# AML, CTF & Sanctions Guidance Part II

Published by the NVB

20 April 2020

Nederlandse Vereniging van Banken

# Content

# Preface

This Part II of the AML, CFT & Sanctions Guidance comprises sector and product specific additional guidance and complements the general Guidance in Part I.

This Part II is incomplete on its own and must be read in conjunction with the main guidance set out in Part I of this AML, CFT & Sanctions Guidance. Please refer to the Preface of Part I for the applicable regulatory framework and the purpose and the scope of the Guidance.

Part II mainly provides an overview of certain sectors and products offered in the current financial industry while focusing on the identification and mitigation of ML TF risks. Specific sanctions risks related to these sectors and products are not (yet) addressed in this part of the guidance and will be further devoloped. Please refer to Part I chapter 4 for the general section on Sanctions.

# Chapter 1

# Retail banking

## Overview of the sector

1.1 Retail banking is the provision of standard current account, loan and savings products to private individuals. For many banks, retail banking is a mass consumer business and will generally not involve close relationship management by a named relationship manager. For the purposes of this Guidance, small and medium enterprises (SMEs) in the Retail sector are addressed in Chapter 2 Business banking.

## What are the money laundering and terrorist financing risks in retail banking?

*Money laundering*

1.2 The proceeds of crime may pass through retail banking accounts at all stages of the money laundering process. However, many millions of retail banking transactions are conducted each week and the likelihood of a particular transaction involving the proceeds of crime is very low. A bank's risk-based approach should therefore be designed to ensure that it places an emphasis within its strategy on deterring, detecting and disclosing in the areas of greatest perceived vulnerability.

1.3 For private individuals, the risk of money laundering is (however not limited to) the association with people who, knowingly or unknowingly, serve as intermediaries for criminals and criminal organisations (known as money mules or smurfers). For example, people are asked to deposit amounts of cash (derived from criminal activities) into their own accounts, followed by wire transfers to other accounts. Typically, the mule is paid for his/her services with a small part of the money transferred. The use of intermediaries makes it difficult to figure out the identity of the fraudster and also the source of funds.

1.4 In addition, there is an increasing risk of fraudulent applications by identity thieves. This may present a higher risk especially in case the customer is onboarded via a non-face-to-face channel, if the bank does not have sufficient controls in place (see Part I).

### *Terrorist financing*

1.5 The risk of terrorist financing in relation to private individual customers is linked (however not limited to) the situation where people who, knowingly or unknowingly, finance a terrorist organization or individual, such as Foreign Terrorist Fighters (FTFs), returnees and home grown terrorists. All these categories needs funds to maintain an organization or network, or buy necessary supplies when preparing for or even conducting a terrorist attack, including training and travelling to the conflict zones.

1.6 While it might not be evident at the onset of the customer relationship that a customer is involved in terrorist activities, red flags such as the customer being reluctant to reply to the bank's request for information on suspicion of TF or adverse media reports that the customer is linked to known terrorist organisations, must lead to further investigations into the customer relationship. In addition to measures taking during onboarding, monitoring of such customer relationships to identify any (other) red flags for terrorist financing plays an important role, as described in section 1.25 below.

## Customer due diligence

### *General*

1.7 For the majority of personal applicants, sole or joint, the standard identification and verification requirements set out in Part I of the AML/CTF and Sanctions Guidance are applicable, including in the case of customers not met face-to-face.

1.8 The AML/CTF checks carried out at account opening are very closely linked to anti-fraud measures and are one of the primary controls for preventing criminals opening accounts or obtaining other services. Therefore, banks should co-ordinate these processes, in order to provide as strong a gatekeeper control as possible.

1.9 Where a bank determines that a particular customer relationship or transaction presents a low degree of risk of ML/TF, having taken into account the risk assessment the bank has carried out, simplified customer due diligence measures may be applied. Banks must thereby consider the risk factors listed in annex II EU Directive 2015/849 and the ESA Guidelines on Risk Factors. This means that banks, before applying simplified due diligence (SDD), must ascertain that the customer relationship presents a lower degree of risk. Refer to pragraphs 1.520 – 1.5.28 of Part I for more information on SDD.

1.10 However, a bank should take care with customers whose identity is verified under a variation from the standard (as described in Part I) and who wish to migrate to other products in due course. The verification of identity undertaken for a basic bank account may not be sufficient for a customer migrating to a higher risk product. Banks should have processes defining what additional due diligence, including where appropriate further verification measures , is required in such circumstances.

1.11 Where the incentive to provide a false identity is greater, banks must consider deploying suitable fraud prevention tools and techniques to assist in alerting to false and forged identification. Where the case demands, a bank might require proof of identity additional to the standard evidence.

*A customer with an existing account at the same bank*

1.12 If it cannot be established that the customer's identity was previously verified, an application will trigger standard identification procedures.

1.13 If the customer's identity has been verified to a standard commensurate with the risk associated with the customer relationship, a second account would normally be opened without further measures, provided the characteristics of the new account are not in a higher risk category than the existing account. Thus, a foreign currency account might require further measures and/or additional customer enquiries but for a new savings account, where the applicant's existing account had been subject to adequate CDD checks, most banks would not require further measures.

*Customers with a bank account with one entity who wish to transfer it to another entity within the financial group*

1.14 Where different Dutch regulated financial institutions in the same financial group (not between different banks) share a customer and (before or after any current customer review) transfer a customer between them, either institution can rely on the other institution's review checks in respect of that customer. Care will need to be exercised by the receiving part of the group to be satisfied that the previous CDD measures provide an appropriate level of assurance for the new account, which may have different risk characteristics from the one held with the other part of the group.

*Non-residents in the Netherlands wishing to open a bank account*

1.15 EU law creates a right for private individuals who are legally resident in the EU and have a sound economic or lawful rationale in the Netherlands to obtain a basic bank account, but this right applies only insofar as banks can comply with their AML/CTF obligations. Where the customer is a non-resident, it should be addressed up front if their needs could be better serviced elsewhere and if there is a sound economic or lawful rationale for the customer requesting the type of financial service.

*Lending (personal loans and mortgages)*

1.16 Many applications for advances are made through intermediaries, who may carry out some of the customer due diligence on behalf of the lender (see 1.24). In view of the generally low money laundering risk associated with mortgage business and related protection policies, and the fraud prevention controls in place within the mortgage market, use of confirmations from intermediaries introducing customers is, in principle, perfectly reasonable, where the introducer is carrying on appropriately regulated business including appointed representatives of authorised banks by Recognised Regulators (see Annex II in Part I).

*Enhanced due diligence*

1.17 Enhanced due diligence is required under article 8 (2) of the Wwft which prescribes that measures must be taken to compensate for the higher risks as reflected in Annex III of EU Directive 2015/849.

The enhanced due diligence measures to be applied in certain high risk situations are described in Part I of this Guidance.

1.18 The following are examples of higher risk situations where enhanced due diligence is required:

- The identification of PEPs as customers
- Adverse media on the customer
- Non-residents especially when there is no sound economic or lawful rationale in the Netherlands

*Financial exclusion*

1.19 According to EU Directive 2014/92/EU and the Wft every lawful EU resident with a relevant connection in the Netherlands is entitled to a basic bank account.[1] This way it is ensured that those categories of individuals which might not qualify for standard banking products ("financially excluded" such as homeless, refugees, inmates) may still have access to a basic bank account.

1.20 The "financially excluded" are not a homogeneous category of uniform risk. Some financially excluded persons may represent a higher risk of money laundering or terrorist financing regardless of whether they provide standard or non-standard evidence to confirm their identity, e.g., a passport holder who qualifies only for a basic account on credit grounds. Banks may wish to consider whether any additional customer information, or monitoring of the size and expected volume of transactions, would be useful in respect of some financially excluded categories, based on the bank's own experience of their operation.

1.21 In other cases, where the available evidence of identity is limited, and the bank judges that the individual cannot reasonably be expected to provide more, but that the customer relationship should nevertheless go ahead, it must consider instituting enhanced monitoring arrangements over the customer's transactions and activity. In addition, the bank should consider whether restrictions should be placed on the customer's ability to migrate to other, higher risk products or services.

1.22 Where an applicant produces non-standard documentation (See chapter 2, Part I), a thourough judgment should be made that the evidence available does not provide a sufficient level of confidence

[1] https://www.betaalvereniging.nl/betaalproducten-en-diensten/basisbankrekening/

that the applicant is who he claims to be, in which event a decision not to open the account would reasonably be justified.

*Monitoring*

1.23 In retail banking operations that are of significant size, automated monitoring in generally applied. However, staff vigilance is also essential, in order to identify counter transactions in particular that may represent money laundering or terrorist financing, and in order to ensure prompt reporting of initial suspicions.

1.24 Particular activities that should trigger further enquiry include lump sum repayments outside the agreed repayment pattern, and early repayment of a loan, particularly where this attracts an early redemption penalty, as these might be indicators of money laundering. Large cash deposits on and cash withdrawals from accounts of retail customers must also trigger further enquiry. Please note that these are examples and therefore not an exhaustive overview.

1.25 The below mentioned indicators/red flags may relate to financing of terrorism by private individuals. It should be noted that they are not exhaustive and may change over time based on changing behaviour of terrorists or their financiers.

*General indicators*

- Any behaviour related to hiding the identity of the client, including usage of false, stolen or fraudulent identity papers;
- Client is reluctant to provide information;
- Transactions occur 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 transaction2;
- Media reports that the client is linked to known terrorist organisations or is engaged in terrorist activities;
- Media reports that the client supports extremist ideologies;
- (Cash) Transactions are structured below the reporting threshold (when applicable);
- Usage of alternative payment methods: cryptocurrency, prepaid debit cards, remittance services by currency/money exchangers, etc.

*Indicators related to Foreign Terrorist Fighters, prior to departure:*

- Purchasing goods at camping or survival stores;
- Purchasing first-person shooter games or engaging in combat training-type activities (i.e. airsoft, paintball);
- Purchase of international airline/bus/train tickets and payment of travel related fees (e.g., visa fees) involving countries near conflict areas;
- Establishing lines of credit and taking out personal loans where no loan repayments are made;
- Liquidating personal assets, including retirement accounts/plans, and obtaining life insurance policies;
- Receiving funds from or sending funds to seemingly unrelated individuals who are located near conflict areas, and the transactions do not appear to have a lawful business purpose. These seemingly unrelated individuals may share common or similar addresses, telephone numbers, or other identifying information.

*Indicators related to Foreign Terrorist Fighters, while staying abroad:*

- When the client is travelling, transactions on the account may show geographical locations near conflict areas, known travel hubs or may show a 'trail' of, for example, payments at petrol stations on the way to the conflict area;
- Typically there is little to none account activity initiated by the clients (i.e. no debit wire transfers, only collections, credit transfers may occur);
- ATM withdrawal near conflict area shortly after credit transfer;
- Transfers using payment instructions for communication purposes;
- Payments related to telecommunication (e.g. Skype, 1 cent verification payments).

*Indicators related to returnees:*

- Sudden account activity initiated by the client after a long period of inactivity;
- Credit transfers from conflict areas or adjacent countries.

# Chapter 2

# Business banking

## Overview of the sector

2.1 Business banking in the Retail sector is by nature a volume business, typically offering services for small Dutch businesses, ranging from sole traders and small family companies to partnerships, professional firms and smaller private companies (e.g. low turnover, low number of employees), also known as small and medium enterprises (SMEs). These businesses are often, but not always, based in the Netherlands in terms of ownership, location of premises and customers. As such, the risk profile may actually be lower than that of larger businesses with a more diverse customer base or product offering, which may include international business and customers. The risk profile may, however, often be higher than that of private individuals, where identification may be straightforward and the funds involved smaller.

## What are the money laundering and terrorist financing risks in business banking?

*Money laundering*

2.2 In relation to small and medium enterprises, a particular area of risk is related to the provision of services to cash-generating businesses. Some businesses are legitimately cash based, including large parts of the retail sector, and so there will often be a high level of cash deposits associated with some accounts. The risk is in failing to identify such businesses where the level of cash activity is higher than the underlying business would justify, thus providing grounds for looking more closely at whether the account may be being used for money laundering. A red flag can be the deposit of unusually large amounts of high value denomination banknotes.

2.3 Where a loan results in the borrower receiving funds from the lender, the initial transaction is not very susceptible of the placement stage of money laundering, although it could form part of the layering stage. The main money laundering risk arises

through the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination. Where loans are made in one jurisdiction, and collateral is held in another, this may indicate an increased money laundering risk.

*Terrorist financing*

2.4 Non-profit organisations (such as charities or religious establishments), which are typically serviced as SMEs, are considered particularly suitable vehicles for financing terrorists and terrorist organisations. Red flags that could be indicators of involvement in terrorist activities are charitable activity in or near conflict areas, unregulated charities, or negative media reports that the customer supports extremist ideologies. Also here it is important to conduct continuous monitoring in order to detect any suspicions of potential involvement in terrorist activities.

## Customer due diligence

*General*

2.5 Essentially, as set out in Wwft 3(2)b identification should initially focus on ascertaining information about the business and its activities and verifying UBOs holding or controlling directly or indirectly, 25% or more of the shares or voting rights, and controllers.

2.6 Uncertainties may often arise with a business that is starting up and has not yet acquired any premises (e.g., X & Y trading as ABC BV, working from the director/principal's home). A search in the trade register of the Chamber of Commerce may not always produce relevant information if the company is newly formed.

2.7 In the case of newly-formed businesses, obtaining appropriate customer information is sometimes not easy. The lack of information relating to the business can be mitigated in part by making sufficient additional enquiries to understand fully the customer's expectations (nature of proposed activities, anticipated cash flow through the accounts, frequency and nature of transactional activity, an understanding of the underlying ownership of the business) and personal identification of the owners/controllers of the business, as well as information on their previous history.

2.8 Banks may encounter difficulties with validating the business entity, particularly where directorships may not have been registered or updated. If a bank can neither satisfy itself as to the identity of a customer or the UBO, nor verify that identity, nor obtain sufficient information on the nature and intended purpose of the customer relationship, it must not enter into a new customer relationship and must terminate an existing one (Wwft 5).

2.9 A bank must be reasonably satisfied that the persons starting up the business are who they said they are, and are associated with the company. Reasonable steps must be taken to verify the identity of the persons setting up a new business, as well as any UBOs, which may often be based on electronic checks. In the majority of cases, the individuals starting up a business are likely to be its UBOs. A check of the amount of capital invested in the business, whether it is in line with the bank's knowledge of the individual(s) and whether it seems in line with their age/experience, etc, may be a pointer to whether further enquiries need to be made about other possible UBOs.

2.10 Wherever possible, documentation of the company's business address should be obtained. Where the bank can plausibly argue that this is not possible because it is in the early stages of start-up, the address of the company should be verified later; in the interim, the bank may wish to obtain evidence of the address(es) of the person(s) starting up the business. In certain circumstances, a visit to the place of business may be helpful to confirm the existence and activities of the business.

*Enhanced due diligence*

2.11 Enhanced due diligence is required under article 8 (2) of the Wwft which prescribes that measures must be taken to compensate for the higher risks as reflected in Annex III of EU Directive 2015/849. The enhanced due diligence measures to be applied in certain high risk situations are described in Part I of this Guidance.

2.12 Banks will need to consider making more penetrating initial enquiries, over and above that usually carried out before taking on businesses whose turnover is likely to exceed certain thresholds, or where the nature of the business is higher risk, or involves large cash transactions. Recognising that there are a

very large number of small businesses which are cash businesses, there will be constraints on the practicality of such enquiries; even so, banks should be alert to the increased vulnerability of such customers to laundering activity when evaluating whether particular transactions are suspicious. In case a customer relationship is deemed to be suspicious, the reporting requirements as described in Part I must be met.

