 Appointment of a Compliance Officer/Department

A bank shall appoint one or more senior persons, or an appropriate unit, to advise management and staff on issuing and enforcing policies and procedures to promote compliance with AML/CFT regulatory requirements, including employee training, suspicious transaction reporting and addressing AML/CFT queries. At least one management-level AML/CFT compliance officer with sufficient seniority and authority within the bank must be appointed. The officer and assistants must be suitably qualified and given adequate resources and access to information to effectively discharge their responsibilities.

13.4 Internal Money Laundering Control Program

A bank shall set its own internal AML/CFT Guidelines and put in place an effective AML/CFT program that matches the size, nature and complexity of its operation and business in Singapore.

a. Know Your Customer Program

The Know Your Customer (KYC) program is central to a bank's AML/CFT control system. Banks must familiarise staff with their KYC program, which they must implement. The program should cover customer identification and customer transaction profiling to help staff members anticipate the likely business activities of a customer. The bank should also develop and implement

monitoring and surveillance processes, which are useful for detecting suspicious transactions.

b. Internal Reporting

Banks shall introduce an internal reporting system to investigate and report on suspicious transactions. Staff members should be trained to ensure they are familiar with the bank's internal reporting system, including the escalation process. Training should include examples of when to escalate suspicious transactions, and how to do so.

13.5 Audit

Banks shall maintain independent audit functions that have adequate resources to assess the effectiveness of the bank's internal policies and procedures, and its compliance with regulatory requirements regularly.

Where a bank is not able to maintain an independent audit function locally, the bank may consider outsourcing the internal audit function to conduct periodic audits, subject to regulatory guidelines on outsourcing.

Banks' AML/CFT framework should be subject to periodic bank-wide audits to assess the effectiveness of AML/CFT measures undertaken by the bank. The frequency and scope of the audits should match the ML/TF risks presented, and the size and complexity of the bank's business. Priority should be given to areas the bank assesses as high risk.

13.6 Employee Hiring

Banks shall develop screening procedures for hiring. These procedures should include but are not limited to:

a. background check with former employers;

b. screening for adverse ML/TF news;

c. bankruptcy searches; and

d. credit history checks (on a risk-based approach).

When another bank approaches a bank for a background check on a former employee, the bank should provide the information where practical.

13.7 Training

Banks should train their employees to detect unusual activities potentially related to ML/TF. This will help banks and their employees avoid prosecution for money laundering and related offences.

To ensure that adequate training is provided to all staff, including directors and management, appropriate programs pitched at the different levels are recommended. Each bank should adopt a training program according to its size, nature and the complexity of its business and operations in Singapore.

New employees should be trained as soon as possible. Refresher training should also be conducted at least every 2 years to ensure that all employees (regardless of seniority) are familiar with bank policies and regulatory developments related to ML/TF. Banks should maintain training records for auditing.

Banks should monitor training and attendance, testing employees' understanding of AML/CFT policies and procedures, and tracking incidents of non-adherence.

The training program should cover the legal aspects of, and typologies used, for ML/TF. It should provide for regular updates and refresher training pitched at employees' job functions and responsibilities.

14 Banking Secrecy and Personal Data Protection Act

14.1 Overview

Banks are reminded to honour Section 47 on banking secrecy in the *Banking Act* and the personal data protection provisions in the *Personal Data Protection Act 2012* (PDPA), and the need to use proper controls to protect customer information and data.

Banks shall:

a. be responsible for personal data in their possession or under their control;

b. develop and use policies and procedures that allow them to meet the requirements of the PDPA;

c. ensure that when they share information within their financial group for CDD and for ML/TF risk management, they do so within the laws of the countries or jurisdictions in which their branches operate;

d. appoint one or more individuals to be responsible for ensuring that their institution complies with the PDPA. The individual(s) may delegate responsibility conferred by that appointment;

e. not be relieved of their obligations under the PDPA by appointing an individual under paragraph (d);

f. establish a procedure to process complaints that may arise from applying the PDPA;

g. communicate to their employees the policies and procedures referred to in paragraph (b); and

h. make available on request the policies and procedures in point (b), and the complaint process in paragraph (f).

Banks should refer to the ABS Code of Banking Practices – PDPA for more detailed management of customer information.

ABS Anti–Money Laundering Principles for Investment and Commercial Banks (2015)

1 Customer Acceptance: General Principles

1.1 General

Banks offering investment and commercial banking services in Singapore should refer to the *Wolfsberg Frequently Asked Questions (FAQs) on Selected Anti–Money Laundering Issues in the Context of Investment and Commercial Banking*[14].

Historically, investment and commercial banks are not associated with high anti–money laundering risk, but banks should assess their customers (including financial institutions) for risk using an RBA to determine an appropriate level of due diligence to be performed.

1.2 Identification and Verification of Identity

Verification of Identity

Banks should take reasonable measures, and use documentary evidence, to verify identity when establishing a business relationship.

Examples of evidence for financial institutions, and corporate and partnership customers include ACRA Bizfile, DP Search, Certificate of Incorporation, Certification of Incumbency, Memorandum and Articles of Association, Letter of Good Standing, Partnership Agreement, stock exchange or regulator's web (or equivalent) information and Bankers Almanac.

Identification documents for verification purposes must be current and banks should obtain copies of these documents.

Syndicated loans

For a syndicated loan customer, CDD documents provided by the borrower to the lead arranger may be verified using relevant information from other public sources. In addition, except for the requirement on the lead arranger to perform appropriate CDD on lenders it invites to participate in the syndicated loan, the lenders are not obliged to perform due diligence on each other.

[Wolfsberg IBCB FAQ – Q.1]

[14] www.wolfsberg-principles.com/pdf/faq/Wolfsberg_IBCB_FAQs_(2006).pdf

Banks, depending on their role in a syndicated loan, should consider the following guidelines when performing CDD on the customer:

Role	Scenarios	CDD Procedures
Lead arranger	Onboarding of new customer	Perform CDD on the customer. The lead arranger should also have procedures for performing an appropriate level of CDD on lenders it invites to participate in the syndicate.
	Selling participation	If a participating bank wishes to sell off its participation, the lead arranger should, using an RBA, consider carrying out CDD on the prospective buyer where required (e.g. when adverse news has been noted on the buyer).
Participating bank	Onboarding of new customer	Participating bank to conduct CDD on lead manager (third-party reliance) to check that the lead manager meets the participating bank's anti–money laundering standard. If so, the lead manager can be relied on to perform CDD and obtain relevant CDD documents from customer. Otherwise, a participating bank should conduct CDD that meets local regulatory requirements.
	Selling of participation	If a participating bank wishes to sell off its participation, it should (using an RBA) consider carrying out CDD on the prospective buyer where required (e.g. adverse news noted on the buyer).
Secondary participating bank	Onboarding of new customer	Participating bank to conduct CDD on lead manager (third-party reliance) to check that the lead manager meets its anti–money laundering standard. If so, the lead manager may be relied on to perform CDD and obtain relevant CDD documents from the customer. Otherwise, the secondary participating bank should conduct CDD that meets local regulatory requirements.

When CDD documents (forwarded by the lead arranger) are not certified true copies, lenders may rely on a lawyer's letter of covenant, which should attest that the CDD documents are either certified true copies or that the lawyer had sighted the original documents.

[Wolfsberg IBCB Part C FAQ – Q.3 and 4]

1.3 Beneficial Owner

Financial Institution

Banks that have a financial institution (FI) customer that may be acting as intermediary for their own customer (institutional intermediary) may adopt an RBA to determine whether a simplified CDD may be applied, based on the understanding or confirmation that the FI is also subject to the same or higher anti–money laundering standards and are supervised for compliance.