2.13 Examples of higher risk situations are:

- High cash turnover businesses: casinos, bars, clubs, taxi firms, launderettes, takeaway restaurants, massage and nail businesses;
- Money service businesses: cheque encashment agencies, bureaux de change, money transmitters;
- Legal entities such as educational establishments, healthcare companies (including child care) making use of subsidies and allowances, especially in relation to a personal budget ( " persoonsgebonden budget" ), may pose a higher risk of fraudulent activities;
- Gaming and gambling businesses;
- Computer/high technology/telecom/mobile phone sales and distribution, noting especially the high propensity of this sector to VAT 'Carousel' fraud;
- Used cars businesses due to susceptibility of tax fraud;
- Companies registered in one offshore jurisdiction as a non-resident company with no local operations but managed out of another, or where a company is registered in a high risk jurisdiction, or where UBOs with significant interests in the company are resident in a high risk jurisdiction;
- Unregistered charities based or headquartered outside the Netherlands, foundations, cultural associations and the like, particularly if centred on certain target groups, including specific ethnic communities, whether based in or outside the Netherlands (see FATF Typologies Report 2003/4 under 'Non-profit organisations' – at www.fatf-gafi.org).

*Monitoring*

2.14 In relation to non-profit organisations, monitoring should be focused on detecting whether the use of funds by the customer is not consistent with the purpose for which it was established, for example wire transfers to other areas than the ones indicated during onboarding or in the official documents of the organisation.

# Chapter 3

# Money service businesses
## (as customers of banks)

### Overview of the sector

3.1 The MSB industry[2] ranges from large international companies with numerous outlets and/or a network of operating agents worldwide to small local MSBs that operate as a principal in their own right.
MSBs offer money transfers which play a vital role in tranfering money to countries without a proper operating financial system and/or with a large population of unbankables. MSBs serve a wide range of different types of customers.

*Article 2:54i Wft*

3.2 An MSB established in the Netherlands must, for the execution of its activities, obtain a license for the undertaking of money transfers from DNB. MSBs which are licensed to operate in NL can be found in the applicalbe register on the website of DNB.

MSBs established and licenced in the EEA may, based on their "EU passport", operate in the Netherlands. However MSBs may only offer their services abroad if they have passed the notification procedure of the supervisor in their home member state and this supervisor has forwarded this notification to host regulator in this case DNB. This chapter focuses specifically on the ML/TF risks of MSBs and the applicable due diligence measures and not on their agents.

3.3 MSBs are subject to the full provisions of the Wwft.

### What are the money laundering and terrorist financing risks in MSBs?

3.4 Several features of the MSB sector make it an attractive vehicle through which criminal and terrorist funds can enter the financial

[2] For definition see glossary in Part I

system, such as the simplicity and certainty of MSB transactions, worldwide reach, the cash character of transactions, the often less stringent customer identification rules that are applied to low value transactions compared with opening bank accounts and reduced possibilities for verification of the customer's identification than in credit or other financial institutions. The nature of the underlying customer's relationship with the MSB and a low frequency of contact with them can also be a significant vulnerability.

3.5 Generally, MSBs can be used for money laundering and terrorist financing in two ways: either by wittingly or unwittingly performing relevant transactions for their customers without knowledge of the illegal origin or destination of the funds concerned, or by a direct involvement of the staff/management of the provider through complicity or through the ownership of such businesses by a criminal organisation. They can be used in all stages of the money laundering process.

3.6 Obtaining ownership of an MSB either directly or via sub-agent relationships provides criminals a perfect tool to manipulate the money transfer system and to launder money. Detecting such cases depends, to a certain extent, on the bank applying CDD measures and monitoring/reporting obligations effectively. The following (non-limitative) indicators could be relevant in this context:

- Reluctance by the MSB to provide information about their AML/CTF policies and procedures and/or the identity of their customers when requested by the bank;
- Use of false identification and fictitious names for customers;
- Turnover of the MSB exceeding, to a large extent, the cash flows of other comparable businesses in the sector;
- Suspicious connections of the MSB owner;
- Suspicious transactions performed on the bank accounts of the MSB or its owner;
- Suspicion that a business (such as a travel agent or corner shop) is actually providing MSB services to the customers of its primary business, or leveraging another business name/type to cover up unregistered activity;
- Overly complicated agent/principal networks (e.g multiple principals for one agent, agents with their own agents etc.) with inadequate oversight by principal;

- Deposits of unusally large amounts of high value denomination banknotes (such as EUR 500);
- The agents of the MSB do not comply to the policies the MSB provided to the bank;
- The money tranfers involving increased/high risk countries, e.g. countries which are known to be used as corridors for ML/TF;
- Periodic transfers made by several people to the same beneficiary or related persons;
- Transfers over a short period of time of low amounts that together represent a large sum of money.

3.7 Many reported cases of abuse involve small value wire transfers (although some involve high-value amounts), but the total value of funds involved in these cases can be quite significant, raising the possible involvement of organised criminal activity.

## Risk assessment

3.8 (Global) banks are increasingly terminating or restricting customer relationships with MSBs. This practise is called “de-risking”. Global organisations such as the World Bank, Financial Stability Board and the FATF are concerned that this practise will frustrate AML/CTF objectives and may not be an effective way to fight ML/TF. By pushing higher risk transactions out of the regulated system into more opaque, informal channels, they become harder to monitor. Banks must take a risk-based approach to implement AML/CTF measures.

3.9 The inherent risk in the MSB sector is not the nature of the sector itself, but the potential for the abuse of the sector by criminals. It is therefore important that banks understand these potential risks, and manage them effectively.

3.10 A bank should establish whether the MSB is itself regulated for money laundering/terrorist financing prevention and, if so, whether the MSB is required to verify the identity of its customers and apply other AML/CTF controls – in the case of a non-NL MSB, whether these obligations and controls are in line with NL standards, or with standards equivalent to those laid down in the EU Directive 2015/849.

3.11 A bank should determine whether the MSB is a principal in its own right, or whether it is itself an agent of another MSB (as part

of a franchise model). MSBs which operate as principal, or through a limited number of offices/agents present a different risk profile from MSBs which operate through a network of agents – it is important to understand the way the latter type of MSB monitors and confirms compliance by its agents with the AML/CTF controls it lays down.

3.12 MSBs which carry out periodic internal or external audits or reviews of their AML/CTF controls, including those at its branches and agents, demonstrate a more pro-active management of their ML/TF profile. The outcome of such audits or reviews will be of interest to banks.

3.13 The information about an MSB that banks should consider obtaining as part of their risk assessment includes:

- Types of products and services offered
  In order to assess risks, banks should know the categories of money services engaged in by the particular MSB customer.
- Maturity of the business, and its owners' experience
  It is relevant to consider whether or not the MSB is a new or established operation, the level of experience the management and those running the business have in this type of activity, and whether or not providing money services are the customer's primary, or an ancillary, business.
- Location(s) and market(s) served
  Money laundering risks within an MSB can vary widely depending on the locations, customer bases, and markets served. Relevant considerations include whether markets served are domestic or international, or whether services are targeted to local residents or to broad markets.
- Anticipated account activity
  Banks should ascertain the expected services that the MSB will use, such as currency deposits or withdrawals, cheque deposits, or funds transfers. For example, an MSB may only operate out of one location and use only one branch of the bank, or may have several agents making deposits at multiple branches throughout the bank's network. In order to monitor the MSB effectively the bank must identify its expected transaction profile.
- Purpose of the account
  Banks should understand the purpose of the account for the MSB. For example, a money transmitter might require the bank account to remit funds to its principal clearing account

or may use the account to remit funds cross-border to foreign-based agents or beneficiaries. Accounts for use in the MSBs remittance business should be separate from accounts used for the administration of the MSB itself.
- The MSB's settlement arrangements, including the relationship with parties involved in the payment chain (from ordering MSB to beneficiary MSB). The MSB involved is expected to have assessed the risks related to these parties and must be able to evidence this.
- The public disciplinary record of the MSB, to the extent that this is available.

3.14 As with any category of customer, there will be some MSBs that present lower risks of money laundering compared with those that pose a significant risk. Banks should therefore take a risk-based approach and neither define nor treat all MSBs as intrinsically posing the same level of risk.

3.15 Annex 3-I lists factors that might indicate a lower, or higher, risk of ML/TF in MSBs.

## Customer due diligence

### *About the customer*

3.16 The bank should ensure that it fully understands the MSB's legal form, structure and ownership, and must obtain sufficient additional information on the nature of the MSB's business, and the reasons for seeking the product or service. See also chapter 2 of Part I.

3.17 It is important to know and understand any associations the MSB may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc.) and the individuals who may influence its operations (political connections, etc.). A visit to the place of business may be helpful to confirm the existence and activities of the MSB.

### *Ownership and control*

3.18 In addition to Part I and following the bank's assessment of the money laundering or terrorist financing risk presented by the MSB, it may decide to verify the identity of one or more directors, as appropriate, in accordance with the guidance for private

individuals in Part I.Banks should at least verify the identity of those who have authority to operate the account or to give the bank instructions concerning the use or transfer of funds or assets.

*MSB's AML/CTF policies*

3.19 As with any other customer subject to AML obligations, the extent to which a bank should enquire about the existence and operation of the anti-money laundering programme of a particular MSB will be dictated by the bank's (re-)assessment of the risks of the particular relationship. Given the diversity of the MSB industry and the risks they face, there may be significant differences among AML programmes of MSBs. The resources and experience available within the MSB's compliance function and, in a principal/agent situation, how the principal ensures and monitors compliance with the AML/CTF standards in their agents, are also relevant.

3.20 In the light of the information that the bank has on the MSB's AML/CTF policies and procedures, it should consider what further steps it should take to be comfortable that these policies are reasonable and effective, possibly including seeing the results of an audit or review of the MSB's AML/CTF policies and procedures.

*Enhanced Due Diligence (EDD)*

3.21 A bank's due diligence should be commensurate with the level of risk of the MSB customer identified through its risk assessment. If a bank's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be required to conduct further due diligence in a manner commensurate with the heightened risk.

3.22 Whenever faced with less transparency or less independent means of verification of the customer entity, banks should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of other shareholders and/or controllers.

3.23 While the extent to which banks should perform further due diligence beyond the minimum will be dictated by the level of risk

posed by the particular customer, it is not the case that all MSBs will always require additional due diligence. In some cases, no further customer due diligence will be required - in other situations, however, the further due diligence required may be extensive. In all cases, the level of due diligence applied will be dictated by the risks associated with the particular customer.

3.24 Depending on the level of perceived risk, and the size and sophistication of the particular MSB, banks may pursue a range of actions as part of an appropriate due diligence review or risk management assessment of an MSB seeking to establish an customer relationship. Similarly, if the bank becomes aware of changes in the profile of the MSB to which services are being provided, additional steps may be appropriate.

3.25 Where the customer is an (unregulated) MSB established outside NL additional due diligence should be undertaken to ascertain and assess the effectiveness of the MSB's internal policy on money laundering/terrorist financing prevention and its CDD and activity monitoring controls and procedures. In larger cases, where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to NL or equivalent standards.

3.26 Where there are indications that the risk associated with an existing customer relationship might have increased, the bank should, depending on the nature of the product or service provided, request additional information, for example as to the MSB's activities, customer base or ownership, in order to decide whether to continue with the relationship.

*Ongoing monitoring*

3.27 Banks are required to conduct ongoing monitoring of customer relationships, and to identify and report known or suspected unusual/suspicious activity or transactions. Risk-based monitoring of accounts maintained for all customers, including MSBs, is a key element of an effective system to identify and, where appropriate, report suspicious activity. The level and frequency of such monitoring will depend, among other things, on the bank's risk assessment and the activity across the account. The bank may require that a regular (or periodic) audit or review

of the MSB's AML/CTF controls is carried out and the results will be handed over to the bank.

3.28 Based on the bank's assessment of the risks of its particular MSB customer, monitoring should include periodic confirmation that initial projections of account activity have remained reasonably consistent over time. The mere existence of unusual transactions does not necessarily mean that a problem exists, but may be an indication that additional review is necessary.

3.29 Examples of unusual activity across MSB accounts, that may or may not be potentially suspicious generally involving significant unexplained variations in transaction size, nature, or frequency through the account, could include (not limited to):

- A money transmitter transferring funds to a different jurisdiction from expected based on the due diligence information that the bank had assessed for the particular money services business. For example, if the money transmitter represented to the bank or in its business plan that it specializes in remittances to Latin America and starts transmitting funds on a regular basis to another part of the world, the unexplained change in business practices may be indicative of suspicious activity;
- A money transmitter or seller/issuer of money ordering deposits currency significantly in excess of expected amounts, based on the due diligence information that the bank had assessed for the particular MSB, without any justifiable explanation, such as an expansion of business activity, new locations, etc.

3.30 Given the importance of the requirement for MSBs to be licensed, a bank should file a suspicious activity report if it becomes aware that an MSB is operating in the Netherlands without an appropriate license.

# Annex 3-I Risk Indicators

To assist banks in determining the level of risk posed by an MSB as a customer, the following are examples that may be indicative of lower and higher risk, respectively. In determining the level of risk, a bank should not take any single indicator as determinative of the existence of lower or higher risk. Moreover, the application of these factors is fact-specific, and a conclusion regarding an account should be based on a consideration of available information.

An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be weighed more heavily than others.

Examples of potentially lower risk indicator:

The MSB:

- Primarily markets to customers that conduct routine transactions with moderate frequency in low amounts;
- Is an established business with a known operating history;
- Is a money transmitter that only remits funds to domestic entities;
- Only facilitates domestic bill payments.

Examples of potentially higher risk indicator:

The MSB:

- Allows customers to conduct higher-amount transactions with moderate to high frequency;
- Offers multiple types of money services products;
- Is a cheque casher;
- Is a money transmitter that offers only, or specialises in, cross-border transactions, particularly to jurisdictions posing heightened risk for money laundering or the financing of terrorism or to countries identified as having weak anti-money laundering controls or to countries subject to detailed and large scale financial sanction regimes;
- Is a currency dealer or exchanger for currencies of jurisdictions posing heightened risk for money laundering or the financing of terrorism or countries identified as having weak antimoney laundering controls;
- Is a new business without an established operating history;
- Is a relatively small concern, with few staff but is a principal with a large agent network - this mitigates against effective supervision and control of agents;

- The MSB has agents who have agents of their own, or the principal is itself an agent of another business; or
- Carries out third party trade based settlements as part of the clearance process.

# Chapter 4

# Private Banking

*Note: This sectoral guidance is incomplete on its own. It must be read in conjunction with the main guidance set out in Part I of the Guidance.*

## Introduction

### *General Overview and Due Diligence*

4.1. Private Banking is the provision of banking and other investment services including advice, discretionary fund management and brokerage to private investors, ranging from the mass affluent to high and ultra-high net worth individuals (HNWI and UHNWI) and their families or businesses to sustain and grow long-term wealth. It is also known as Wealth Management (see EBA, ESMA Joint Guidelines 2017, chapter 5 point 143).

4.2 Although Private Banking is identified as inherently high risk, it does not necessarily mean that all customers serviced by Private Banking have to be considered higher risk.Private Banking customers must be subject to EDD measures, which may entail the application of the following requirements (not limited to):

- Verifying the source of funds and/or wealth; see Part I Chapter 2.3.
- Establishing the destination of funds;
- Ensuring that a customer's use of complex business structures such as trusts and private investment vehicles is for legitimate and genuine purposes.

## AML/CTF Risks

### *General*

4.3 Private Banking entails potentially higher integrity risks. In general these customers are very wealthy and often use more complex products and complex (tax-driven) structures. This follows, Annex III 4AMLD and art. 8 of the Wwft that states that EDD should be undertaken with reference to the Annex.

*Inherent Risks in Private Banking*

4.4 Money launderers are attracted by the availability of specialised products and the provision of services that operate internationally, utilise detailed knowledge of customers create a secure and reputable private banking environment and are familiar with transactions for private investors. This generates a layer of respectability that 'covers' criminal activity and, it is felt, protects it from investigation. The following factors contribute to the vulnerability of private banking:

- Wealthy and powerful customers: Such customers may be reluctant or unwilling to provide adequate documents, details and explanations. The situation with regard to them is exacerbated where the customer enjoys a high public profile, and may fall into the category of Politically Exposed Person (PEP), indicating that they wield or have recently wielded political or economic power or influence.
- Multiple and complex accounts: wealthy customers often have many accounts in more than one jurisdiction, either within the same bank or group, or with different financial institutions. In the latter situation it may be more difficult for relationship managers to accurately assess the true purpose and business rationale for individual transactions.
- Cultures of confidentiality: better off private banking customers may seek extra reassurance that their need for confidential business will be conducted discreetly will be met. However, requests for confidentiality should not lead to unwarranted levels of secrecy that suit those with criminal intentions or interfere with regulatory requirements.
- Concealment: The use of services such as offshore trusts and the availability of structures such as shell companies in some jurisdictions helps to maintain an element of secrecy about beneficial ownership of funds and may give rise to significant misuse. Care should be taken to ensure that use of banking and investment services in such countries does not facilitate the development of layers of obscurity that assist those with criminal intentions.
- Jurisdictions maintaining statutory banking secrecy: there is a culture of secrecy in some jurisdictions, supported by local legislation, in which private banking customers may hold accounts without being detected as doing so; it is very

difficult if not impossible to investigate whether these accounts have been used for laundered money.

- Corrupt jurisdictions: there are jurisdictions where corruption is known, or perceived, to be a common method of acquiring personal wealth. Attempts may be made to launder assets gained from corrupt practices in these jurisdictions through wealth management services.
- Movement of funds: The transmission of funds and other assets by private customers may involve high value transactions, and rapid transfers of wealth across accounts in different countries and regions of the world; this can facilitate the concealment of illicit funds before the authorities can catch up with them.
- The use of concentration accounts: i.e. multi-customer pooled/omnibus type accounts these are used to collect together funds from a variety of sources for onward transmission and can hide laundered money in the pooling; they are seen as a potential major risk.
- Credit: the extension of credit to customers who use their assets as collateral also poses a money laundering risk unless the lender is satisfied that the origin and source of the underlying asset is legitimate.

4.5 Secured loans where collateral is held in one jurisdiction and the loan is made from another are common in the private banking areas. Such arrangements may serve a legitimate business function and make possible certain transactions which may otherwise be unacceptable due to credit risk. But they may also make it easier to conceal the sources of illicit funds. Collateralised loans raise different legal issues depending on the jurisdiction of the loan, but foremost among these issues are the propriety and implications of guarantees from third parties (whose identity may not always be revealed) and other undisclosed security arrangements that may hide the true nature of the collateral. Particular care should be taken where the lender is relying upon the guarantee of a third party not otherwise in a direct customer relationship, and where the collateral is not in the same jurisdiction as the lending firm.

## Assessment of the Risk

4.6 The role of the relationship manager is particularly important to the private bank in managing and controlling and mitigating the money laundering or terrorist financing risks it faces. Relationship managers develop strong personal relationships with their customers, which facilitates the collection of the necessary information to know the customer's business and financial affairs, including knowledge of the source(s) of the customer's wealth. However, wealthy customers can have business affairs and lifestyle that may make it difficult to establish what is "normal" and therefore what may constitute unusual behaviour.

4.7 Relationship managers must, however, at all times be alert to the risk of becoming too close to the customer and to guard against the risks from:

- A false sense of security;
- Conflicts of interest which may compromise the firm's ability to meet its AML obligations and its wider financial crime responsibilities;
- Undue influence by others, especially by the customers themselves.

# Chapter 5

# Discretionary and Advisory Investment Management

## Overview of the sector

5.1 Investment management includes both discretionary and advisory management of segregated portfolios of assets (securities, derivatives, cash, property etc.) for customers. Where investment management is provided as part of a broader "private banking" service please refer to Chapter 7. In cases in which an investment manager is the customer of the bank please refer to brokerage services for funds (Chapter 13).

5.2 Discretionary managers are given powers to decide IPO securities selection and to undertake transactions within the portfolio as necessary, according to an investment mandate agreed between the manager and the customer.

5.3 Advisory relationships differ, in that, having determined the appropriate securities selection, the manager has no power to deal without the customer's authority - in some cases the customer will execute their own transactions in light of the manager's advice.
This should not be confused with "financial advice", which involves advising customers on their investment needs (typically for long-term savings and pension provision) and selecting the appropriate products.

5.4 The activities referred to above may be carried out for private or institutional investors. Typical investors to whom investment managers provide services are high net worth individuals, trusts, companies, government bodies and other investing institutions such as pension schemes, charities and open/closed-ended pooled investment vehicles.

## Customer Due Diligence

### *Who is the customer from CDD perspective?*

5.5 Who the customer of the bank is depends on the role fulfilled by the bank, which can take different forms:
a) The bank fulfils an investment management role;
b) The role of investment manager is fulfilled by an independent asset manager, who introduces the customer to the bank;
c) The bank performs an intermediary role for its customer in the provision of the product by a third party.

5.6 In cases in which the bank fulfils the role of investment manager, the customer is the company or individual that owns the segregated portfolio or assets under management.

5.7 Where the customer is introduced to the bank by an independent investment manager who has a mandate to act on behalf of the customer, a customer relationship exists with both the investment manager and the customer. (See chapter 13)

When an independent investment manager introduces its own funds to the bank, what constitutes a customer relationship, may depend on the way in which the contractual obligations are organised. When one of these subfunds is party to a commercial contract between the bank and the investment manager, this is likely to constitute a customer relationship with the subfund.

In fulfilling their CDD obligations banks may consider taking a risk based approach by placing reliance on the CDD performed by the investment manager in situations that have been determined to be lower risk. Refer to Part I, Chapter 2 for more information on reliance on third parties.

5.8 Where the bank performs an intermediary role and the product is offered by a third party, the bank remains responsible for performing CDD on the customer provided with the product. However, the bank may consider relying on the third party's CDD measures taking into account Part I, Chapter 2.

### *Customer due diligence*

5.9 Please refer to Part I, Chapter 2 for the applicable CDD measures.

*Custody and third party payments/transfers*

5.10 In cases in which money or investments are to be received from or transferred to someone other than a person who has been verified as a customer or UBO, the reasons behind the payment/transfer and the capacity of the third party will need to be understood. It should also be taken into consideration to which extent their identity may need to be verified. Whether this is the responsibility of the bank or a separate custodian will depend on how custody is provided and what the bank's role is with regard to the payment or transfer. Various likely scenarios are discussed in the following paragraphs.[3]

5.11 When the customer enters into an agreement directly with a custodian other than the bank, it is the custodian that should be concerned about third party payments and transfers. However, the bank should consider the issue itself, if it is involved in the transmission of funds or otherwise passes instructions to the custodian regarding a receipt or withdrawal of funds/investments.

5.12 The bank may provide custody notionally as part of its service to the customer, but outsource the safe-keeping function to a sub-custodian. In these circumstances, the bank will usually instruct the sub-custodian regarding receipts or withdrawals from the portfolio and should therefore take appropriate steps to verify the identity of any third party that may be involved. The bank should also ensure that the issue is addressed, either by itself or by the sub-custodian, where the customer is able to instruct the sub-custodian directly.

5.13 The bank may perform the custody function in-house, in which case it must take appropriate steps itself to verify the identity of any third parties that may be involved.

5.14 In any event, when the bank is asked to receive, make or arrange payment to/from someone other than a person it has verified as a customer or UBO, it should seek to understand the reasons behind the payment and the capacity of the third party and consider the extent to which the identity of that third party may need to be verified.

.....

[3] This issue concerns additions to and withdrawals from the customer's portfolio, as opposed to the settlement of transactions undertaken by the bank in the course of managing the portfolio.

*Additional customer information*

5.15 The customer take-on process for investment management customers usually involves gaining an understanding of the customers and their needs, and establishing at the outset the likely inflows and outflows of funds. Developments in this area and updates on customer information should be sought periodically from the customer or his adviser.

5.16 The customer information, obtained for the purposes of agreeing the bank's mandate and the ongoing management of the customer's portfolio, will usually comprise the additional information necessary to understand the nature and purpose of the relationship in a money laundering context, against which the customer's future activity should be considered.

*Monitoring*

5.17 Customer activity relates only to inflows and outflows of money that do not relate to the bank's own dealings in the portfolio of investments. Most movements into or out of the portfolio will usually be expected (e.g., pension scheme contributions or funding of pensions benefits). The bank should establish the rationale behind any unexpected ad hoc payments made or requested by the customer

## Money Laundering risk

5.18 In terms of money laundering risk, there is little difference between discretionary and advisory investment management. In both cases, the bank may itself physically handle incoming or outgoing funds, or it may be done entirely by the customer's custodian.

5.19 In either case, the typical bank deals with low volumes of high value customers, for whom there is likely to be a take-on process that involves a level of understanding of the customer's circumstances, needs and priorities and anticipated inflows and outflows of funds, in order to determine suitable investment parameters.

5.20 There is likely to be ongoing contact, often face-to-face, with the customer in order to review market developments and

performance, and review the customer's circumstances, etc. Unexpected inflows/outflows of funds are not common occurrences - ad hoc requirements and movements are usually the subject of discussion between the bank and the customer.

5.21 The risk of money laundering to the investment management sector, in the context of the "typical" circumstances described above, would be lower. Clearly, however, the risk will increase when dealing with certain types of customer, such as offshore trusts/companies, PEPs and customers from higher risk jurisdictions, and may also be affected by other service features that a bank offers to its customers[4]

.....

[4] Banks that provide investment management alongside banking facilities and other complex services should refer to Chapter 7: *Private Equity*.

# Chapter 6

# Asset Finance

## Introduction and legal obligations

### *General*

6.1 Asset Finance is a broad term referring to the financing of 'fixed assets'; they are typically tangible, such as equipment, transport vehicles, and plant and machinery, but not always (e.g. software). Assets can range from the very expensive, such as trains, ships, aeroplanes and oil rigs; through a mid-range such as plant and machinery, industrial installations and large IT projects; to low-value assets such as smaller IT and office equipment, cars and commercial vehicles.

6.2 Asset Finance customers (sometimes called 'End Users') can be businesses (in the form of legal persons or natural persons); public sector entities; and not for profit entities.

6.3 Household goods (home media and computing; 'white goods'; furniture) do not generally fall into the Asset Finance definition, even though they are assets. Rather they would come under the umbrella of Consumer Finance, unless being acquired by a commercial enterprise for commercial purposes, when these assets would fall into the definition of Asset Finance. Consumers (Non-Business) financing their cars would typically come under the umbrella of Motor Finance

### *Financial Products*

6.4 A variety of financial instruments are used to finance assets by Financial Institutions:
**(a) Lease:**
There are essentially two forms of lease (both identical from a legal perspective):
**Finance Lease:** the lessor purchases the asset, and the minimum contractual repayments recoup most (and generally all) of the capital cost of the goods for the lessor.

**Operating Lease:** the lessor purchases the asset, and the minimum contractual repayments recoup materially less than the capital cost of the asset for the lessor. A common form of operating lease is 'contract hire', which gives the customer the use of the asset, together with additional services such as maintenance and replacement of worn parts. Cars, commercial vehicles, forklift trucks and aeroplanes are often financed this way.

During the life of the contract, ownership of the asset resides with the lessor. At the end of the lease, legal title to the asset cannot pass directly from lessor to lessee, but in the case of finance leases the lessor will typically relinquish its own interest in the asset, or make arrangement for title to pass to the lessee via a third party.

**(b) Hire Purchase:**
The Hiror purchases the asset, and the contractual repayments due from the Hirer recoup the full cost of the asset for the Hiror. During the life of the contract, ownership of the asset resides with the Hiror. At the end of the contract, the Hirer has an Option to Purchase the asset for a nominal sum, which the Hiror fully expects the Hirer to exercise (and it would be highly unusual for the Hirer not to exercise such Option).

**(c) Conditional Sale:**
The lender purchases the asset, and the contractual repayments by the customer recoup the full cost of the asset for the lender. During the life of the contract, ownership of the asset resides with the lender, but at the end of the contract legal title in the asset automatically passes to the customer.

**(d) Credit Sale:**
The lender purchases the asset, and the contractual repayments by the customer recoup the full cost of the asset for the lender. On day one of the contract, legal ownership of the asset passes to the customer.

**(e) Loan:**
The lender does not purchase the asset, but advances a sum of money to the customer (or sometimes to the vendor of the asset on behalf of the customer) for the customer to do so. The customer therefore takes legal title to the goods directly from the

vendor. The contractual repayments by the customers recoup the full loan advance for the lender.

All financial products as described above are in scope of the Wwft. As set out in the 'Nota naar aanleiding van Verslag'[5] the Wwft does not make a distinction between the various services a Financial Institution can offer. This means that when a Financial Institution is subject to the Wwft, Operating Lease is also in scope of the Wwft.

6.5 The contracts for the financial instruments may contain ancillary features, such as the provision of services, or provision for extension or early termination, but the basic legal characteristics should not change.

## Customer Due Diligence

*Who is the customer from AML perspective?*

6.6 A natural person or legal entity with whom a customer relationship is established, or a transaction will be carried out. In the case of asset finance the 'end-user'of the asset, or any party with whom the financial institution enters into a customer, professional or commercial relationship that is connected to the professional activities such as vendors, dealers etc.

6.7 The identification requirements on which guidance is given in Part I, will apply to a banks' customer (i.e. parties with whom they have a contractual relationship).

6.8 The CDD measures carried out at the commencement of the customer relationship and the ongoing due diligence are very closely linked to anti-fraud measures. Banks must ensure that they coordinate both the identification and ongoing customer due diligence processes for customers in order to provide as strong a gatekeeper control as possible.

6.9 Financial institutions must carry out risk-based CDD measures to gain a full understanding of the customer and their business before opening a facility. This should be at a level to provide identification and establish expected activity patterns of their

.....

[5] https://zoek.officielebekendmakingen.nl/kst-34808-6.html

customers and their activities to meet the requirements set out in Part I.

## The Money Laundering Risks in Asset Finance

6.10 The various specific features of Asset Finance can increase or decrease the risk of money-laundering/terrorist financing, and the key features are considered below:

- Repaying borrowed money over time, or paying lease rentals over a medium-term period, provides a very slow means of 'layering' the proceeds of crime. *Lower Risk.*

- The amount of credit obtainable is generally limited by the strength of the financial statements of the customer. In other words, layering a lot of money would only be possible for a financially strong business (which by implication would be registered for VAT, would undergo some accounting inspection, even if not subject to audit, etc). *Lower Risk.*

- Customer has to acquire a 'business asset';
  - Many business assets have little or no resale value, so present a poor opportunity for being realised for cash, even allowing for the 'costs' that money-launderers are prepared to tolerate. Industry jargon sometimes refers to such assets as 'soft assets', despite them often being 'tangible'. *Low Risk.*
  - Certain assets do have reliable resale values (for example – although not an exhaustive list - cars, motorhomes, commercial vehicles, 'yellow' plant, some machinery). Such assets should attract a greater CDD risk-score. Industry jargon sometimes refers to these as 'hard assets'. *Medium Risk*.
  - Luxury assets may be desirable to criminals in their own right (e.g. expensive cars); these should attract the highest CDD risk score. *Higher Risk.*

- Payment of Finance Agreement instalments:
  - By the customer via direct debit from a NL bank account. *Low Risk*.
  - By cash. Should be closely investigated and understood. The source of the funds in such instances

should be clearly established. *High Risk*.

- Overpayments should only be reimbursed to the customer named on the agreement. Any requirement to pay over monies to 'unrelated third parties' should attract consideration as potentially suspicious. *High Risk.*

6.11 Providers of Asset Finance should make specific risk assessment of the following:

- The suitability of the asset for the customer. Does it make sense for this customer to want to acquire that asset?