[Wolfsberg IBCB Part A FAQ – Q.2]

1.4 Practices for Walk-In Customers and Non-Face-to-Face Banking Relationships

Services initiated through electronic channels are generally acceptable. However, banks are to ensure that the authorised personnel with whom they are dealing have a mandate from the FI customer. Banks are to perform CDD (identification and verification) on the authorised persons, and use appropriate measures to verify the identity of non-face-to-face customers.

2 Customer Acceptance: Situations Requiring Additional Diligence or Attention and Prohibited Customers

Where a complex transaction is involved, banks are to understand the structure of the proposed transaction and its purpose, and determine if the purpose of the transaction is consistent with its structure and whether the transaction makes economic sense.

[Wolfsberg IBCB Part B FAQ – Q.1]

3 Updating Customer Files

Financial Institution

Banks are reminded to update FI customers' files periodically. Updated CDD information may be obtained from the Bankers Almanac and/or directly from the FI customers via the banks' questionnaires. FI customers should be asked to confirm or attest that they comply with the same or a higher AML/CFT standard regime. Banks may adopt an RBA in updating the expired identity documents of the FI customers' authorised persons, with greater focus on foreigners and those with higher ML/TF risks.

ABS Anti–Money Laundering Principles for Private Banks (2015)

1 Customer Acceptance: General Principles

1.1 General

Banks offering private banking services in Singapore are recommended to refer to the Wolfsberg AML Principles on Private Banking, and the Private Banking Advisory Group's Private Bank Code and Industry Sound Practices, as long as these principles and guidance are consistent with the AML/CFT Notices and other relevant regulations.

Due to the higher inherent risks (large assets, high volume of cross-border transactions, higher risk and PEP customers) in private banking, banks must be very prudent when onboarding customers and use greater due diligence (including reviewing customers' historical transactions) during periodic reviews.

Before onboarding a customer, the private banker (PB) should assess the purpose of the account to be opened and that the sources of funds are legitimate. The assessments are to be documented and verified where required. The PB should confirm in writing that the information obtained during the due diligence process and while maintaining the account does not indicate that the funds are proceeds from serious tax crimes or are illegitimate. Where the PB is unable to make a definitive assessment of the customer, they should escalate the case to senior management or an appropriate approving authority for review and guidance.

[PBIG – paragraph 4-1]

Banks must inform customers of their stance against tax illicit activities, and communicate that customers are responsible for their own tax obligations.

[PBIG – paragraph 2-2]

Banks should try to accept only those customers whose source of wealth and funds can be reasonably established to be legitimate. The PB who sponsors the customer for acceptance is largely responsible for this. Mere fulfilment of internal review procedures does not relieve the PB of this basic responsibility.

[Wolfsberg PB Guidelines – paragraph 1.1 and PBIG– paragraph 6-1-2]

1.2 Identification and Verification of Identity

Verification of Identity

A private bank typically serves more sophisticated customers, and services may include opening accounts in the name of trusts, foundations and private investment companies. As such, the bank will need to take reasonable measures to verify the identity when establishing a business relationship as noted below:

a. Natural persons: Identity should be verified with official identity papers or other reliable, independent source documents, data or information as appropriate (e.g. valid passport, national identity card with a photograph or utility bill [as proof of address]).

b. Corporations, partnerships, foundations: Identity should be verified with documentary evidence the organisation exists (e.g. ACRA Bizfile, DP Search, Certificate of Incorporation, Certification of Incumbency, Memorandum and Articles of Association, Letter of Good Standing and/or Partnership Agreement).

c. Trusts: Identity should be verified with evidence of the formation and existence of the trust, or similar documentation. The identity of the trustees should be established and verified (e.g. by trust deed or a Letter of Undertaking).

[Wolfsberg PB Guidelines – paragraph 1.2.2]

1.3 Beneficial Owner

Beneficial ownership must be established for all accounts. Beneficial owners will usually include the individuals:

a. who have ultimate control through ownership or other means over the funds in the account; and/or

b. who are the ultimate source of funds for the account and whose source of wealth should be subject to due diligence.

Mere signature authority does not necessarily constitute control for these purposes.

[Wolfsberg PB Guidelines – paragraph 1.2.3]

Due diligence must be done on all beneficial owners (for different types of customers) identified in applying the following principles:

a. Natural persons: Where the account is in the name of an individual, the PB must establish whether the customer is acting on his/her own behalf. If doubt exists, the bank should establish the capacity in which and on whose behalf the account holder is acting.

b. Legal entities: Where the customer is a private investment company, the PB should understand the structure of the company sufficiently to determine the provider of funds, the beneficial owner(s) of the assets held by the company and those with the power to give direction to the directors of the company. This principle applies regardless of whether the share capital is in registered or bearer form.

c. Trusts: Where the customer is a trust, the PB should understand the structure of the trust sufficiently to determine:

   i) the provider of funds (e.g. settlor);

   ii) those who have control over the funds (e.g. trustees or an effective controller);

   iii) any persons or entities who have the power to remove the trustees; and

   iv) the beneficiaries or nominated beneficiaries of the trust.

d. Partnerships: Where the customer is a partnership, the PB should understand the structure of the partnership sufficiently to determine the provider of funds and the general partners.

e. Foundations: Where the customer is a foundation, the PB should understand the structure of the foundation sufficiently to determine the provider(s) of funds and how the foundation is managed.

f. Unincorporated associations: The above principles apply to unincorporated associations.

[*Wolfsberg PB Guidelines – paragraph 1.2.3*]

1.4 Intermediaries

Regardless of the type of intermediaries (e.g. external asset managers and introducers) that a private bank deals with, the bank shall perform due diligence on all intermediaries it works with. The bank should at least perform CDD measures on intermediaries, as indicated.

CDD on Introducers

a. Identify and verify introducers;

b. Media screening; and

c. Periodic reviews, including media screening and/or updating CDD documents.

CDD on External Asset Managers

a. Identify and verify the beneficial owners/connected persons of the external asset managers (EAM);

b. Media screening of beneficial owners and connected persons;

c. Verify that the EAM applies the same or higher CDD standards;

d. Periodic reviews, including media screening and/or updating of CDD documents; and

e. If the EAM is operating outside Singapore, obtain confirmation from the EAM and assess whether it meets anti-money laundering and CDD standards that are at least equivalent to Singapore's. Onsite review of EAM is also encouraged.

1.5 Practices for Walk-In Customers and Non-Face-to-Face Banking Relationships

Generally, a bank offering private banking services should not accept walk-in customers or relationships initiated through electronic channels without referrals and subsequent visit. If a private bank accepts non-face-to-face customers, it shall put in place comprehensive measures to identify and verify the identity.

[Wolfsberg PB Guidelines – paragraph 1.2.6]

1.6 Due Diligence

Before a bank establishes a business relationship with a customer, a PB shall obtain information to establish the:

a. purpose or reason for opening the account;

b. anticipated account activity;

c. source of wealth (description of the economic activities that generated the customer's net worth);

d. source of funds (description of the origin and the means of transfer for monies that are accepted for opening the account);

e. estimated net worth; and

f. references or other sources to corroborate reputational information where available.

Unless other measures are sufficient to perform due diligence (e.g. favourable and reliable references), the bank shall meet the customer face-to-face before opening the account.

[*Wolfsberg PB Guidelines – paragraph 1.3*]

1.7 Oversight Responsibility

Banks shall require that a person other than the PB approve all new accounts for all new customers.

[*Wolfsberg PB Guidelines – paragraph 1.6*]

2 Customer Acceptance: Situations Requiring Additional Diligence or Attention and Prohibited Customers

2.1 General

Customers who are not initially deemed to warrant enhanced due diligence may be subjected to greater scrutiny because of:

a. monitoring of their activities due to STRs filed;

b. external inquiries from relevant authorities;

c. negative information (e.g. negative media reports);

d. use of complex structures;

e. request for hold mail services without satisfactory reasons;

f. non-face-to-face business relationship; or

g. other factors that may expose the bank to reputational risk.

[PBIG Guidelines – paragraph 3.1]

3 Updating Customer Files

3.1 General

The PB is responsible for updating the customer's file regularly. The PB's supervisor or an independent control person should review the customer's file regularly (with the minimum based on the anti–money laundering risk review cycle) to ensure consistency and completeness.

If a customer is not able to provide an updated CDD document (e.g. Certificate of Incumbency or a Letter of Good Standing) during a periodic review, the PB should follow up with the customer to obtain signed confirmation that the customer's status has not changed from the information noted on the non-individual CDD document, and to obtain the renewal receipt of entity registration. The bank may adopt an RBA to periodically request that a customer provide a copy of updated CDD documents.

For CDD documents with expiry dates (e.g. passports), the bank should obtain updated copies from the customer and its connected parties, beneficial owners, and natural persons appointed to act on its behalf periodically, where required.

Senior management must approve the reviews of PEP customers. For other categories of customers requiring enhanced CDD measures, the bank's policies and procedures should indicate whether the involvement of senior management and/or other control functions is required. The bank's policies and procedures should indicate the type of management information and the frequency with which it is required.

[Wolfsberg PB Guidelines – paragraph 3]

4 Monitoring

4.1 General

The PB has primary responsibility for reviewing account activities. The PB will be familiar with significant transactions and increased activity in the account and will be especially aware of unusual or suspicious activities.

Apart from the PB's day-to-day monitoring of significant transactions, the bank should also ensure that during periodic reviews, the customer's past transactions are assessed to judge whether they were consistent with the customer's profile.

Where large size transactions are not for investments but are simply funds transferred into or out of an account, banks should try to understand the underlying reasons for the movements, especially if these are cross-border transactions with no clear underlying links or reasons. Where the

transactions do not match the customer's profile, the bank should assess whether the transactions are suspicious and determine whether a re-profiling of the customer is warranted.

Similarly, where private bank accounts are used for transactions other than those envisaged (e.g. for payment for commercial deals and not for investments), these accounts should have enhanced monitoring.

The parameters and thresholds banks use to identify suspicious transactions should be properly documented and independently validated to ensure they are appropriate for its operations and context.

ABS Anti–Money Laundering Principles for Retail Banks (2015)

1 Customer Acceptance: General Principles

1.1 Environment of Retail Banks

Retail banks offer a wide range of products and services to the public through their branches, the internet and other channels. Generally, retail banking customers are considered to pose less of a money-laundering risk given that they:

a. generally perform fewer high-value transactions;

b. are usually domestic; and

c. usually open accounts in their own name or through less complex structures, rather than through personal investment companies or other more complex legal arrangements that may be less transparent.

Retail banks offer a wide range of products and services, including:

a. checking and savings accounts;

b. fixed deposits;

c. loans (e.g. mortgage loans, vehicle loans, housing loans); and

d. credit Cards.

These products and services are usually not complex and the associated money laundering risks are generally low.

With the generally lower customer and product ML/TF risks in retail banking, most retail bank customers undergo standard CDD. EDD is only performed when the customer falls into one of the bank's higher ML/TF risk categories.

Although most retail account customers open and operate accounts in their own name and right, banks should still enquire if a beneficial owner exists. They could do this be getting a declaration from the customer, and the bank should take reasonable measures to identify and verify the identity of the beneficial owner, to corroborate the customer's declaration.

While the customer and product ML/TF risks are generally low, some retail bank activities do carry higher risks because of:

a. the higher volume of transactions;

b. the higher frequency of physical cash transactions (e.g. cash deposits and withdrawals via ATMs and over the counter);

c. providing services to cash-intensive businesses; and

d. large credit balances in credit card customers' accounts.

Banks should have policies and procedures in place to handle cash deposits conducted over the counter. The policies and procedures should take into account the higher ML/TF risks from

unusually large cash deposit amounts relative to the customer's account and business activity. An unusually large cash deposit not consistent with a client's profile is a red flag for a suspicious transaction. Similarly, a third party depositor who is unknown to the bank and for whom the bank has not performed CDD may pose a higher ML/TF risk (as it could involve money mules, illegal money lenders or terrorist financiers). Banks should therefore consider setting thresholds for the acceptance of cash deposits based on a customer's profile, to effectively supplement its transaction monitoring system controls. This will in turn provide for due escalation and filing of STRs, and an effective defence against ML/TF.

Please refer to paragraph 6.13 Ongoing Monitoring, on the measures retail banks should adopt to address ML/ TF risks.

1.2 Practices for Non-Face-to-Face Banking Relationships

Retail banks may onboard customers via non-face-to-face channels including telephone, post, fax or internet. Common non-face-to-face transactions include applications for credit cards and deposit accounts via the internet.

When a bank establishes business relationships via non-face-to-face channels, it should have adequate additional controls to identify and verify the identity of a customer and manage the risk of impersonation. Apart from obtaining a copy of the customer's valid passport or national identity card, the bank could obtain extra assurance of customers' identity by requesting documents through secure channels such as a customer's Central Provident Fund (CPF) statement via CPF Weblink. A bank may consider performing additional checks to verify the identity of a customer. Such checks may include a call back to the customer at a telephone number indicated in a copy of the customer's telephone bill provided to the bank, or a mail sent to the address indicated in a copy of the customer's utility bill or any other official documents provided to the bank.

When a bank receives an application to establish a business relationship via a party acting on its behalf, the bank should use the same customer identification and verification procedures as it does for applications received through direct channels.

When an intermediary introduces a customer to a bank, and when this introduction means the intermediary's customers become the bank's customers, the bank should generally use the same verification methods as if it were dealing with a direct customer. However, if the bank intends to rely on the introducing intermediary to perform CDD measures, it shall put in place policies on this reliance that would meet paragraph 9 of MAS Notice 626 and the accompanying MAS Guidelines.

2 Updating Customer Files

2.1 Credit, Charge and Other Cards

Apart from the principal cardholder, the bank should where relevant, obtain updated CDD information for categories of customers including:

a. supplementary credit card or charge card holder;

b. an employee to whom the business credit card is issued;

c. the sole proprietor or partnership that is liable for the business credit card issued;

d. any employee or officer of a body corporate to whom the corporate card is issued, and the body corporate;

e. the guarantor of any guaranteed credit card or guaranteed charge card (who must be screened before client acceptance); and

f. the merchant for whom the bank opens or maintains an account (including a ledger account) for the purchase of goods by, or provision of services to any person from the merchant, using any credit card or charge card.

Banks must perform sanctions screening on the categories of customers listed from 2.1a to 2.1f above, before client acceptance, and on an on-going basis. Where there is a positive hit against a sanctions list, the bank must terminate and disallow the use of the credit or charge card, even though the relevant credit limit may be covered or guaranteed by a principal/corporate cardholder or guarantor, and report the case to the relevant authorities.

It is good practice for banks to perform media screening on principal, corporate and supplementary cardholders. Banks should establish policies and procedures for handling adverse news about a cardholder.