- The bona fides of the Vendor of the asset.
  - Is it a properly established business?
  - Does its location make sense given the customer's location?
  - Is the business related in any way to the Customer (e.g. common directors, same address, etc.)? If 'yes', then asset-sale-purchase may not be genuine, in which case:
    - Potential 'fund-raising'';
    - Possible money-laundering 'fraud'.
  - In the case of 'Sale and Leaseback', the Asset Finance provider should obtain the original underlying invoices from bona fide suppliers to customer, and confirm that the invoices have been paid by customer. Asset Finance provider should mark the original invoices as being financed by them, before returning them to the customer. This process helps assure the bona fides of the transaction, and avoids 'double financing' and handling the proceeds of crime.

6.12 Early termination of a finance agreement (i.e. just after its inception) presents the greatest opportunity for laundering money to money-launderers. Many early terminations (and notably 'upgrades') make commercial sense, but those that appear like a cash purchase dressed-up as a short-term finance agreement could be 'layering' and could provoke suspicion of money-laundering.

6.13 Loans, depending on how they are processed, may pose lower or higher risk of money laundering or terrorist financing:

- Where the lender pays the loan advance to a bona fide supplier in settlement of a bona fide invoice addressed to customer, the financial instrument presents a lower risk of money laundering and terrorist financing;
- Where the lender pays the loan advance directly to customer, and has no practical control of how customer uses the loan advance, then the potential risk of money laundering and terrorist financing increases.

6.14 With the exception of a few characteristics, the features of Asset Finance render it ‘low risk’ from a money-laundering and terrorist financing perspective. An Asset Finance provider that implements sensible credit policies and procedures will be likely to avoid the higher-risk features of Asset Finance.

# Chapter 7

# Private Equity

## Introduction

*Scope*

7.1 This chapter will provide guidance on the relationship between a bank and a private equity firm. In particular focusing on the following situations:

(i) The private equity firm as customer of the bank;

(ii) The bank has a customer relationship that contains a private equity firm in the ownership structure.

*Definition*

7.2 Private equity (for the purpose of this chapter) relates to:

- The marketing, raising and acceptance of moneys into private equity funds (usually from institutional investors);
- The investing of these funds by providing long term finance to a range of businesses, from early stage to large established companies. Usually the investee companies are unquoted but transactions include quoted companies from time to time (for example, public to private transactions);
- The management of these investments (often involving active board participation) and exercise of negotiated equity holder rights; and
- The subsequent realisation of the investment.

*Private equity parties*

7.3 In a private equity context there are several distinct groups that play a role in activities as mentioned under 7.2.

7.4 Investors in a private equity fund are mostly eligible counter parties/professional investors , such as insurance companies, pension funds, other financial services companies, charitable

organisations and some funds of funds.[6] There may also be a small number of high net worth individuals.

7.5 A private equity firm will set up, manage and advise limited partnerships. The investors will typically invest in such partnerships as limited partners.

7.6 Investee companies refers to the target company into which the funds are invested. This company will either be an existing legal entity or newly created.

7.7 Purchaser on exit refers to the buyer of an existing investment from a private equity firm. The realisation of a private equity transaction will typically be made either by means of listing, sale to a trade buyer, sale to existing management or a secondary sale to another private equity fund.

## Customer Due Diligence

7.8 A bank will commonly have a relationship with a private equity firm as a customer or encounter one in the ownership structure of a customer. In both cases the general guidance as set out in Chapter I with regard to CDD applies.
The process of establishing sufficient insight into the ownership structure and establishing the UBO may require additional effort due to the complexity as a result of investor funds. This is often a result of the split between ownership and effective control.

7.9 A bank should obtain sufficient information to determine whether;

- Any person qualifies as UBO amongst the group of investors, or,
- Any person who exercises control over the group of investors or the private equity firm.
- Senior managing officials of the private equity firm qualify as UBO in absence of the aforementioned.

7.10 Where a private equity firm or manager (of a fund of eligible counterparties/professional investors) is subject to supervision in the EU or an equivalent jurisdiction, the bank may consider, on a

[6] A multi manager investment – comprised of pooled investment funds, that invests in other types of funds.

risk-based approach, relying on a statement made by such a party regarding the UBOs.

7.11 Funds are often widely held and it is unlikely that there will in fact be any investor which is an UBO with an interest of more than 25% or effective control. Where such a natural person UBO is encountered, this person must be identified and risk-based measures taken to verify their identity.

7.12 Depending on the results of the risk evaluation, it may be appropriate to obtain documents (for example basic constitutional documents), or a combination of documents and representations, from the private equity firm.

## Money Laundering Risk

*Factors of increased and decreased ML risk*

7.13 The susceptibility of the private equity sector to money laundering is generally considered to be low. Based on the following factors:

- Regulation in an EU or equivalent jurisdiction;
- The investors group being comprised of eligible counterparties/professional investors;
- Investors in funds tend to have a long established relationship with a private equity firm, resulting in a usually well known investor base and a relatively constant source of funding;
- Transfer of interest in investment funds is only possible after due diligence by a fund manager and specific approval from a general manager.

7.14 The following will generally increase the risk of money laundering in a relationship with a private equity firm:

- Insufficient oversight and regulation in a non-equivalent jurisdiction;
- High net worth individuals and/or PEPs amongst the investor base;
- Unwillingness of the private equity firm to explain its due diligence procedures;
- Investment of the private equity firm in higher risk sectors.

# Chapter 8

# Corporate Finance

## Introduction

*General overview of the sector*

8.1 Corporate finance activities are associated with transactions in which capital is raised in order to create, develop, grow or acquire businesses:

- The issue of securities. These activities might be conducted with an issuer in respect to itself, or with a holder or owner of securities. Examples include: arranging an initial public offering (IPO), a sale of new shares, or a rights issue for a company, as well as making arrangements with owners of securities concerning the repurchase, exchange or redemption of those securities;
- The financing, structuring and management of a body corporate, partnership or other organisation. Examples include: advice about the restructuring of a business and its management, and advising on, or facilitating, financing operations including securitisations;
- Changes in the ownership of a business. Examples include: advising on mergers and acquisitions; takeovers, or working with a company to find a strategic investor;
- Business carried on by a bank for its own account where that business arises in the course of activities covered in the points above, including cases where the bank itself becomes a strategic investor in an enterprise.

## Money laundering risk in corporate finance

8.2 As with any financial service activity, corporate finance business can be used to launder money. The money laundering activity through corporate finance will not usually involve the placement stage of money laundering, as the transaction will involve funds

or assets already within the financial system. However, corporate finance could be involved in the layering or integration stages of money laundering. It could also involve the concealment, use and possession of criminal property and arrangements to do so, or terrorist funding.

8.3 The money laundering risks associated with corporate finance relate to the transfer of assets between parties, in exchange for cash or other assets. The assets can take the form of securities or other corporate instruments.

8.4 The challenge is to spot the money laundering behind the corporate finance transaction. Customer risk relates primarily to parties involved in corporate finance transaction including but not limited to PEPs (politically exposed persons). And secondly to the risk of violating International provisions, such as sanctions (i.e. circumvention, corruption, criminal activities or tax evasion).

### Assessment of risk elements in this sector

8.5 In order to combat financial crime, including money laundering and terrorist financing, it is important to obtain on a risk-based approach background knowledge about all the participants in a corporate finance transaction, and not just those who are customers.

8.6 In its assessment of the financial crime risk of a particular corporate finance transaction, a bank should use - where possible and appropriate - the information it has obtained as a result of the due diligence it normally undertakes in any corporate finance transaction. This may include, but not be limited to, firms assessing the probity of directors, shareholders, and any others with significant involvement in the customer's business and the corporate finance transaction.

8.7 The money laundering risks associated with corporate finance activity can be mitigated if a bank understands or obtains assurances from appropriate third parties and/or the customer as to the source and nature of the funds or assets involved in the transaction. Banks should consider, on a risk-based approach, the need to corroborate this information.

8.8 In addition, a bank should assess on a risk-based approach whether the financial performance of an enterprise is in line with

the nature and scale of its business, and whether the corporate finance services it seeks appear legitimate in the context of those activities. The outcome of this assessment should be consistent with the purpose and intended nature of the customer relationship.

8.9 Identification of business activity and industry type may include the identification of the turnover for past years, jurisdictions to and from which the money will flow, countries of the customer's main suppliers, main clients, main investments and list of countries where the customer generates majority of their income, and establishment of purpose and intended nature of the relationship should include but is not limited to rationale why the customer wishes to enter into the customer relationship with a bank, role of the enterprise in the respective customer group, nature of the activities of the enterprise, and product(s) / service(s) sought by the enterprise and explanation on their purpose.

## Who is the customer for CDD purposes?

*Issuer of securities*

8.10 Where a bank is facilitating the issue or offer of securities by an entity, that entity is the bank's customer.

8.11 In circumstances where vehicles are created for the purpose of issuing securities to investors e.g. Special Purpose Vehicles / Special Purpose Acquisition Company's (SPV, SPAC, respectively), the issuing SPV/SPAC will be considered the customer of the bank. These issuing SPVs or SPACs are often set up as "orphan" structures, typically owned by other entities which can either be discretionary in nature (e.g. Trusts) or not (e.g. TCSP). In such situations, the economic beneficiary (i.e. the issuer) may not have an obvious equitable interest in the SPV/SPAC. In which case additional information regarding the entity that has provided assets to the SPV and insight into how participation/investment into the SPV is structured is advised to understand the legitimate business purpose.

8.12 In transactions where assets are consolidated into or contributed to SPVs (e.g. certain notes or obligations), the bank should consider the source of funds of these assets and the identity of

those entities/individuals providing the assets for the SPV. Where the bank is unable to identify the source of this 3rd party, money laundering risk arises, for example inadequate identification of a potential sanctioned party.

*Purchaser of securities*

8.13 Purchasers of securities must be considered as customers for CDD purposes when:

- A direct relationship already exists between the bank and the purchaser;
- A direct pitch by the bank to a potential purchaser will create a customer relationship for the bank;
- Purchasers of securities may be deemed to be customers of the bank delivering the securities in settlement.

*Owners of securities*

8.14 Where a bank advises the owners of securities, in respect of the repurchase, exchange or redemption by an issuer of those securities, the owners will be customers of the bank for CDD purposes.

*Financing, structuring and management of a body corporate, partnership or other organisation*

8.15 The entity with which a bank is doing investment business, whether by way of advice provided to the entity, or through engaging in transactions on its behalf, will be a customer of the bank for CDD purposes.

8.16 The activity undertaken by a bank may entail the bank dealing in some way with other entities/parties on behalf of the customer entity, for example, through the sale of part of its customer's business to another entity or party. In these circumstances, the other entity or party whom the bank deals with on behalf of the customer will not also become the bank's customer as a result of the bank's contact with them during the sale. (For Securitisations transactions see paragraph 13.1)

*Changes in the ownership of a business*

8.17 The entity with which a bank is mandated to undertake investment business, whether by way of advice or through engaging in transactions, will be the customer of the bank for CDD purposes.

8.18 Other entities or parties affected by changes in ownership, for example a takeover or merger target, will not become the bank's customers, unless a bank provides advice or other investment business services to that entity or party. Similarly, an approach by a bank to a potential investor on behalf of a customer does not require the bank to treat the potential investor as its customer for CDD purposes, unless the bank provides advice or other investment business services to that investor.

*Business carried on by a bank for its own account*

8.19 Where a bank makes a principal investment in an entity, that entity will not be a customer of the bank. A principal investment in this context means an investment utilising the bank's capital and one that would not involve the bank entering into a customer relationship within the meaning of the Wwft. If, as well as making a principal investment in an entity, a bank enters into a customer relationship with that entity, for example, by providing investment services or financing to the entity, the bank must treat the entity as a customer. When a bank has determined that the investment is not subject to the requirements of the Wwft, it may nevertheless wish to consider, in a risk-based approach whether there are any money laundering implications in the investment it is making and may decide to apply appropriate due diligence measures.

8.20 A bank should establish at the outset whether it has a customer relationship with another regulated firm and, if so the identity of that firm has to be verified (see Part I).

## Customer due diligence

8.21 Corporate finance activity may be undertaken with a wide range of customers, but is predominantly carried on with listed and unlisted companies or their owners. The guidance contained in Part I, Chapter 2 indicates the customer due diligence procedures that should be followed in these cases. However,

the following is intended to amplify aspects of the Part I, Chapter 2 procedures, with particular reference to the business practices and money laundering risks inherent in a corporate finance relationship.

8.22 In addition to the standard due diligence requirements laid out in Part I, it is important to check the history of the customer and to carry out reputational checks about its business and representatives and shareholders before customer acceptance.

### Timing

8.23 In corporate finance transactions, when a mandate or an engagement letter is signed is generally considered the point at which the bank enters into a binding relationship with the customer. Note, it is common for a bank to begin discussions with a customer before a mandate or engagement letter has been signed, and a bank may put in place indemnity or conditional commitment arrangements prior to agreeing any express mandate or engagement Such arrangements may not constitute a binding customer relationship, as they are often designed to afford legal protections to the parties early on in a discussion and before the bank and its prospective customer(s) agree to a binding customer relationship.

8.24 A bank should determine when it is appropriate to undertake customer due diligence on a prospective customer and where applicable any UBOs. In all cases, however, the bank must ensure that it has completed appropriate customer due diligence before a binding customer relationship has been established.

8.25 Where, having completed customer due diligence, a mandate or engagement letter is not entered into until sometime after the commencement of the relationship, a bank is not required to obtain another form of evidence confirming the customer's agreement to the relationship with the bank prior to the signing of the mandate, provided it is satisfied that those individuals with whom it is dealing have authority to represent the customer.

### SPVs / SPAs Companies

8.26 Where SPV (Special Purpose Vehicle) / SPA (Special Purpose Adquisition) represents a legal entity or a group of entities that is

created specifically for a particular transaction, the identity, ownership structure and the purpose of the vehicle have to be established. Such vehicle is created by an originator or sponsoring bank to fulfil a temporary objective or a particular transaction in the interest of the sponsoring bank. The originator/collateral manager and purpose of the SPV can be identified via the prospectus or other transaction documents.

8.27 Depending on the purpose of the SPV, the originator can set up an SPV within its own ownership and control structure or as an 'off-balance sheet vehicle' (orphan company).

### Other evidence for customer due diligence

8.28 Where there is less transparency over the ownership of the customer, for example, where ownership or control is vested in other entities such as trusts or special purpose vehicles (SPV's), or less of an industry profile or less independent means of verification of the customer, a bank should consider how this affects the ML/TF risk presented. It will, in certain circumstances, be appropriate to conduct additional due diligence, over and above the bank's standard evidence  It should also know and understand any associations the customer may have with other jurisdictions. It may also consider whether it should verify the identity of the UBOs, in addition to the standard CDD measures described in Part I Chapter 2. A bank may, subject to application of its risk-based approach, use other forms of evidence to confirm these matters.  Consideration should be given as to whether or not the lack of transparency appears to be for reasonable business purposes.  Banks will need to assess overall risk in deciding whether the "alternative" evidence, which is not documentary evidence as specified in Part I Chapter 2, is sufficient to demonstrate ownership and the structure as represented by the customer.

### Subsequent activity for a customer

8.29 Some corporate finance activity involves a single transaction rather than an ongoing relationship with the customer.  Where the activity is limited to a particular transaction or activity, and the customer subsequently engages the bank for other activity, the bank should ensure that the information and customer due diligence it holds are up to date and accurate at the time the

subsequent activity is undertaken.

8.30 During the lifetime of the transaction, the CDD has to be up to date. The periods of the time driven review has to be set up according to the risk classification of the customer and event triggers have to include all relevant situations which might change the customer profile.

### Securitisation transactions

8.31 Securitisation is the process of creating new financial instruments by pooling and combining existing financial assets, which are then marketed to investors. A bank may be involved in these transactions in one of three main ways in the context of corporate finance business:

- As advisor and facilitator in relation to a customer securitising assets such as future receivables. The bank will be responsible for advising the customer about the transaction and for setting up the special purpose vehicle (SPV), which will issue the asset-backed instruments. The bank may also be a counterparty to the SPV in any transactions subsequently undertaken by the SPV;
- As the owner of assets which it wants to securitise;
- As counterparty to an SPV established by another bank for its own customer or for itself - that is, solely as a counterparty in a transaction originated by an unconnected party.