ABS Anti-Money Laundering Principles for Trade Finance (2015)

1 Objective

This section aims to provide clarity and guidance for adopting industry best practices when banks develop their RBA to detect and prevent ML/TF when onboarding customers and processing their requests at the transactional level in the area of trade finance. It seeks to supplement the guidance on AML/CFT controls in trade finance in the MAS Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking[15] issued on 22 October 2015.

2 Overview

Banks undertake trade finance to facilitate trade or commerce, which generally involves moving and/or transferring goods or services pursuant to buying or selling goods or services between two or more parties. Trade finance activities include a mix of money transmission instruments, performance or default undertakings and provision of credit facilities.

Open Account Trade

The majority of world trade is carried out on open account terms, whereby the buyer and seller agree to the terms of the contract as usual, and goods or services are subsequently delivered to the buyer via a clean payment through the banking system. Under such open account terms, which rely heavily on the level of trust between the two parties, banks will generally see only the clean payment and will not always be aware of the underlying reason for the payment.

For supporting products associated with trade conducted on open account terms, such as the various types of supply chain financing and invoice financing, banks will need to adopt a risk-based approach for due diligence based on the nature of the products offered. For example, transaction-level documentation checks may not be feasible for electronic financing solutions. Banks are therefore advised to determine internally the risk factors to consider in their due diligence process.

3 Money Laundering in Trade Finance

Based on the estimates of the IMF and the United Nations Office on Drugs and Crime, it is estimated that 3.6% of global gross domestic product is laundered every year by criminal organisations[16], a high proportion of which involves cross-border transactions. The FATF as well as other organisations and supervisory authorities have identified that criminal organisations and terrorist financiers can easily manipulate the international trade flows and financing to move money to disguise its origins and integrate it into the legitimate economy.

Criminal organisations and terrorist financiers are also finding trade finance products more attractive as supervisory authorities and banks have gradually built up effective controls to combat other more traditional methods of ML/TF.

However, it should also be noted and recognised that trade finance is a core banking business, which benefits the real economy. According to the Bank for International Settlements (BIS), trade finance

---

[15] www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Guidance%20on%20AML%20CFT%20Controls%20in%20Trade%20Finance%20and%20Correspondent%20Banking.pdf.

[16] www.fatf-gafi.org/faq/moneylaundering/.

directly supports about one-third of global trade.[17] Hence, the approach to manage trade-based ML/TF risks needs to be balanced and risk-based.

The basic techniques of trade-based money laundering as highlighted by the FATF in its June 2006 study include:

a. under-invoicing: by misrepresenting the price of the goods in the invoice and other documentation (stating it below the true value), the buyer gains excess value when the payment is made (e.g. under-invoicing of a shipment of new Hyundai cars at US$500 per car);
b. over-invoicing: by misrepresenting the price of the goods in the invoice and other documentation (stating it above the true value), the seller gains excess value as a result of the payment (e.g. over-invoicing of a shipment of paper clips at US$200,000 per carton of 6 packs);
c. multiple invoicing: by issuing more than 1 invoice for the same goods, a seller may appear to justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than 1 bank to facilitate the payments and transactions (e.g. the seller issues 2 or more invoices for the same shipment of goods to secure multiple financing for the same transaction);
d. over-shipment: the seller ships more than the invoiced quantity or quality, thereby misrepresenting the true value of goods in the documents. The effect is similar to under-invoicing (e.g. the manufacturer or seller ships 1,000 air filters but invoices the buyer for only 800 units);
e. under-shipment: the seller ships less than the invoiced quantity or quality of goods, thereby misrepresenting the true value of the goods in the documents. The effect is similar to over-invoicing (e.g. the seller ships only 50 containers of paper products when the invoice shows the quantity as 80 containers);
f. phantom shipment: no goods are shipped and all documentation is fake; and
g. deliberate obfuscation of the goods shipped: by falsifying the information to disguise the type or the source of the goods shipped to mislead the other parties and to avoid suspicion (e.g. dual-use goods).

The above techniques can imply fraud by one party against another, but in the case of money laundering, it usually involves both parties colluding to obtain value in excess of what would otherwise be an arm's-length transaction in order to move funds without being detected. The collusion may arise, for example, because the same person controls the parties or because the parties are attempting to evade taxes on some part of the transactions.

3.6 In cases involving money laundering through open account trade transactions, which rely heavily on pre-arranged structures and collusion between the "buyer" and "seller" involved in the money laundering operation, this trust will be implied, allowing them to opt for open account transactions wherever possible, subsequently avoiding the normal third-party (i.e. bank) scrutiny that is part of documentary trade transactions. This reduces the risk of arousing suspicion as it removes the need to provide the documents that normally accompany a documentary trade transaction.

---

[17] Committee on the Global Financial System (No. 50), *Trade Finance: Developments and Issues*. www.bis.org/publ/cgfs50.pdf.

While banks may be able to source pricing information for certain types of commodities, it is acknowledged that such information is not available for all transactions. Even for commodities where pricing is available, it is indicative, as actual terms include factors other than cost, such as payment terms, freight and insurance. Such checks should be carried out on a best effort basis with banks giving due consideration to what they internally consider as risk factors.

4 Terrorism Financing and Proliferation Financing in Trade Finance

To recap, terrorism financing is defined as the solicitation, collection or provision of funds intended to be used to support terrorist acts or organisations. Funds may be from legitimate or illicit sources.

Proliferation financing is the act of providing funds or financial services that are used, in whole or in part, for manufacturing, acquiring, possessing, developing, exporting, trans-shipping, brokering, transporting, transferring, stockpiling or using nuclear, chemical or biological weapons and their means of delivery, as well as related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Proliferation financing is primarily combated using sanctions against specific countries and on certain goods.

As a result, the most effective RBA to tackle such risks in trade finance is for banks to ensure they screen all names in all transactions (e.g. countries, counterparties, vessel names and individuals) against regulatory sanctions lists.

5 Mitigating Money Laundering and Terrorism Financing in Trade Finance

As per the FATF Recommendations[18], banks should adopt and design their RBA to ensure that it emphasises deterrence, detection and disclosure in the areas of greatest perceived vulnerability – trade-based money laundering, terrorism financing and proliferation financing techniques – to counter them as far as is practicable. In designing their RBA, banks should be aware of the prevailing money laundering techniques to mitigate the risks of their involvement in illicit transactions.

Banks may then adopt more flexible measures for the most effective and efficient use of their resources, and apply preventive measures that match the nature of the risks. Please refer to Appendix 5 for a sample of red flag indicators.

In recommending an RBA, the FATF noted that "it is important that competent authorities acknowledge that in a risk-based regime, not all banks will adopt identical AML/CFT controls and that a single isolated incident of insignificant, crystallised risk may not necessarily invalidate the integrity of a bank's AML/CFT controls."

The FATF also noted that banks should understand that "a flexible RBA does not exempt them from applying effective AML/CFT controls". It added, "Countries and competent authorities should take account of the need for effective supervision of all entities covered by AML/CFT requirements. This will support a level playing field between all banking service providers and avoid that higher risk activities shift to institutions with insufficient or inadequate supervision."

---

[18] *Best Practices Paper: Best Practices on Trade Based Money Laundering*. www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

The starting point for an effective RBA is first to identify and acknowledge the risks of trade-based ML/TF in the bank's business.[19] The consideration of the risks could be part of the bank's overall ML/TF risk assessment, which senior management approves.