8.32 As a general rule, the bank should be more concerned with the identity of those who provide the assets for the SPV, as this is the key money laundering risk. Where an SPV does not have a customer relationship with the bank, and the bank demonstrates the link between the provider of the funds and the SPV, then said SPV is not subject to fulfilment of all CDD requirements.

8.33 Whether a purchaser of the instruments issued by the SPV will be treated as customers will depend upon the relationship the bank has with them. Purchasers of instruments issued by the SPV arranged by a bank will not be customers of the bank so long as their decision to purchase is based on offering documentation alone, or on advice they receive from another bank, who will have a customer relationship with them. However, as part of a bank's risk-based approach, and for reputational reasons, it may also feel it appropriate to undertake due diligence

on those who are purchasers of the instruments issued by the SPV.

8.34 In addition to verifying the identity of the customer in line with normal practice for the type of customer concerned, the bank should satisfy itself that the securitisation has a legitimate economic purpose. Where existing internal documents cannot be used for this purpose, background information, obtainable in many cases from rating agencies and prospectus, be used to record the purpose of the transaction and to assess the money laundering risk.

8.35 The bank needs to follow standard identity procedures and all CDD requirements with regard to the other customers of the bank to which it sells the new instruments issued by the SPV it has established. If the bank is dealing with a regulated agent acting on behalf of the SPV, it may place reliance on the CDD performed by the agent as described in Part I, Chapter 2.6. If the bank is dealing with an unregulated agent of the SPV, the bank must follow all CDD requirements for both the agent and the SPV.

### Monitoring

8.36 The money laundering risks for banks operating within the corporate finance sector can be mitigated by the implementation of appropriate, documented, monitoring procedures.

8.37 Monitoring of corporate finance activity will generally, due to the relationship-based, rather than transaction-based (in the wholesale markets sense), nature of corporate finance, be undertaken by the staff engaged in the activity, rather than through the use of electronic systems.

8.38 The essence of monitoring corporate finance activity involves understanding the rationale for the customer undertaking the transaction or activity, documenting the intended use of proceeds, so that the staff can make a professional judgment on whether the monitored transactions is logical and appropriate. The bank should also update this periodically, to ensure that the logical and appropriateness of the transactions can always be determined.

8.39 The bank will have ongoing relationships with many of its customers where it must ensure that the documents, data or

information held are kept up to date. Where, as is likely in some cases with corporate finance activities, the customers may not have an ongoing relationship with the bank, it is important that the bank's procedures to deal with new business from these customers is clearly understood and practised by the relevant staff. It is a key element of any system that up to date customer information is available as it is on the basis of this information that the unusual is spotted, questions asked and judgements made about whether something is suspicious.

# Chapter 9

## Trade Finance

*Banks addressing the money laundering/terrorist financing risks in trade finance should also have regard to the guidance in Chapter 10: Correspondent Relationships.*

### Overview of the sector

9.1 'Trade Finance' is used to describe various operations, including the financing – usually but not exclusively by financial institutions - undertaken to facilitate trade or commerce, which generally involves the movement of goods and services between two points – it can therefore be domestic or international. The trade finance element may only be part of the overall financial component and may have multiple variations, e.g., a domestic trade finance transaction could support an international movement of goods, or on occasion only services may be involved (see paragraph 15.9: Funds transmission/payments). Such operations comprise a mix of money transmission instruments, default undertakings and provision of finance, which are described in more detail below. A glossary of trade finance terms used in this guidance is set out in Annex 9-I.

9.2 In the context of this guidance, the term 'Trade Finance' is used to refer to the financial component of an international trade transaction, i.e., managing the payment for goods and/or related services being imported or exported. Trade finance activities may include issuing letters of credit, standby letters of credit, bills for collection or guarantees. Trade Finance operations are often considered in a cross-border context but can also relate to domestic trade.

9.3 Past estimates suggest that approximately only a fifth of world trade is conducted by means of trade finance products and services; the rest is conducted on "Open Account" terms, whereby a 'clean' payment is made by the buyer of the goods or services direct to the seller, i.e., not requiring presentation of the supporting trade documentation to the banks through which the payment is effected. It follows that whenever credit and liquidity

are scarce or trust between the transacting parties has not been established, sellers in particular will be inclined to revert to Trade Finance.

9.4 In Open Account transactions, unlike transactions where trade finance instruments are used, the bank is only aware of the payment and will not be aware of the reason for the payment, unless the relevant details are included in the associated SWIFT messages. Banks will therefore be able to carry out sanctions screening only on the payment, with anti money laundering checks achieved to the extent practicable by its risk-based transaction monitoring. Where credit is being provided, however, the bank may have more information to enable it to understand the reasons for the transaction and the financial movements. Banks are not required to investigate commercial transactions outside their knowledge, although if documentation they see as part of the banking transaction gives rise to suspicion, they should submit a SAR to the local competent authorities .

9.5 The focus of this guidance is on those standard products used for the finance of the movement of goods or services across international boundaries. The products are:

- Documentary Letters of Credit (LCs),
- Documentary Bills for Collection (BCs)
- Guarantees.

Most of these standard products have trade related documents (invoices, transport documents etc) that are sent through financial institutions (FI's) and are examined by documentary checkers within the financial institution for consistency with the terms of the trade transaction. Such operations are illustrated (in simple terms) in Annex 9-II, and are described in more detail below.

.

9.6 These products are governed internationally by sets of rules of practice issued by of the International Chamber of Commerce (ICC). The ICC rules governing BCs are fundamentally different from the ICC rules governing LCs. The checks, which have to be made within limited timeframes by the financial institution (Collecting or Presenting bank, see below), on BCs are limited to determining that the documents received appear to be as listed in the collection instruction.

9.7 International trade finance transactions will usually involve financial institutions in different locations, acting in a variety of capacities. For the purpose of LCs these may include an Issuing Bank, an Advising Bank, Nominated Bank, Confirming Bank or Reimbursing Bank. For BCs there will be a Remitting, Collecting or Presenting Bank. The nature of the capacity in which a financial institution may be involved is important, as this will dictate the nature and level of information available to the financial institution in relation to the underlying exporter/importer, the nature of trade arrangements and transactions. The fragmented nature of this process, in which a particular financial institution may of necessity have access only to limited information about a transaction, means that it is not possible for any financial institution to devise hard coded rules or scenarios, or any patterning techniques in order to implement a meaningful transaction monitoring system for the whole transaction chain.

9.8 The main types of trade finance operations are described in more detail below. Whilst they are addressed separately, they are not necessarily mutually exclusive and these operations may be combined in relation to a single transaction, series of transactions or, on occasion, in relation to a particular project. In terms of assessing risk, it is important to understand the detailed workings of individual operations/financial instruments, rather than automatically assuming that they fit into a particular category simply because of the name that they may have been given.

9.9 **Funds Transmission/Payments**
Trade finance operations often involve transmission of funds where the payment is subject to presentation of document(s) and/or compliance with specified condition(s). Financing may on occasion be provided either specifically related to the instrument itself, or as part of a general line of credit.

9.10 **Default Undertakings**
As the term implies, such undertakings normally only involve payment if some form of default has occurred. Typical undertakings in this category are bonds, guarantees, indemnities and standby letters of credit. Provision of finance is less common than with funds transmission/payment instruments, but could also occur.

9.11 **Structured Financing**
This category comprises a variety of financing techniques, but

with the common aim of facilitating trade and commerce, where financing is the primary operation, with any associated Trade Finance instrument and/or undertaking being subsidiary. On occasion, such financing may be highly complex e.g., involving special purpose vehicles (SPVs). Finance may be provided against evidence of performance under a trade contract, often on a staged basis that represents progress in that contract.

## What are the financial crime risks in Trade Finance?

### *General*

9.12 A key risk around trade finance business is that seemingly legitimate transactions and associated documents can be constructed simply to justify the movement of funds between parties, or to show a paper trail for non-existent or fraudulent goods. In particular, the level and type of documentation received by a bank is dictated principally by the applicant or instructing party, and, because of the diversity of documentation, banks may not be expert in many types of the documents received as a result of trade finance business (although experienced trade finance staff should have a good understanding of the most commonly used types of document). Such a risk is probably greatest where the parties to an underlying commercial trade transaction are in league to disguise the true nature of a transaction. In such instances, methods used by criminals to transfer funds illegally range from over and under invoicing, to the presentation of false documents or spurious calls under default instruments. In more complex situations, for example where asset securitisation is used, trade receivables can be generated from fictitious parties or fabricated transactions (albeit the use of asset securitisation in trade finance is a very limited activity). The use of copy documents, particularly documents of title, should be discouraged, and should raise a due diligence query, except where the location of the original documents (of title) and the reasons for their absence is disclosed to and acceptable by the banks in the transaction. Banks should implement additional safeguards with respect to related party transactions, e.g. requiring further escalation and scrutiny, requesting documentary evidence to verify the authenticity, and understand the role of the related party(ies) in the transaction. A list of FATF's Red Flags Indicators is included in Annex 9-V.

9.13 A form of trade finance is generally used instead of clean payments and generic lending to provide additional protection for the commercial parties and independent and impartial comfort when parties require some level of performance and payment security or when documentation is required for other purposes e.g., to comply with Customs, other regulatory requirements, control of goods and/or possible financial institution requirements. The key money laundering/terrorism risks arise when such documentation is adapted to facilitate non-genuine transactions, normally involving movement of funds at some point. A third party documentary letter of credit ("3rd Party LC") is a product whereby the bank issues an authenticated undertaking that represents a commitment to pay a beneficiary a specified amount of money against documents presented that comply with the terms and conditions as specified. The key difference from a regular LC is that the 3rd party is named as the "ordering party" as per the instruction of an existing customer.

### Money laundering and terrorism financing risk

9.14 Trade finance is not considered to be an increased risk product in in relation to money laundering and terrorism financing in itself, but the international trade and the processes and systems that support it are vulnerable for abuse for the purpose of money laundering and terrorism financing when viewed in combination with the risks related to the customers involved in trade finance and their backgrounds, their business activities as well as the nature of the goods, and the countries involved in the trade transaction. Depending on this combination there may be situations where there are higher risks and additional scrutiny is required, taking also the counterparty of the customer involved in the transaction into consideration.

9.15 The Financial Action Task Force (FATF), regulators and others have identified misuse of the trade system as one of the methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the legitimate economy or use it to finance terrorism. FATF typologies' studies indicate that criminal organisations and terrorist groups exploit vulnerabilities in the international trade system to move value for illegal purposes. Cases identified included: illicit trafficking in narcotic drugs; illicit trafficking in stolen or other goods; corruption and bribery; fraud; counterfeiting/piracy of products; and smuggling. More

complicated schemes integrate these fraudulent practices into a complex web of transactions and movements of goods and money.

9.16 Given the nature of the business, there is little likelihood that trade finance will be used by money launderers in the placement stage of money laundering. However, trade finance can be used in the layering and integration stages of money laundering as the enormous volume of trade flows obscure individual transactions and the complexities associated with the use of multiple foreign exchange transactions and diverse trade financing arrangements permit the commingling of legitimate and illicit funds.

*Trade-based money laundering and terrorist financing*

9.17 FATF's June 2008 Best Practices document of Trade-Based Money Laundering[7] defined trade-based money laundering and terrorist financing (TBML/FT) as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities". Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail". Examples of how TBML/FT may be carried out include, but are not limited to: misrepresentation of the price, quantity or quality of imports or exports; and money laundering through fictitious trade activities and/or through front companies. The study concludes that "trade-based money laundering represents an important channel of criminal activity and, given the growth in world trade, an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive". The term 'trade transactions' as used by the FATF is wider than the trade transactions described in this sectoral guidance.

9.18 FATF's June 2006[8] study notes that the basic techniques of trade-based money laundering include:

.....

[7] https://www.fatfgafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

[8] https://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

- **Over Invoicing:** by misrepresenting the price of the goods in the invoice and other documentation (stating it at above the true value) the seller gains excess value as a result of the payment[9].
- **Under invoicing:** by misrepresenting the price of the goods in the invoice and other documentation (stating it at below the true value) the buyer gains excess value when the payment is made.
- **Multiple invoicing:** by issuing more than one invoice for the same goods a seller can justify the receipt of multiple payments. This will be harder to detect if the colluding parties use more than one financial institution to facilitate the payments/transactions.
- **Short shipping:** the seller ships less than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to over invoicing
- **Over shipping:** the seller ships more than the invoiced quantity or quality of goods thereby misrepresenting the true value of goods in the documents. The effect is similar to under invoicing.
- **Deliberate obfuscation of the type of goods:** parties may structure a transaction in a way to avoid alerting any suspicion to financial institutions or to other third parties which become involved. This may simply involve omitting information from the relevant documentation or deliberately disguising or falsifying it. This activity may or may not involve a degree of collusion between the parties involved and may be for a variety of reasons or purposes.
- **Phantom Shipping:** no goods are shipped and all documentation is completely falsified.

9.19 Generally, these techniques rely upon collusion between the seller and buyer, since the intended outcome of the trade is to obtain value in excess of what would be expected from an arms' length transaction, or to move funds from point A to point B without being detected or accounted for by the authorities. The collusion may arise, for example, because the parties are controlled by the same persons, or because the parties are attempting to evade taxes on some part of the transaction. The

.....

A report by Global Financial Integrity showed there was an estimated average of $725billion to $810 billion per annum in illicit financial flows from Developing Countries between 2000 and 2009. Of these amounts, 55% was due to trade mispricing. See http://iff-update.gfip.org/

techniques could however also involve fraud by one party against another.

9.20 *Market pricing; m*aking a determination as to whether over-invoicing or under-invoicing (or any other circumstances where there is misrepresentation of value) may be involved cannot be based on the trade documents alone. Furthermore, it is not feasible to make such determinations on the basis of external data sources; most products are not traded in public markets and therefore there are no publicly available market prices.

Even in transactions involving regularly traded commodities, which are subject to publicly available market prices, banks generally are not in a position to make meaningful determinations about the legitimacy of unit pricing due to the lack of relevant business information, such as the terms of a business relationship, volume discounting, specific quality of the goods involved etc. Available prices may not reflect the agreed price used in any contract of sale or purchase and these details will not usually be available to the banks involved due to the competitive sensitivity of such information

9.21 However, there may be situations where unit pricing appears manifestly unusual. This means that even with a layman's knowledge the price can obviously not be correct. Manifestly unusual pricing may prompt appropriate enquiries to be made based on the bank's risk-based approach (RBA). In case price assessment results in an increased risk conclusion enhanced due diligence is required. As illustration, when manifestly unusual pricing is assumed, such enhanced due diligence may consist of assessment on:

- pricing of previous comparable transactions.
- available open sources.

9.22 Some countries require that for the importation of certain types of goods, independent inspection agents certify that the goods meet the specified quality standards and that the prices charged are appropriate. The buyer and seller may also agree to use inspection agents, who will issue a certificate confirming the quality and/or price. Trade Finance staff should understand the circumstances where inspection certificates are required.

*Sanctions/Proliferation financing*

9.23 These trade finance guidance assume compliance with applicable, national and regional sanctions and embargoes and with the Non-Proliferation of Weapons of Mass Destruction ("NPWMD") requirements of the United Nations ("UN")

9.24 There is at present no agreed definition of proliferation or proliferation financing. FATF's Working Group on Terrorist Financing and Money Laundering[10] has proposed the following definition of proliferation financing for the purposes of its work:

*[Proliferation financing is] the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or 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].*

9.25 Dual-use goods are items that have both commercial and military or proliferation applications. This can include goods that are components of a weapon, or those that would be used in the manufacture of a weapon (*e.g.,* certain machine tools that are used for repairing automobiles can also be used to manufacture certain component parts of missiles).

9.26 Dual-use goods destined for proliferation use are difficult to identify, even when detailed information on a particular good is available. Regardless of the amount of information provided for a particular good, highly specialised knowledge and experience is often needed to determine if a good may be used for proliferation. Dual-use items can be described in common terms with many uses – such as "pumps" – or in very specific terms with more specific proliferation uses – such as metals with certain characteristics. Further, many goods are only regarded as dual-use if they measure-up to very precise performance specifications.

9.27 Proliferation differs from money laundering in several respects. The fact that proliferators may derive funds from both criminal

.....

[10] Combating Proliferation Financing: A Status Report on Policy Development and Consultation - February 2010

[11] The definition of an act of proliferation financing need not involve knowledge. However, when considering the responsibilities of financial institutions or a possible criminal basis of proliferation financing, a subjective element will be indispensable.

activity and/or legitimately sourced funds means that transactions related to proliferation financing may not exhibit the same characteristics as conventional money laundering. Furthermore, the number of customers or transactions related to proliferation activities is likely to be markedly smaller than those involved in other types of criminal activity such as money-laundering.

9.28 There are a variety of United Nations (UN) and national and regional sanctions in place. These include:

- Country-based financial sanctions that target specific individuals and entities.
- Trade-based sanctions, e.g., embargos on the provision of certain goods, services or expertise to certain countries.
- Sectoral sanctions: a comprehensive set of sanctions introduced by the EU and the US aimed at certain industry sectors (financial services, energy, mining and defence) and prohibiting certain types of transactions primarily with a new debt/equity issuance nexus. The applications of such sanctions can be very complex in nature as all aspects of the transaction shall be considered in determination whether it might give rise to a breach. It should be noted, that entities designated within sectoral sanctions regimes are not subject to asset freeze.

In recent years there has also been a series of UN Security Council Resolutions which have, inter alia, introduced targeted financial sanctions and/or activity-based financial prohibitions in respect of certain countries which relate to the prevention of WMD proliferation. For further guidance, banks should refer to the DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act [12].

9.29 Compliance with the sanctions in force within jurisdictions is relevant to all the products and services offered by banks. Sanctions that require the embargo of certain goods and services have particular relevance in relation to the provision and facilitation of trade finance products.

9.30 A summary of the legal and regulatory obligations in relation to proliferation financing is set out in Annex 9-III.

[12] https://www.toezicht.dnb.nl/en/binaries/51-212353.pdf

9.31 The use of trade finance to breach sanctions and/or for the proliferation of weapons of mass destruction (WMD) could potentially take advantage of the complex and fragmented nature of existing global finance activity where multiple parties (in many cases with limited knowledge of one another) become involved in the handling of trade finance.

9.32 In June 2008, FATF published a Proliferation Financing Report[13] which assessed these risks.

9.33 In April 2010 the FATF published a February 2010 report from their Working Group on Terrorist Financing and Money Laundering '*Combating Proliferation Financing: A Status Report on Policy Development and Consultation'* which further analysed the risks and possible policy responses. Annex 9-IV reproduces that report's discussion of how various types of entity in the financial sector might become involved in proliferation activities.

## Assessing the trade-based financial crime risk

9.34 A bank's risk-based approach should be designed to ensure that it places an emphasis on deterring, detecting and disclosing in the areas of greatest perceived vulnerability, in order to counter to the extent practicable the above trade-based money laundering, terrorist financing and proliferation financing techniques.

Annex 9– VI of this Guidance document provides further information on this for banks.

### *Money laundering/terrorist financing*

9.35 The ability of a bank to assess the money laundering/terrorist financing risks posed by a particular transaction will depend on the amount of information that it has about that transaction and the parties to it. This will be determined by the bank's role in the Trade Finance operation. The amount of information available to a bank may vary depending on the size/type of the bank and the volume of business that it is handling. Where possible when assessing risk, banks may take into consideration the parties involved in the transaction and the countries where they are based, as well as the nature of any goods forming the basis of an

[13] http://www.fatf

underlying commercial transaction. Depending on the bank's role in the transaction the bank need to determine the level of customer due diligence and transaction due diligence.

9.36 One of the basic principles of trade finance is that the bank deals with documents and not with goods, services or performance to which the documents may relate. The bank does not get involved with the physical goods nor does it have the capability to do so. This overarching principle is the basis for defining what degree of scrutiny and understanding the bank can bring to the identification of unusual activity involving a trade finance transaction.

9.37 Apart from direct information, banks should have regard to public sources of information that are available at no or minimal direct cost, such as those available on the internet. For example, banks may validate bills of lading by reference to the websites of shipping lines, most of whom offer a free facility to track movements of containers. By using the unique container reference number, banks may be able to confirm that the container was loaded on a designated vessel and that vessel is undertaking the claimed voyage. The websites of many shipping lines provide details of the current and future voyages being undertaken by their ships and up to date information regarding their precise location. Banks would not be expected to investigate commercial transactions outside of their knowledge, although naturally if documentation they see as part of the banking transaction gives rise to suspicion, this should be reported.

9.38 When developing a risk-based strategy banks should consider, but not restrict their consideration to, factors such as the size of the transaction, nature of the transaction including goods and services involved, the parties involved in the transaction including geographical location of the parties as well as the customer's business mix.

9.39 As a rule of thumb the due diligence must be risk-based and sufficiently extensive for the bank to be able to form a reasonable belief in the legitimacy of the transaction and to be confident that it knows which risks it runs in order to manage those risks appropriately.

9.40 Banks need to be aware of trade-based money laundering techniques when developing their risk-based strategy and consider how best to mitigate the risks to themselves. The FATF

has listed some red flag indicators in its June 2006 report, which are reproduced in Annex 9-V.

9.41 In certain specific, highly structured transactions banks should exercise reasonable judgement and consider whether additional investigation should be undertaken. Such investigation may include determining whether over-invoicing or under-invoicing, or any other misrepresentation of value, may be involved, which cannot usually be based solely on the trade documentation alone. Price verification for financial crime control purposes is difficult for Banks. Banks generally are not in a position to make meaningful determinations about the legitimacy of unit pricing due to the lack of relevant business information, such as the terms of a business relationship, volume discounting or the specific quality of the goods involved. Further, many products are not traded in public markets and there are no publicly available market prices. Even where goods are publicly traded, the current prices may not reflect the agreed price used in any contract of sale or purchase and these details will not usually be available to the banks involved due to the competitive sensitivity of such information. However, in situations where unit pricing appears manifestly unusual banks should consider whether they have a suspicion of financial crime and whether they should accordingly submit a SAR to the local authorities.

*Proliferation financing*

9.42 Particular issues arise in relation to possible proliferation financing risks presented by customers and products, and these are discussed in Annex 9-VI.

*General*

9.43 It is recommended that banks create a risk policy (including the risk of financial crime abuse), controls and procedures appropriate to their business which they may be required to justify to their regulators.

9.44 Whilst it is recognised that banks will not be familiar with all types of documentation they see, they should pay particular attention to transactions which their own analysis and risk policy have identified as high risk and be on enquiry for anything unusual.

9.45 In addition to this Guidance, banks may also find some useful information in the private sector Wolfsberg Group guidance - Trade Finance Principles 2019 - (see http://www.wolfsbergprinciples.com/ and then go to Wolfsberg Publications - Wolfsberg Standards).

## Due Diligence Risk Assessment

### *General*

9.46 Customer Due Diligence is not only performed when establishing a business relationship, but is an ongoing process during the existence of the relationship. This includes (ongoing) monitoring of the activities and transactions of a customer, in this document referred to as transaction due diligence.

### *Customer Due Diligence*

9.47 With the partial exception of Collections (see below), the required due diligence must be undertaken on the customer who is the instructing party for the purpose of the transaction (see below). The circle of parties involved may be wider than the formal parties in a contract and may include those who act on behalf of the contractual party (representatives) and those on whose behalf the contractual party is acting (UBO). Depending on the risk involved, due diligence on other parties to the transaction, including other customers, should be undertaken where appropriate . Reference to Part I, Chapter 5 should be made as appropriate.

9.48 It should be noted that the instructing party will normally be an existing customer of the bank but, if not, due diligence must be undertaken on the instructing party before proceeding with the transaction. If the instructing party is not an existing customer, the bank should consider either:

- establish that there is another material party than the instructing party involved in the transaction and has duly passed all required customer due diligence procedures (refer to Part I Chapter 5), this may be a beneficiary party or an approved risk participant; where this is the case the bank may proceed;
- undertake customer due diligence on the instructing party before proceeding with the transaction (see Part I, Chapter 5).

*Transaction due diligence*

9.49 The ability to assess the money laundering or terrorism financing risks posed by a particular transaction will depend on the amount of information available. The bank should consider to assess the money laundering and terrorism financing risks of each single transaction relating to trade finance products prior to executing the transaction using all available information in documentation about the transaction in combination with the knowledge available within the bank. Documentation should be reviewed not only for compliance with terms, but also for anomalies or red flags that could indicate unusual or suspicious activity. The bank should pay attention to the following aspects, not exhaustive and take in to account the the Red Flags in Annex 9-V:

- the geographies in relation to which the customer trades, and the trading routes used;
- the goods traded in relation to the activities of the customer;
- the type and nature of parties with whom the customer does business (e.g. customers, suppliers, etc.);
- the role and location of agents and other third parties used by the customer or the material party in relation to the business (where this information is provided by the customer or the material party).

If as a result of the transaction due diligence a risk indicator is identified, the bank should consider performing an event driven review on the customer.

9.50 The outcome of the transaction due diligence may lead to the conclusion that instead of the instructing party, other parties should be considered as the bank's customer and should be treated accordingly.

9.51 The following list of instructing parties is not exhaustive and where necessary banks will need to decide in each case who the instructing party is (these enquiries are in addition to the standard due diligence undertaken by the bank as a condition of its account relationship):

- Import (Outward) Letters of Credit - the instructing party for the issuing bank is the **applicant**. Questions from the issuing bank that should arise during the initial due diligence process where LC facilities are required would be such as to establish from the applicant:

- The countries in relation to which the applicant trades, and the trading routes utilised
- The goods traded
- The type and nature of parties with whom the applicant does business (e.g., customers, suppliers, etc)
- The role and location of agents and other third parties used by the applicant in relation to the business (where this information is provided by the applicant)

- Export (Inward) Letters of Credit - the instructing party for the advising/confirming bank is the issuing bank.
  - The advising/confirming bank should undertake appropriate due diligence on the issuing bank (as set out in Part II, Chapter 16: Correspondent Relationships). The due diligence may support an ongoing relationship with the issuing bank which will be subject to a relevant risk-based review cycle. Due diligence on the issuing bank is not therefore required in relation to each subsequent transaction.
  - In other circumstances, the advising bank may not have an ongoing relationship with the issuing bank or reimbursing undertaking bank (IRU)and may simply act to process the transaction, in which case due diligence may be conducted on a different basis. As a minimum the advising bank will need to ensure that there is a means of authenticating any LC received from the issuing bank.
  - If the bank does not have an ongoing correspondent relationship with the issuing bank or the IRU bank and the bank simply acts as advising bank to process the transaction, the bank may proceed it the beneficiary is an existing customer of the bank and has duly passed all required customer due diligence procedures.
  - Although there is no requirement to carry out customer due diligence on the LC beneficiary, banks may decide to carry out some checks on the beneficiary using desk research e.g., check existence at Chamber of Commerce (or equivalent foreign registry), with on-line trade directories, professional advisers or availability of financial statements – subject to their own risk-based approach – to confirm the validity of the transaction if

the LC is issued by a bank in a country that is considered high risk and if the nature of the transaction (goods, shipment from/to, payment terms etc) warrants further investigation. Financial statements are a useful source of information, as they usually provide a description of the company's main activities, as well as giving information about the size of its financial operations.

- Import (outward) Collections - the instructing party is the customer/applicant.
    - Banks should carry out due diligence on the instructing party (exporter) who in many cases will be their customer, on whom they have already carried out due diligence.

- Export (inward) Collections - due diligence should be carried out on the drawee, who will normally be the importer or party acting on behalf of the importer. In most cases the drawee will be an existing customer of the bank receiving the collection, on whom standard due diligence for CDD purposes will already have been carried out. Depending on the nature of the transaction and whether it is consistent with the known trading activity of the customer and normal scale thereof, further enquiry may be prudent on a case by case basis.

- Bonds/Guarantees - the instructing party is the applicant/principle/account party and may be either a customer, correspondent bank or other third party.
    - This party must be a customer of the bank and have duly passed all customer due diligence procedures.
    - The bank should consider to establish that the requested guarantee and involved parties match with the nature, size an activities of the customer.

9.52 The distinction between customer due diligence and transaction due diligence is essential when dealing with transactions on behalf of third parties (e.g. issueing of a guarantee for a customer on behalf of one of its subsidiaries, the latter being a party to the guarantee and the one on whose behalf the guarantee will be issued). In case of the involvement of a third party in a trade transaction close attention should be paid to the relationship between the parties involved as part of the transaction due

diligence. The depth of the required transaction due diligence depends on the complexity of the structure. The outcome of the transaction due diligence may lead to the conclusion that instead of the instructing party, the third party should be considered as the customer and should be treated accordingly

If the outcome of the transaction due diligence leads to the conclusion that the risks involved are unacceptable for the bank this should always lead to an enhanced due diligence on the existing customer.

*Sanctions/proliferation financing – CDD and screening*

9.53 The ability of banks to implement *activity-based controls* against proliferation is limited, due to the lack of technical expertise of banks, the limited information available as a basis for such controls and banks' inability to examine whether such information is correct; the structural differences between money laundering and proliferation financing and the lack of clear financial patterns uniquely associated with proliferation financing; and the fragmented nature of the trade cycle, which limits each bank's visibility of the whole transaction.

9.54 *Targeted financial sanctions*[14] provide banks with proliferation-related information on which they can take action. Targeted financial sanctions are considered to be most effective when they are implemented globally *i.e.* by the UN, since a designated entity cannot as easily turn to third-country banks to evade sanctions.

9.55 Some jurisdictions have established their own capability to impose targeted financial sanctions on individuals and entities they deem involved in WMD proliferation, independent of sanctions agreed by the UN Security Council. The European Union (EU) has also adopted such sanctions based on specific legislation relating to certain countries of specific proliferation concern.

9.56 Targeted financial sanctions may also prompt a proliferation-related entity to conceal its involvement in a transaction. This may involve the use of unusual financial mechanisms which may

[14] For the purposes of this guidance, "targeted financial sanctions" includes not only asset freezing, but also prohibitions to prevent funds from being made available to "designated" or "listed" persons and entities.

arouse suspicion among legitimate exporters, or patterns of activity which may generate suspicion of money laundering or terrorism financing.

9.57 Where lists of certain natural or legal persons, entities or bodies (also known as 'targets') are available, banks should consider whether undertaking real-time screening of transactions is appropriate. Lists of targets in this context could potentially include both targets subject to targeted financial sanctions e.g., UNSCR 1737, under which transactions with named targets are prohibited; as well as (if such lists are made available), targets of proliferation concern, which have been identified as high-risk by competent authorities and which could be subject to enhanced due diligence and/or suspicious activity reporting. Banks should be careful not unintentionally to treat all types of lists as financial sanctions lists, thus running the risk of prohibiting business with these targets and jurisdictions altogether. Real-time screening against listed targets has limitations, however, and may be evaded if the listed target changes its name or operates through a non-listed front company.

9.58 Alternative approaches would be required to identify and prevent proliferation financing activity conducted by non-listed targets. These could include both manual systems – enhanced due diligence, increased monitoring, and enhanced frequency of relationship reviews – and automatic systems such as post-event monitoring of account activity.

9.59 Post event monitoring, using multiple risk indicators, may in any event have the potential to identify proliferation financing activity.