A framework for managing the identified ML/TF risks should then be established, and documented clearly in the bank's policies and procedures. The basic tenets of the framework should include:

a. clear and documented roles and responsibilities for bank staff in managing the ML/TF risks;
b. the bank's roles in different types of trade finance transactions and their instructing parties, which determines the due diligence required for each role based on the RBA, and the information needed to conduct such due diligence;
c. the baseline checks to be performed for the bank's trade finance transactions;
d. the types of transactions or products deemed more complex or riskier, and requiring more care in processing;
e. the types of transactions deemed to pose higher ML/TF risks, and the enhanced checks or due diligence processes for such transactions;
f. monitoring of trade finance transactions;
g. periodic refresher training about the bank's policy on the AML/CFT risk management framework, which should be tailored to different staff members' functions; and
h. a list of red flag indicators relevant to the bank's business model to guide staff in identifying transactions that may warrant further review.

Many trade finance banks have, when dealing with suspicious transactions, grappled with the seemingly conflicting obligations towards AML/CFT regulations and the commercial obligations under the rules for conducting trade and payments set down by the International Chamber of Commerce (ICC).

As a result, it is recommended that the bank's policies and procedures clarify that the commercial obligations prescribed by the ICC do not take precedence or absolve the bank of its regulatory obligations towards AML/CFT requirements or other financial crime regulatory requirements.

[19] See UK FCA Thematic Review TR13/3 – *Banks' control of financial crime risks in trade finance*, sections 3.2.2 and 3.2.4. The FCA expects banks to adopt an RBA to their assessment and management of financial crime risk in relation to trade finance, and recommends "completing a documented financial crime risk assessment for trade finance business that gives appropriate weight to money laundering risk, as well as sanctions risk".

6 Bank's Role and the Instructing Party in a Trade Finance Transaction

The instructing party in a trade finance transaction shall be treated as the customer for the purpose of the transaction. The list below provides some guidance on who is the instructing party or customer, depending on the role of the bank.

	Bank's role	**Instructing party (customer)**
i)	Letter of credit (LC) issuing bank	Applicant (including applicant bank where the bank does not have a direct relationship)
ii)	Advising/confirming bank	LC issuing bank
iii)	Negotiating/paying bank	LC issuing bank/beneficiary
iv)	Remitting bank of outward collections	LC issuing bank or exporter/seller
v)	Collecting bank of inward collections	Remitting bank/collecting bank or importer/buyer bank
vi)	Guarantees/standby letters of credit	Applicant or counter-guarantor (as the case may be)

The role and capacity in which the bank is acting in the transaction will determine whether it should get additional information about the trade finance transaction. The bank's policies should clearly set out the circumstances when additional information shall be required, depending on the role of the bank concerned.

Bank's Role of an Open Account Trade Transaction

Banks are rarely involved in an open account trade transaction until a clean payment is made at the end (which could be after the goods have been delivered). The seller and buyer will generally not give the bank handling the open account payment supporting documentation. In most cases, the bank will have little inherent opportunity, need or cause to understand the nature of the underlying trade transaction, or to review any trade-related documents (e.g. contracts and invoices).

A bank that handles a payment related to an open account trade transaction generally does so in one (or both) of two capacities:

a. The seller or buyer is its commercial customer, in which case the bank is debiting or crediting the account of a customer for which it would be expected to have conducted a certain amount of client due diligence.
b. The seller or buyer is the commercial customer of the bank's correspondent banking customer (i.e. the seller or buyer is the customer of the respondent bank to whom the bank provides correspondent banking services), in which case the bank would not necessarily have any general knowledge about the expected behaviour of its respondent bank's customer.

The nature of the international payments system is such that banks will generally not be able to differentiate a payment related to an open account trade transaction from other clean payments

when presented as an application to make a payment or to credit the account of the beneficiary. A bank handling such payments will be able to perform the basic screening and monitoring related to payments transactions, but it will not, given the absence of underlying transactional information, generally be able to otherwise discern suspicious activity.

7 Information for Establishing Trade Finance Facilities and Transactions Undertaken

Information relevant for understanding the client's trade finance profile should be obtained at the onboarding stage for offering trade finance services (irrespective of whether an account or a credit facility is opened with the bank). This is in addition to information required as part of the CDD process. Banks may develop templates and/or questionnaires for obtaining such information and document the information in the CDD files and systems.

Banks may choose to adopt an RBA, taking into account factors such as business model, product parameters and client profile. Suggested information to be obtained at the onboarding stage includes:

a. major trading partners or counterparties of the customer, i.e. buyers and sellers;
b. nature of goods and/or services traded;
c. country or countries for sourcing and supplying;
d. trade cycle (i.e. the terms of payments and/or receipts);
e. source(s) of funds (i.e. operating account); and
f. anticipated volume and throughput (i.e. number of transactions, their value and quantity).

Suggested information to be obtained during transactional checks includes:

a. buyers and/or sellers;
b. goods traded and/or purchase or sale price;
c. vessel used and flag of vessel;
d. port of loading and port of discharge
e. other counterparties of the customer (including shippers, consignees, notifying parties, shipping agents etc. as shown on the documents)

Banks are expected to periodically monitor client transaction patterns against the client profile and update the profile in discussion with the client, as required.

8 Additional Information for Trade Finance Transactions that Present Higher ML/TF Risks

Banks should have a framework for assessing trade finance transactions that could pose higher ML/TF risks. Examples of such transactions include those involving multiple parties and/or where information is not readily available, transactions where there are screening hits against vessel names, discrepancies or ambiguity in trade documents, transhipments or use of multiple ports etc.. Staff should be trained to identify such higher risk transactions and exercise greater due diligence when handling such transactions.

If at the initial stage of a trade finance transaction or during the course of any trade finance transaction, the bank becomes aware that the transaction presents higher ML/TF risk, the bank should obtain information in addition to that set out in paragraph 7 above. The bank's policies should include additional checks when faced with higher risk trades. These checks could include:

a. enquiring as appropriate into the ownership and background of the other parties in the transaction (e.g. the beneficiary, shipping company, commercial operator and shipping lines) and taking further steps to verify information or the identity of key individuals as the case demands;
b. seeking information from the instructing party about the frequency of trade and the quality of the business relationships existing between the parties to the transaction. This should be documented to assist future due diligence;
c. seeking information from the instructing party on proposed trade routes;
d. checking the vessel's movements from independent sources (e.g. MarineTraffic, Lloyd's Seasearcher and Bloomberg) to find out the ports of call, as well as to confirm that the vessel did call at the port of loading and discharge, which is usually a sign of genuine shipment;
e. checking the name history of the vessel;
f. seeking information on the International Maritime Organization (IMO) number of the vessel to find out whether the vessel is sanctioned or linked to a sanctioned shipping company;
g. checking the transaction against warning notices from external public sources (e.g. the ICC's International Maritime Bureau);
h. referring the transaction to external agencies specialising in search and validation services for bills of lading, such as the ICC Commercial Crime Services if there is suspicion of fraud in the issue of the bill of lading;
i. checking details of the source of goods and whether the transaction involves dual-use goods where there is suspicion on the goods traded, from the description of the goods and the trade parties involved (e.g. military institutions or governments);
j. checking public information sources for prices of goods such as commodities, where the contract price is significantly different from the market and deciding if further investigation is required;
k. attending and recording relationship meetings with the instructing party, and visiting them by arrangement; and
l. conducting post-event checks into the verification of shipments, drawing a sample of transactions at random and across a cross-section of the bank's trade finance clients, where necessary.

9 Monitoring of Trade Finance Transactions

Due to the complexity and documentation-focused processes of trade finance transactions, monitoring these transactions tends to require some element of human intervention and judgment. However, banks could configure their transaction monitoring controls to flag “unusual transactions” based on the red flags in their business model.