9.60 *Goods based screening*; evaluation of the goods involved in a transaction very often requires a large amount of technical knowledge only available to export controls experts and/or exporters. Goods lists pose a tremendous challenge even for export control enforcement and certainly a greater one for real time screening than entity lists. Furthermore, banks in general lack the expertise to discriminate between legitimate and proliferation-sensitive goods. Therefore, banks are not in a position to determine, at any stage in a trade transaction, whether an export license is required or whether counterparties to the trade have obtained a valid export license. The documentation required for preparing a trade financing arrangement rarely contains a detailed description of the product, much less

information as to whether there are any third-country licencing requirements attached to the product. Goods lists, in themselves, should not be used as a basis for transaction screening, as their limited effectiveness, and greater difficulty, make them an inefficient safeguard.

CDD and screening section should specify that banks are expected to perform sanctions screening both at the inception of the trade finance transaction and at the point of submission of the trade finance documents, as some of the transactional details, (e.g. vessels, ports of call etc), may not be known at trade inception and also there could be subsequent updates to the sanctions lists.

9.61 Where highly structured Trade Finance transactions are concerned, or where EDD is conducted as a matter of routine or in case sanctions regulations apply, it may be appropriate for the Banks involved to obtain appropriate assurances that export licencing requirements have been satisfied.

When enhanced due diligence is conducted it may be appropriate to obtain assurances whether export licensing requirements apply. It should be documented whether these requirements have been satisfied.

*Enhanced due diligence*

9.62 Where the nature of a transaction displays higher risk characteristics than normal business undertaken for the customer (instructing party), for example, the buyer falls into a higher risk category then the bank should consider undertaking additional due diligence in line with its risk policies. Some of the checks banks could undertake (not all of which may be applicable or available in each case) include:

- Make enquiries as appropriate into the ownership and background of the other parties to the transaction e.g., the beneficiary(ies), agents, shipping lines, taking further steps to verify information or the identity of key individuals as the case demands;
- Seek 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;

- Check the transaction against warning notices from external public sources, for example the ICC's International Maritime Bureau;
- Refer the transaction to external agencies specialising in search and validation services in respect of bills of lading, shipping services and commodity prices, for example the ICC Commercial Crime Services;
- Check details of the source of goods;
- Check public source information for prices of goods such as commodities – where the contract price seems manifestly unusual or is significantly different from the market [say 25%] then consider further investigation;
- Attend and record relationship meetings with the instructing party, visit them by arrangement;
- For export letters of credit, refer details to other Group resources on the ground in the country of origin, to seek corroboration.
- Checks into the verification of shipments after the UCP operation is over, drawn at random from a sample of transactions, across a cross section of the bank's trade finance customers. This may help to identify spurious transactions where buyers and sellers act in collusion.
- Where relevant, certificate of origin to establish the origin of commodities.

9.63 The enhanced due diligence should be designed to further understand the nature of the transaction, the related trade cycle for the goods involved, the appropriateness of the transaction structure, the legitimacy of the payment flows and what control mechanisms exist.

9.64 The nature of business and the anticipated transactions as described and disclosed in the initial due diligence stage may not necessarily suggest a higher risk category but if, during the course of any transaction any high risk factors become apparent, this may warrant additional due diligence. For example – although these may in some cases be used legitimately - where third party middlemen or traders use back to back or transferable LCs to conclude offshore deals, or where the buyer is itself a middleman or trader.

9.65 The bank must substantiate why it is comfortable to provide the product or service requested by the customer. If the customers explanation of a request for particular products or services is inconclusive or otherwise unacceptable and remains so after

enhanced due diligence, the bank must refuse the customer's request.

*Specific Trade products – structured financing*

*Forfaiting*

9.66 The diverse nature of forfaiting business is such that the exact nature of the transaction needs to be considered. For example, the need to ensure authenticity may lead to enquiries being made of the importer's management, and it may be necessary to examine the commercial parts of documents, dependent on the nature of the underlying commercial transaction.

9.67 In the primary Forfaiting, or origination, market, a bank will usually be dealing directly with an exporter, who will be its customer and on whom it should carry out due diligence in accordance with Part I, Chapter 5. In addition, as part of its risk-based approach, a bank, where appropriate, should scrutinise the other party to the underlying commercial transaction, as well as the transaction itself, to satisfy itself of the validity of the transaction. The amount and depth of scrutiny will depend on the bank's risk assessment of the customer and transaction.

9.68 In the secondary Forfaiting market, the bank's customer will be the person from whom it buys the evidence of debt. However if it holds a Forfait asset to maturity it will be receiving funds from the guarantor bank and thus it should as a matter of course perform due diligence on this entity as well. Using a risk-based approach, banks should also consider whether they should conduct some form of due diligence on the underlying parties to the transaction, as well as on the transaction itself. This will depend on a risk assessment of the countries and the types of customers or products and services involved. It may be necessary to examine documentation on the underlying commercial transaction. However, it should be borne in mind that the further away from the original transaction the purchaser of a Forfait asset is, the harder it will be to undertake meaningful due diligence.

*Structured Financing*

9.69 As stated above, structured finance transactions are diverse in nature. Due diligence should be undertaken on all relevant parties in accordance with the bank's own risk

policy/assessment, including, where relevant, certificate of origin to establish the origin of commodities (for example, crude oil).

## Monitoring

9.70 Banks should have regard to the general guidance set out in Part I, section 5.7 on monitoring and in Chapter 6, on reporting suspicious transactions, and requesting consent where appropriate. The depth and frequency of monitoring to be undertaken will be determined by a bank's risk analysis of the business and/or the parties involved. Banks should, however, implement such controls and procedures appropriate to their business, but in any event must comply with any applicable legal or regulatory requirements.

9.71 Banks may refer to sources of information that may be relevant to assessing the risk that particular goods may be 'dual-use', or otherwise subject to restrictions on their movement. For example, there are public resources (such as the EC's TARIC database) that can indicate which restrictions might apply to exports from the EU with specific tariff codes: it will show where trade in some types of good under that category might be licensable or prohibited. Exporters must already provide tariff codes to the customs authorities (who use them to calculate the tax levied on the trade), so should be able to provide them to their banks, insurers and their agents. These can be used to identify transactions that might present higher risk or require further due diligence checks, particularly in situations where the risks are perceived to be higher. For example, have issuing banks, applicants or beneficiaries of letters of credit, or freight companies and shipping lines moving the goods, been highlighted by national authorities as being of concern? (This information will often be recorded on commercially-available due diligence tools). Does the trade involve jurisdictions previously implicated in proliferation activity?

9.72 Techniques dependent on a bank's risk analysis/policy could range from random, after the event, monitoring to checking receivables in any form of securitisation transaction to seek to determine if they are legitimate.

9.73 In the automatic monitoring of transactions the drivers that flag 'unusual transactions' tend to be built around:

- payment values;
- volume of payments;
- countries of payment;
- originator/beneficiary names;

- patterns in relation to a country or entity name;
- volume of shipments (e.g., tonnes).

However, the exact configuration of monitoring systems will differ between banks.

9.74 Alerts generated from these automatic systems are usually subject to some type of human intervention. Therefore, the effective application of a risk-based approach to monitoring is only possible if based on intelligence-based risk indicators, such as geographical combinations or geographical patterns of high-risk payment flows.

9.75 Depending on the screening tool that it employs, a bank may be able to screen SWIFT messages for indications of prohibited or licensed goods, such as armaments.

9.76 The ability of a bank to detect suspicious activity will often be constrained. For instance, in the case of fragmented trade finance arrangements the availability of information will be a particularly limiting factor in enabling banks to understand who the ultimate buyer (or seller) of a product is, or what the ultimate end use of product may be. Whilst all banks are expected to have a form of financial transaction monitoring in place, the information presented to a bank will clearly vary according to its role in a particular transaction and the type of payment system used. For instance in the case of letters of credit, the bank will have some – albeit often limited - information on the underlying transaction if it is the issuing bank and less information if it is the advising bank. The extent to which available information will need to be verified will also vary depending on this role

### Staff awareness, training and alertness

9.77 The bank must train staff on how trade finance transactions may be used for ML/TF and in the bank's procedures for managing this risk. This training should be directed specifically at those staff directly involved in trade finance transactions, including those in relevant back office functions, and should be tailored around the specific risks that this type of business represents.

9.78 Trade Finance staff need regular training which may include how to perform an analysis of pricing for those goods where reliable and up-to-date pricing information can be obtained, how to identify where a unit price would be seen as manifestly

unusual and the escalation process that should be followed. The same applies to dual use goods. Staff should be aware of dual use goods issues, as well as the common types of goods which have a dual use and should attempt to identify dual use goods in transactions wherever possible. Trade Finance staff need to have a high level understanding of export licence regimes and of the importance of seeking evidence from relevant parties to the transaction that an export licence has been obtained for appropriate transactions.

9.79 The FATF's red flag indicators set out in Annex 9-V, although directed primarily at governmental agencies, nevertheless should be a useful aid to those devising banks' training programmes. In addition the several case studies set out in the study may also provide good training material.

# ANNEX 9-I Glossary of trade finance terms used in this guidance

*Trade-Based Money Laundering and terrorist financing.*The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities

*Bills of Exchange*. A signed written unconditional order by which one party (drawer or trade creditor) requires another party (drawee or trade debtor) to pay a specified sum to the drawer or a third party (payee or trade creditor) or order, on demand or at a fixed or determinable future time. In many European jurisdictions, transactions will be subject to the Geneva Conventions on Bills of Exchange 1932. Bills of Exchange can be payable at sight or at a future date, and if either accepted and/or avalised, represent a commitment by the accepting or Avalising party to pay funds, thus making them the primary obligor.

*Acceptances/Deferred Payment Undertakings*. Where the drawee of a bill of exchange signs the bill with or without the word "accepted" on it, the drawee becomes the acceptor and is responsible for payment on maturity. Where banks become the acceptor these are known as "bankers' acceptances" and are sometimes used to effect payment for merchandise sold in import-export transactions. Avalisation that occurs in forfaiting and some other transactions is similar to acceptance but does not have legal standing under English law. Banks may also agree to pay documents presented under a documentary credit payable at a future date that does not include a bill of exchange. In such instances the bank incurs a deferred payment undertaking.

Promissory Notes. These are a written promise committing the issuer to pay the payee or to order, (often a trade creditor) a specified sum either on demand or on a specified date in the future. (This is similar to a bill of exchange).

*Guarantees and Indemnities*. Sometimes called Bonds, these are issued when a contractual agreement between a buyer and a seller requires some form of financial security in the event that the seller fails to perform under the contract terms, and are normally issued against a backing "Counter Indemnity" in favour of the issuing bank.

There are many variations, but a common theme is that these are default instruments which are only triggered in the event of failure to perform under the underlying commercial contract.

*Documentary Credits*. Historically, these were one of the most commonly used instruments in Trade Finance transactions and although their usage has declined in recent years, particularly in intra-Western European trade, unfavourable credit conditions could reverse this trend, especially in developing markets (at least in the short term). They remain in extensive use in trade involving deep sea transport and in certain geographical areas e.g., South East Asia. In its simplest form a Documentary Credit is normally issued by a bank on behalf of a purchaser of merchandise or a recipient of services (a trade debtor), in favour of a beneficiary, usually the seller of the merchandise or provider of services (a trade creditor). The issuer (usually a bank) irrevocably promises to pay the seller/provider at sight, or at a future date if presented with documents which comply with the terms and conditions of the Documentary Credit. Effectively, the Documentary Credit substitutes the Issuing Bank's credit for that of the applicant subject to the terms and conditions being complied with. When a Documentary Credit is confirmed by another bank, the Confirming Bank adds its own undertaking as principal to that of the Issuing Bank i.e. the Confirming Bank becomes a primary obligor in its own right. There are many more complex variations than this simple example, but almost all Documentary Credits worldwide are issued and handled subject to the applicable International Chamber of Commerce (ICC) Uniform Customs & Practice for Documentary Credits in force (currently UCP 600).

*Collections*. A typical documentary collection involves documents forwarded by an exporter's bank to an importer's bank to be released in accordance with the accompanying instructions. These instructions could require release of documents against payment or acceptance of a bill of exchange. As with Documentary Credits, there are a number of possible variations and the term collection is also used in other contexts. However, Collections of the type described above are normally but not always handled subject to the applicable ICC Uniform Rules for Collections - URC in force (currently ICC Publication 522).

*Standby Letters of Credit*. Unlike Documentary Credits, Standby Letters of Credit are default instruments which are sometimes issued instead of a guarantee. They may be issued subject to the applicable

ICC rules in force, currently either UCP 600 or International Standby Practices (ISP 98), but may also contain specific exemption wording.

*Discounting*. A bank may discount a bill of exchange or a deferred payment undertaking, paying less than the face value of the bill/documents to the payee or trade creditor for the privilege of receiving the funds prior to the specified date. The trade debtor may not be informed of the sale and the trade creditor may continue to be responsible for collecting the debt on behalf of the discounter.

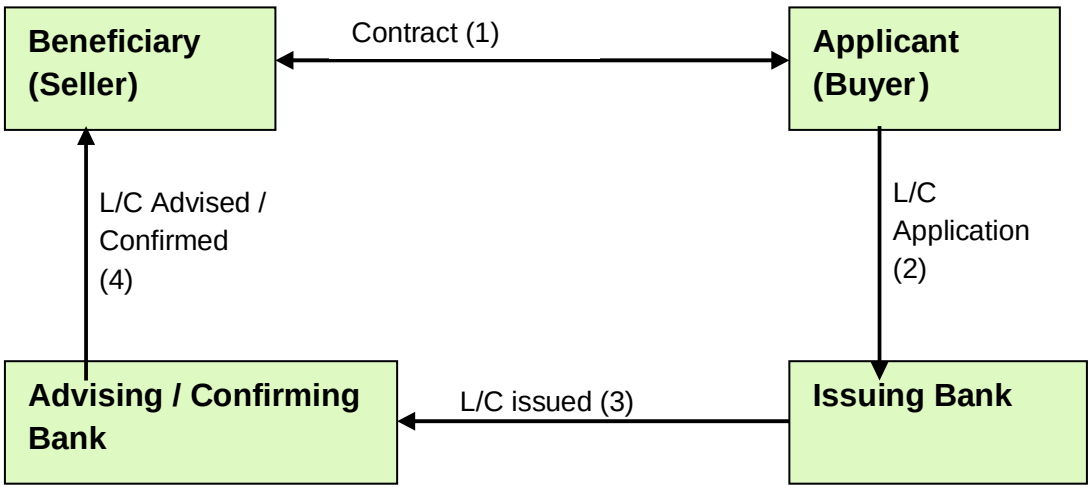
*Negotiation*. This term has a variety of meanings dependent on the jurisdiction/territory in which it is being used but for the purposes of UCP 600 means "the purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) and/or documents under a complying presentation, by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank".

*Forfaiting*. This is a financing mechanism traditionally designed for use by trade creditors who export goods. Forfaiting, however, may also involve the direct provision of finance to importers and the provision of working capital by credit institutions for the purposes of funding trade transactions in their countries. The trade creditor or exporter sells evidence of a debt, usually a promissory note issued by the importer or a bill of exchange accepted by the importer or proceeds due under a Letter of Credit such proceeds being assigned by the exporter. The sale is normally made without recourse to the trade creditor/exporter in which case the person buying the debt will usually require the importer's payment obligations to be guaranteed by a bank (avalised).

# ANNEX 9-II Process of trade finance products

The Process for a Confirmed Documentary Credit payable at sight at the counters of the nominated bank

**1.1** **Stage 1**




*Basic Documentary Credit Procedure*

The documentary credit procedure involves the step-by-step exchange of documents required by the credit19 for either cash or a contracted promise to pay at a later time. There are four basic groupings of steps in the procedure: (a) Issuance; (b) Amendment, if any; (c) Utilisation; and (d) Settlement. A simplified example follows:

*(a) Issuance*

Issuance describes the process of the buyer's applying for and the issuing bank opening a documentary credit and the issuing bank's formal notification of the seller either directly or through an advising bank.