Alerts generated from these systems can then be analysed or further reviewed. The analysis, based on intelligence-based risk indicators such as geographical combination or geographical patterns of high-risk payment flows, is instrumental to an effective RBA for trade finance transaction monitoring.

The depth and frequency of monitoring to be undertaken will be determined by the bank’s risk analysis of the business and/or the parties involved.

Despite the above, the ability of a bank to detect suspicious activity will often be constrained. The extent to which available information will need to be verified will also vary depending on the bank’s role.

10 Potential Trade-Based Red Flag Indicators

Trade-based red flag indicators aid banks in identifying potentially suspicious transactions for further analysis and review. The list of indicators is intended solely as an aid, and must not be applied as a routine instrument in place of common sense and reasonable assessment. Please refer to Appendix 5 for examples of red flag indicators.

11 Staff Training

Banks should conduct periodic training on their AML/CFT risk management framework, tailored to different staff functions within the organisation.

Appendix 1 – Methods and Stages of Money Laundering

1. The methods of "placement" are:

    a. Structured deposits (often known as "smurfing", where large sums are broken down into smaller sums, often below any cash transaction reporting (CTR) thresholds (e.g. S$10,000, A$10,000);

    b. setting up cash businesses (e.g. circus, fun fair, food outlets);

    c. using professional service providers (e.g. lawyers, accountants);

    d. using casinos;

    e. buying monetary instruments (e.g. cashier's orders, postal money orders, traveller's cheques);

    f. buying high-value goods (e.g. precious metals, antiques and paintings);

    g. using shell/shelf[20] companies incorporated in tax haven countries.

2. The methods of "layering" are:

    a. wire transfers;

    b. false trading in cross-border transactions (e.g. export and import businesses);

    c. using shell/shelf companies from tax haven countries;

    d. using professional service providers (e.g. lawyers, accountants, company formation agents);

    e. using existing customer's account ("stool pigeon" or "cuckoo transactions") where "account holder" and "account user" are no longer the same person;

3. The methods of "integration" are:

    a. buying real estate and other assets;

    b. buying into existing legitimate businesses (e.g. restaurants, food outlets);

    c. buying shares, securities, derivatives and other investment instruments.

[20] A company set up with no intention of operating commercially may be defined as a "shell company". An aged company with no activity for a period of time or a company readily set up and with the intention of being sold may be defined as a "shelf company".

Appendix 2 – ABS Guidelines on Tax Crime

ABS Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism: Tax Crime as a Predicate Money Laundering Offence

1. The key legislation governing money laundering offences and other related matters is the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, (Cap 65A)* of Singapore.

2. The CDSA adopts the "predicate list" of money laundering offences approach, which means that the laundering of proceeds derived from activities specified in that list are criminalised as "money laundering offences".

3. With effect from 1 July 2013, the Second Schedule to the CDSA provides that serious tax offences pursuant to Sections 96 and 96A of the *Income Tax Act, (Cap 134)* of Singapore and Sections 62 and 63 of the *Goods and Services Tax Act, (Cap 117A)* of Singapore are money laundering predicate offences for direct tax and indirect tax offences respectively.

> ABS reiterates the clarification provided by the MAS in its response to the feedback on the Consultation Paper to Designate Tax Crimes as Money Laundering Predicate Offences in Singapore (issued in March 2013).
>
> The MAS clarified that its supervisory expectations in respect of deterring money from tax evasion is similar to that applied to other predicate offences pursuant to the AML regime. Accordingly, banks are expected to review their existing AML policies and procedures to ensure that they remain relevant and enhanced as required for incorporating necessary requirements for tax evasion crimes.
>
> MAS has also clarified that banks are expected to assess whether there is suspicion that a customer's assets emanate from serious offences (including fraudulent or wilful tax evasion), file a Suspicious Transaction Report and apply appropriate risk mitigation and control measures. Banks are not expected "to determine if their customers are fully compliant with all their relevant tax obligations globally".
>
> With regard to an offence that is not a predicate tax offence (i.e. other tax-related offences not specifically criminalised by CDSA), the general principle to note is that banks should not be seen to be aiding or abetting any crime.
>
> Banks should take an RBA and devise a robust methodology for screening their customers against tax crimes risk. Banks should refer to Private Banking in Singapore: Code of Conduct as amended by the Private Banking Industry Group (PBIG Code). www.abs.org.sg/pdfs/Publications/Singapore_PB_Code_with_ISP_FINAL.pdf

4. With reference to Guideline 3 above, all banks should, inter alia:

   a. review their existing AML/CFT policies, controls and procedures to ascertain any gaps and enhancements required in relation to mitigating the risk of tax evasion;

   b. implement effective controls and preventive measures for tax evasion as is done in the case of all other predicate offences;

c. assess whether there is any suspicion that customers' assets are proceeds of serious tax crimes pursuant to the Second Schedule of the CDSA;

d. not accept a prospective customer if there are reasonable grounds to suspect that the customer's assets are the proceeds of tax evasion;

e. for an existing customer, where there is suspicion of tax evasion, conduct enhanced monitoring. In such a case, the bank should obtain senior management approval if there are grounds to continue with such a relationship or alternatively consider discontinuing the relationship; and

f. file an STR where there is knowledge or suspicion of tax evasion.

5. To illustrate further and provide guidance based on the MAS Consultation Paper (issued in October 2012) and its Response to the Feedback on the Consultation Paper to Designate Tax Crimes as Money Laundering Predicate Offences in Singapore (issued in March 2013), banks should enhance existing due diligence measures with additional customer acceptance and monitoring checks to ascertain a customer's tax-risk profile. Some of the measures include:

   a. RBA and red flags – the bank will need to understand whether red flags exist that will highlight the suspicion or existence of tax evasion. These may include:

      i) using complex structures (including trust structures) and the reasons behind these structures. In such cases, banks should identify and verify the UBOs, understand the ownership and control of these structures and ascertain whether the structures are used in connection with predicate tax evasion crimes. These may also include complex structures in low tax jurisdictions, as appropriate; and

      ii) the jurisdiction in which such structures mentioned in (i) above are created and the tax reputation of such jurisdictions;

High Tax Risk and High Tax Rate Countries

Banks should devise their own list of jurisdictions deemed to be "high risk" either from a high tax risk or high tax rate perspective. They can take guidance from various reports issued by international bodies such as the Organisation for Economic Cooperation and Development (OECD) and the Global Forum on Transparency and Exchange of Information for Tax Purposes to establish jurisdictions that have been identified as having material deficiencies complying with the international standard for transparency and exchange of information. These reports may include:

1. OECD list of uncooperative tax havens – These are jurisdictions that have not embraced the OECD principles on standards of transparency and effective exchange of information. Banks should also take note of countries that are making progress to implement necessary measures for tax-related transparency and exchange of information. While banks may use the OECD list as a red flag indicator, they should not rely on this list as a definitive or exhaustive determinant of a customer's tax-risk profile. In May 2009, the Committee on Fiscal Affairs removed all 3 remaining jurisdictions (Andorra, the Principality of Liechtenstein and the Principality of Monaco) from the list of uncooperative tax havens. Consequently, no jurisdiction is currently listed as an uncooperative tax haven by the Committee on Fiscal Affairs.

2. OECD list of countries that have signed the Convention on Mutual Administrative Assistance in Tax Matters.

3. Peer Reviews published by the Global Forum on Transparency and Exchange of Information for Tax Purposes. These reviews can be found in the link: http://www.oecd-ilibrary.org/taxation/global-forum-on-transparency-and-exchange-of-information-for-tax-purposes-peer-reviews_2219469x.

4. High tax rate jurisdictions – A further consideration may also be customers or potential customers from jurisdictions that are not deemed as uncooperative but who are trying to evade high (or higher) tax in their jurisdiction and channel their money outside their home country, as well as those customers that emanate from jurisdictions with high tax evasion rates.

5. *Issues in International Taxation and the Role of the IMF* (issued on 28 June 2013). This paper lists certain tax evasion and tax avoidance scenarios that can be used as a guide.

iii) occasions where the tax structure provided in the tax plan is not consistent with the actual fund flows or the actual physical structure recorded in documents such as incorporation documents and proofs of addresses;

iv) customers who do not have business or personal interests in Singapore. In such cases, customers should be asked to justify opening an account in Singapore;

v) customer requests for hold mail services without satisfactory reasons;

vi) occasions when the bank is not able to complete CDD measures; where there are no acceptable reasons for such non-completion of the CDD such as where the customer does not provide information requested by the bank, withdraws an application or

instructions to establish business relations or a pending transaction, or terminates existing business relations;

vii) customers who are evasive when asked about tax matters;

viii) non-face-to-face business relationships;

ix) negative tax-related reports from media and background screening on the customer or the customer's jurisdiction of domicile or tax residence during on boarding, as well as periodic reviews. In addition to news on convictions, the bank should also consider news on allegations;

x) inconsistent transactional behaviour when compared with the expected account activity, including transferring money to certain countries that may appear suspicious, the number of fund transfers surpassing expected transaction patterns, or withdrawal of unusually large sums of cash where such withdrawals are not customary for that customer;

xi) withdrawals in physical cash;

xii) transactional behaviour that does not match the known customer profile;

xiii) account closure suspected to be related to a situation where tax legislation is tightened or when the bank requests additional information on tax-related matters;

xiv) customers who only buy products that are also available in the customer's home jurisdiction without satisfactory reasons or where such transactions appear to be suspicious;

xv) hold mail that is not collected and the customer has not visited Singapore for a long time;

xvi) fund movements that originate from or flow to jurisdictions known to harbour tax criminals without satisfactory reasons or where such transactions appear to be suspicious;

xvii) considering any other parameters pertinent to a customer or product or service offered to the customer, including other suspicious circumstances such as using insurance wrappers[21] without a valid reason; accounts managed by external asset managers (that are not recommended by the bank); a major portion of the foreign customer's assets under management are held in the customer's Singapore account(s) without satisfactory reasons; cash-backed loans involving entities in high tax rate or high tax risk jurisdictions, or commercial transactions passing through personal or personal investment company accounts.

b. As part of the CDD exercise, banks should seek to understand the customer's tax-risk profile. Banks may use an RBA in this regard as mentioned by the MAS in the *Response to Feedback Received – Consultation Paper to Designate of Tax Crimes as Money Laundering Predicate Offences in Singapore* (issued in March 2013). Banks should consider measures including:

[21] "Insurance wrappers" are instruments into which investors can place stocks, hedge funds or virtually any other bankable assets, allowing them to pay less tax on investment income

i) requesting additional information from the customer where there is insufficient information available in the bank's records to identify and assess the tax evasion risk the customer poses;

ii) verifying the information or representations the customer makes ;

iii) requesting tax status declarations from customers, where necessary;

iv) evaluating the tax risk or evasion vulnerability based on the business activity of the customer and factors mentioned in (a) above, as well as any other relevant risk factors; and

v) conducting enhanced due diligence and more regular periodic review of customers who present high risk of tax evasion.

c. Banks should institute ongoing monitoring procedures for detecting transactions that may be related to tax predicate offences and adopt appropriate risk mitigation for high-risk accounts. An RBA could be taken, with focus on customers from high tax rate countries or high tax evasion risk countries.

d. Banks must file an STR when they suspect or have evidence that a customer has been evading taxes.

6. Banks should take guidance from various reports and guidelines issued by international bodies such as the OECD and the Global Forum on Transparency and Exchange of Information for Tax Purposes on tax evasion or tax crimes, red flag indicators and high tax risk jurisdictions, as may be relevant.

Appendix 3 – ABS Guidelines on the New Cross-Border Currency/Bearer Negotiable Instruments Reporting Regime

1. Introduction

1.1 The *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act* (CDSA) was amended on 19 September 2007 to introduce a Cross-Border Currency/Bearer Negotiable Instruments Reporting Regime (CBCRR) in Singapore. From 1 September 2014, the threshold for reporting of Cross-Border Movements of Physical Currency and Bearer Negotiable Instruments was revised from S$30,000 to S$20,000.

1.2 Under CBCRR, all persons who move more than S$20,000 (or its equivalent in a foreign currency) worth of physical currency or bearer negotiable instruments (CBNI) into or out of Singapore through cargo, post or other means, are required to report to the Suspicious Transaction Reporting Office (STRO) of the Commercial Affairs Department (CAD) no later than 1 business day (or, if the report is to be sent by post, no later than 2 business days) prior to moving the cash. All persons who receive from outside Singapore more than S$20,000 or its equivalent in CBNI have to make a declaration in the prescribed form within 5 business days upon receipt. The prescribed form to be used is the Physical Currency and Bearer Negotiable Instruments Report (Traveller) or NP727 form, which can be found on the CAD website.

1.3 In addition, recipients of CBNI the total value of which exceeds S$20,000 or its equivalent, which has been moved to them from outside Singapore through cargo, post or physical means (such as carried by a person), are required to submit the NP727 form to the STRO within 5 business days upon receipt.

1.4 The legislation took effect on 1 November 2007. Please refer to the Singapore Police Force website at www.spf.gov.sg/cbni and the CAD website at www.cad.gov.sg/topNav/hom/ for more information on the CBCRR, including information and a guide on how to fill in the forms.

1.5 Failure to give a full and accurate report is an offence under the CDSA. Any person who contravenes the CDSA can be fined up to S$50,000, or jailed for up to 3 years, or both. The cash may also be seized if the person fails to give the report.

[Cross Border Movements of Physical Currency and Bearer Negotiable Instruments, CDSA]

2. Impact on Banks

2.1 Banks should make a report under the CDSA when:

a. the bank is moving CBNI exceeding S$20,000 (or its equivalent in a foreign currency) into or out of Singapore for its own account, i.e. as a principal; or

b. the bank is moving CBNI exceeding S$20,000 (or its equivalent in a foreign currency) into or out of Singapore at the request of its customer, the bank should inform the customer of its reporting obligation under Section 48C or Section 48E of the CDSA. The bank should then get the customer's permission to furnish customer information in its report to CAD. If the customer refuses to give

permission, the bank should decline to move the CBNI for the customer.

2.2 If the customer brings or sends the CBNI to the bank and the bank is just a recipient and is not involved in moving the CBNI into or out of Singapore, the bank need not make a report under Section 48E of the CDSA (unless the bank finds the transaction suspicious, in which case it should file a Suspicious Transaction Report (STR) – see below).

3. Filing STRs

3.1 Banks should file an STR if:

a. based on the customer's high volume of CBNI transactions, they suspect that the customer is engaging in criminal activity;

b. they suspect that the customer is attempting to evade, or has evaded, the new cross-border CBNI reporting requirements (for example, by structuring CBNI transactions to put them below the S$20,000 threshold);

c. the customer refuses to give permission for the bank to disclose customer information, after requesting the bank move the CBNI into or out of Singapore, or if the customer changes their mind after being told of the bank's reporting obligation.

4. Definition of Physical Currency and Bearer Negotiable Instruments

4.1 Physical currency means the coins and printed money (of Singapore or of a foreign country) that is designated as legal tender and circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue.

4.2 A bearer negotiable instrument (BNI) is a traveller's cheque or any negotiable instrument that is in bearer form, endorsed without any restriction, made out to a fictitious payee or otherwise in such form that title thereto passes upon delivery, and includes a negotiable instrument that has been signed but with the payee's name omitted (e.g. a BNI may include a bill of exchange, bearer cheque, promissory note, bearer bond, bearer share, money order or postal order).

4.3 The following are exempt from the reporting requirements under Sections 48C and 48E of the CDSA:

a. a bill of lading, airway bill, warehouse receipt or cargo receipt;

b. any BNI moved into or out of Singapore or received from outside Singapore by a local financial institution for settling an account with a foreign financial institution;

c. any bearer bond or bearer securities moved into or out of Singapore or received from outside Singapore by a local financial institution while providing custodial services for securities to its customers;

d. a stored value facility;

e. the person is a commercial passenger/goods carrier;

f. the cash is in the possession of any of the carrier's passengers;

g. a commercial goods carrier is also not required to submit a report if the CBNI is carried on behalf of another person and the other person did not disclosed to the carrier that the goods carried include CBNI, and the carrier does not know and has no reasonable grounds to believe that the goods carried on behalf of the other person include CBNI.

[Paragraph 48C, CDSA; Reporting Of Cross Border Movements of Physical Currency and Bearer Negotiable Instruments, CAD]

Appendix 4 – ABS Guidelines on Suspicious Transactions relating to Terrorism Financing

The following situations are intended mainly to be indicative of suspicious transactions. While each situation may not be sufficient to suggest that terrorism financing is taking place, a combination of such situations may support such a transaction. The list is by no means exhaustive, and will need constant updating and adapting for changing circumstances and new methods of terrorism financing. The list is intended solely as an aid, and must not be applied unthinkingly as a routine instrument without analysis or context.

Banks should pay particular attention to:

1. Accounts

   a. An account that at times receives deposits and at other times is dormant for no apparent reason. This account is then used to create an apparently legitimate financial background through which additional fraudulent activities may be carried out;

   b. A dormant account with a minimal balance suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the deposited amount has been substantially withdrawn;

   c. When opening an account, the customer refuses to provide information required by the bank, attempts to provide only a minimal level of information or provides information that is misleading or difficult to verify;

   d. An account for which several persons have signing authority, yet these persons do not appear to have any family or business relationship;

   e. An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations, but for which the same person or persons has/have signing authority, when there is no apparent economic or legal reason for such an arrangement (e.g. individuals serving as company directors for multiple companies headquartered at the same location);

   f. An account opened in the name of a recently formed legal entity in which the level of deposits is disproportionately high relative to the expected income of the founders of the entity;

   g. The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer;

   h. An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation; and

   i. An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

2. Deposits and Withdrawals

   a. Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business (for example, deposits that include a mix of business, payroll and social security cheques);

   b. Large cash withdrawals made from a business account not normally associated with cash transactions;

   c. Large cash deposits made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted using cheques or other payment instruments;

   d. Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to relate to the normal use of the account;

   e. Multiple transactions carried out on the same day at the same branch of a bank but with an apparent attempt to use different tellers;

   f. The structuring of deposits through multiple branches of the same bank or by groups of individuals who enter a single branch at the same time;

   g. The deposit or withdrawal of cash in amounts that are consistently just below identification or reporting thresholds;

   h. The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements; and

   i. The deposit or withdrawal of multiple monetary instruments in amounts that fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

3. Wire Transfers

   a. Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements;

   b. Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the wire transfer, when the inclusion of such information would be expected;

   c. Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries; and

   d. Foreign exchange transactions that are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations that have no apparent business connection with the customer, or to countries of specific concern.

4. Characteristics of the Customer or His or Her Business Activity

   a. Funds generated by a business owned by individuals of the same origin or involvement of multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types;

   b. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.);

   c. Stated occupation of the customer is not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area);

   d. Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction;

   e. A safe deposit box is opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box; and

   f. Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

5. Transactions Linked to Locations of Concern

   a. Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g. countries designated by national authorities, FATF non-cooperative countries and territories);

   b. Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (e.g. countries designated by national authorities, or FATF non-cooperative countries and territories);

   c. A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern;

   d. The use of multiple accounts to collect and then funnel funds to a small number of foreign beneficiaries, both individuals and businesses, particularly when these are in locations of specific concern;

   e. A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations;

f. The opening of accounts of financial institutions from locations of specific concern; and

g. The sending or receipt of funds by international transfers from and/or to locations of specific concern.

Appendix 5 – Examples of Red Flags for Trade-based Related Transactions

The list below is a sample of red flags for trade–based related transactions. It is not exhaustive and each bank should establish its own list of red flags that is tailored and updated according to its business activities and circumstances, using a risk-based approach.

a. The commodity is shipped to (or from) a jurisdiction designated as "higher risk" for ML/TF activities.

b. Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.

c. Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.

d. The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities.

e. The type of commodity shipped appears inconsistent with the exporter's or importer's regular business activities.

f. The method of payment appears inconsistent with the risk characteristics of the transaction.

g. The transaction involves the receipt of cash (or other payments) from third-party entities that have no apparent connection with the transaction.

h. The transaction involves the use of repeatedly amended or frequently extended letters of credit.

i. The commodity is transhipped through one or more jurisdictions for no apparent economic reason.

j. The shipment does not make economic sense.

k. The transaction involves related-party transactions.

Appendix 6 – Recommended Reading for Practitioners

a. Bank for International Settlements (Basel Committee on Banking Supervision)
www.bis.org/bcbs
b. The Financial Action Task Force
www.fatf-gafi.org/
c. Wolfsberg Standards
www.wolfsberg-principles.com
d. The Egmont Group of Financial Intelligence Units
www.egmontgroup.org/
e. Australian Transaction Reports & Analysis Centre (Austrac)
www.austrac.gov.au
f. Financial Crimes Enforcement Network (Fin CEN)
www.fincen.gov
g. Hong Kong Monetary Authority (HKMA)
www.info.gov.hk/hkma/eng/guide/index.htm
h. Monetary Authority of Singapore (MAS)
www.mas.gov.sg
i. The Association of Banks in Singapore (ABS)
www.abs.org.sg
j. Singapore Statutes
statutes.agc.gov.sg
k. Prudential Regulation Authority (PRA)
www.bankofengland.co.uk/pra/Pages/default.aspx
l. Financial Conduct Authority (FCA)
www.fca.org.uk/
m. Swiss Financial Market Supervisory Authority (FINMA)
www.finma.ch/e/Pages/default.aspx
n. Commercial Affairs Department (CAD)
www.cad.gov.sg
o. Organisation for Economic Co-operation and Development (OECD)
www.oecd.org
p. International Monetary Fund (IMF)
https://www.imf.org
q. Joint Money Laundering Steering Group (JMLSG)
www.jmlsg.org.uk/
r. Dann, C. et al. (2014) *A Guide on Financial Crime Prevention in Trade Finance*.
s. Financial Conduct Authority Thematic Review TR13/3 – *Banks' Control of Financial Crime Risks in Trade Finance*
https://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf
t. Committee on the Global Financial System (No.50) – Trade Finance: Developments and Issues
https://www.bis.org/publ/cgfs50.pdf
u. Singapore National Money Laundering and Terrorist Financing Risk Assessment Report 2013
www.mof.gov.sg/portals/0/data/cmsresource/Press%20Release/2013/Singapore%20NRA%20Report.pdf