(1) Contract – The Buyer and Seller agree on the terms of sale: (a) specifying a documentary credit as the means of payment, (b) naming an advising bank (usually the Seller's bank), and (c) listing required documents. The naming of an Advising Bank may be done by the buyer or may be chosen by the issuing bank based on its correspondent network.

(2) Issue Credit – The Buyer applies to his bank (Issuing Bank) and the issuing bank opens a documentary credit naming the Seller as beneficiary based on specific terms and conditions that are listed in the credit.

(3) Documentary Credit – The Issuing Bank sends the documentary credit either directly or through an advising bank named in the credit. An advising bank may act as a bank nominated to pay or negotiate (nominated bank) under the credit or act as a confirming bank where it adds its undertaking to the credit in addition to that of the issuing bank. Only in those cases where an advising bank is not nominated to negotiate or confirm the credit is the role of that bank simply an advising bank.

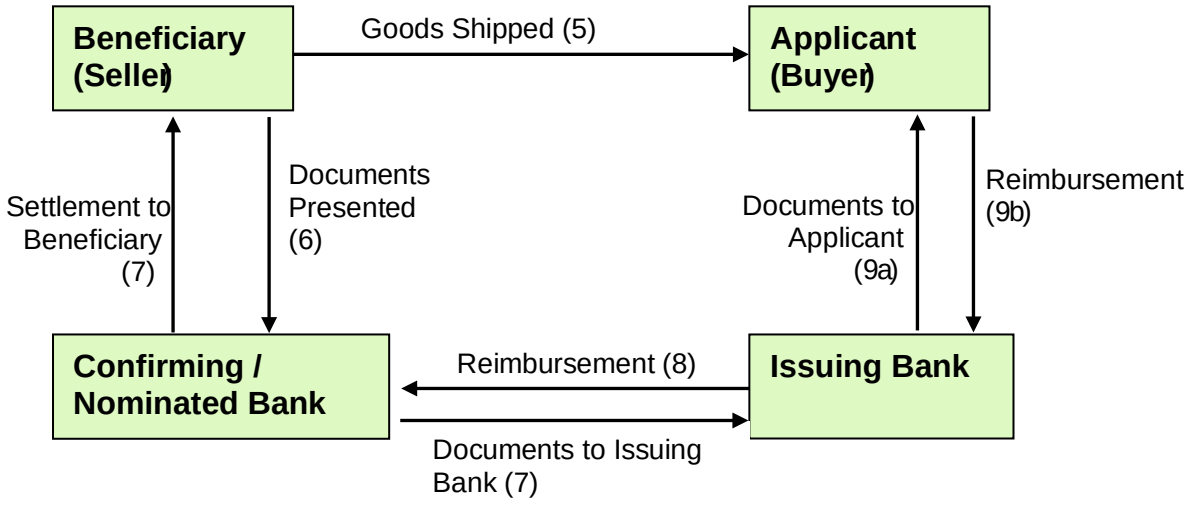
(4) Credit Advice - The advising, nominating or confirming bank informs (advises) the seller of the documentary credit. *(b) Amendment*
Amendment describes the process whereby the terms and conditions of a documentary credit may be modified after the credit has been issued.

When the seller receives the documentary credit, it may disagree with the terms and conditions (*e.g.* the transaction price listed in the credit may be lower than the originally agreed upon price) or may be unable to meet specific requirements of the credit (*e.g.* the time may be too short to effect shipment).

If the seller wants to amend the terms prior to transacting, the seller can request these from the buyer. It is at the discretion of the buyer to adopt the proposed amendments and request an amendment to be issued by the issuing bank. An amended letter of credit would be issued by the issuing bank to the seller through the same channel as the original documentary letter of credit.

Amendments to a letter of credit require the agreement of the issuing bank, confirming bank (if any), and the beneficiary to become effective.

**1.2** **Stage 2**



*(c) Utilisation*

Utilisation describes the procedure for the seller's shipping of the goods, the transfer of documents from the seller to the buyer through the banks (presentation), and the transfer of the payment from the buyer to the seller through the banks (settlement). For example:

(5) Seller ships goods – The seller (beneficiary) ships the goods to the buyer and obtains the documents required by the letter of credit.

(6) Seller presents documents to Advising or Confirming Bank or directly to the Issuing Bank – The seller prepares and presents a document package to his bank (the advising or confirming bank) consisting of (a) the transport document if required by the credit, and (b) other documents (*e.g.* commercial invoice, insurance document, certificate of origin, inspection certificate, etc.) as required by the documentary credit.

(7) Nominated or Confirming Bank reviews documents and pays Seller - The nominating or confirming bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit and (b) pays the seller (based upon the terms of the credit) which may mean that payment does not occur until after (5). An advising bank does not normally examine the documents, but simply forwards them on to the confirming or issuing bank for their examination.

(8) Advising, Nominated or Confirming Bank transfers documents to Issuing Bank – The Advising, Nominated or Confirming bank sends the documentation by mail or courier to the issuing bank.

(9) Issuing Bank reviews documents and reimburses the Nominated or Confirming Bank or makes payment to the beneficiary through the Advising Bank – The Issuing Bank (a) reviews the documents making certain the documents are in conformity with the terms of the credit, under advice to the Buyer that the documents have arrived, and (b) pays the beneficiary through the advising bank or reimburses the nominated or confirming bank (based upon the terms of the credit) and,

(10) Buyer reimburses the Issuing Bank – The Buyer immediately reimburses the amount paid by the issuing bank or is granted a credit by the issuing bank allowing it to reimburse the issuing bank at a later date.

(11) Buyer receives documents and access to goods – The Issuing Bank sends the documents by mail or courier to the buyer who then takes possession of the shipment.

*(d) Settlement*

The form of payment is specified in the original credit, and must therefore be accepted by the seller. The following are common settlement methods:

- The Sight Credit (Settlement by Payment) – In a sight credit, the value of the credit is available to the exporter as soon as the terms and conditions of the credit have been met (as soon as the prescribed document package has been presented to and checked by the issuing, nominated or confirming bank and found to be conforming to the terms and conditions of the credit) or once the advising bank has received the funds from the issuing bank (unconfirmed). Payment may be effected directly by the nominated bank or confirming bank upon their examination of the documents and they are reimbursed for that payment by the issuing bank.

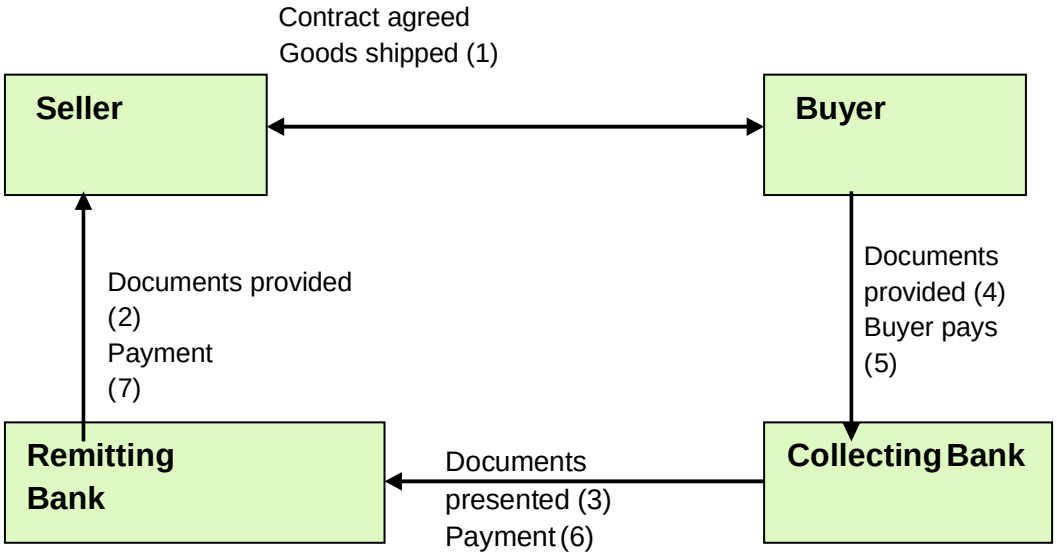
- The Usance Credit (Settlement by Acceptance) – In a Usance Credit, the beneficiary presents the required document package to the bank along with a time draft drawn on the issuing, nominated or confirming bank, or a third bank for the value of the credit. Once the documents have been found to be in order, the draft is accepted by the bank upon which it is drawn (the draft is now called an acceptance) and it may be returned to the seller who holds it until maturity.

- The Deferred Payment Credit - In a deferred payment credit the issuing bank and/or the nominated or confirming bank accepts the documents and pays the beneficiary after a set period of time. The issuing, nominated or confirming bank makes the payment at the specified time, when the terms and conditions of the credit have been met.

- Negotiation is the term used where a bank other than the issuing bank agrees to advance funds or discount drafts to the exporter before the issuing bank has paid. Discounting an accepted draft has the same effect.

A letter of credit will normally require the presentation of several documents including a Draft, Commercial Invoice, Transport Document, Insurance Document, Certificates of Origin and Inspection, Packing and Weight Lists.

## 1.3 The Documentary Collection Process




The documentary collection procedure involves the step-by-step exchange of documents giving title to goods for either cash or a contracted promise to pay at a later time.

Contract for the purchase and sale of goods – The Buyer and Seller agree on the terms of sale of goods: (a) specifying a documentary collection as the means of payment, (b) naming a Collecting Bank (usually the buyer's bank), and (c) listing required documents.

(1) Seller ships the goods – The Seller ships the goods to the Buyer and obtains a transport document from the shipping firm/agent. Various types of transport documents (which may or may not be negotiable) are used in international trade and only where required by the underlying transaction is a negotiable document used.

(2) Seller presents documents to Remitting Bank – The Seller prepares and presents a document package to his bank (the Remitting Bank) consisting of: (a) a collection order specifying the terms and conditions under which the bank is to hand over documents to the Buyer and receive payment, and (b) other documents (*e.g.* transport document, insurance document, certificate of origin, inspection certificate, etc.) as required by the buyer.

(3) Remitting Bank sends documents to Collecting Bank – The Remitting Bank sends the documentation package by mail or by courier to the Collecting Bank in the Buyer's country with instructions to present them to the Buyer and collect payment.

(4) The Collecting Bank reviews and provides documents to Buyer – The Collecting Bank (a) reviews the documents making sure they appear to be as

described in the collection order, (b) notifies the Buyer about the terms and conditions of the collection order, and (c) releases the documents once the payment or acceptance conditions have been met. Acceptances under documentary collections are known as “Trade Acceptances” which, when accepted (by the Buyer), only carry the obligation of the buyer as opposed to a “Bankers Acceptance’ commonly used under a letter of credit which carries the obligation of a bank.

(5) Buyer provides payment to Collecting Bank – The Buyer (a) makes a cash payment, or if the collection order allows, signs an acceptance (promise of the Buyer to pay at a future date) and (b) receives the documents and takes possession of the shipment.

(6) Collecting Bank provides payment to Remitting Bank – The Collecting Bank pays the Remitting Bank either with an immediate payment or, at the maturity date of the accepted bill of exchange if it receives payment from the Buyer.

The Remitting Bank pays the Seller.

# ANNEX 9-III Proliferation financing – the relevant legal and regulatory obligations

1. The system of international and national counter-proliferation controls includes a framework of treaties and United Nations (UN) Resolutions, which 'universalised' export controls that were previously implemented mainly on a voluntary and national basis. UN Security Council Resolutions decide also that all States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall; establish, develop, review and maintain controls on providing funds and services related to such export and trans-shipment such as financing.

*General obligations: export controls versus financial controls*

2. The general obligation on member states is to prevent the activities outlined above. Although UN resolutions primarily require implementation of export controls and do not specifically require states to establish an asset freezing regime, some jurisdictions have implemented national targeted financial sanctions as a route to meet finance-related obligations under the appropriate UN resolutions.

3. Export controls are the primary counter-proliferation safeguard because:

   - International regimes determine the nature of controlled goods - including *dual-use goods*
   - Controlled goods require export licences from national authorities
   - Licences are issued for specific end-users

4. The FATF has studied the specificities and functioning of export controls and the characteristics of international finance. It concluded that financial measures can supplement, but are not a substitute for effective export controls. Export controls are focused on preventing the illegal transfer of proliferation-sensitive goods and may affect financial activity as a secondary effect. Financial measures can reinforce export controls by addressing aspects of an illegal transfer of proliferation-sensitive goods that take place outside the jurisdiction of the country where the illegal export has occurred, such as the financial activities of the associated front company or end-user located in a second jurisdiction.

*Obligations in relation to financial controls*

*UNSCR*

6. UN Security Council resolutions are addressed to member states, requiring them to take specific actions as regards the subject matter. They therefore do

not in themselves directly impose obligations on banks. Member states are required to introduce domestic controls to prevent proliferation and specifically to take actions in relation to sanctioned states.

# ANNEX 9-IV Witting and unwitting actors

**[EXTRACT FROM FATF FEBRUARY 2010 WORKING GROUP REPORT]**

Proliferators abuse typical trade structures to facilitate their activities, which include supporters, financiers, logistical support, front companies, assets, shippers and facilitators. Entities that are knowingly engaged in proliferation, such as a front company, may also be involved in legitimate business. Other actors used by a network may knowingly support proliferation, be “wilfully blind” that they are being used for illicit purposes, or are truly unwitting actors. When an entity is engaged in both legitimate and illicit trade it may be less likely for financial institutions to suspect illegal activity.

*Front and Other Companies*

In individual cases, proliferation networks have employed companies to conceal the true end-use or end-user of traded goods. Most front companies are sensitive to public exposure and disruption of legitimate activities.

Front companies established by proliferators conduct transactions similar to those of companies engaged in legitimate business. Front companies used by proliferators may be similar to those established by money launderers. As is the practice of other criminal organisations, proliferators create companies for a seemingly legitimate commercial purpose and commingle illegal funds with funds generated by legal commercial activity. In some cases, front companies established by proliferators do not engage in any legal activity at all. Front companies may use fraudulent accounting practices and establish various offshore entities in jurisdictions with lax controls to disguise illegal operations. Proliferators are also known to change the names of front companies, or to use multiple names for the same front company, to prevent the detection of the companies’ association with proliferation – or other illicit activity.

Front companies used by proliferators are often located in a major trading hub of a foreign jurisdiction with lax export controls, but may also be found in jurisdictions with more established controls. They can be shell corporations with a fictitious business and physical location or can have normal commercial and industrial operations.

Front companies can arrange shipping services, routing or re-routing goods acquired by the importer or its intermediary. The same and/or additional companies

can also be located in jurisdictions with weak financial controls, enabling related financial transactions to settle the underlying trade without detection.

In exceptional cases, front companies may seek complicity within a particular jurisdiction's government for signoff by national authorities, by production of false cargo manifests to misdirect customs, law enforcement, and intelligence as to the true nature of the goods being exported and their end-use.

*Brokers*

Brokers are involved in the negotiation or arrangement of transactions that may involve the transfer of items (often between third countries) or who buy, sell or arrange the transfer of such items that are in their ownership. In addition they may also become involved in ancillary activities that facilitate the movement of items such as, but not limited to: *i)* providing insurance; *ii)* marketing; *iii)* financing; and *iv)* transportation / logistics. Illicit brokers illegally participate in proliferation by circumventing existing controls and obfuscating trade activities.

Brokers used by proliferation networks are often individuals relying on simple commercial structures, who are very mobile (financially and geographically) so that they can operate from any jurisdiction.

*Other Intermediaries*

Intermediaries may include companies and individuals that purchase or sell sensitive goods for further manufacture or redistribution. Intermediaries may have a particular knowledge of a jurisdiction's commercial infrastructure. Intermediaries that are knowingly engaged in proliferation will use this knowledge to exploit vulnerabilities in export control systems to the advantage of the proliferator.

*Financial Institutions*

Proliferation networks may use financial institutions to hold and transfer funds, settle trade and pay for services. Proliferation networks may use both private and public financial institutions for international transactions. States seeking to acquire WMDs may also use foreign branches and subsidiaries of stateowned banks for proliferation finance-related activities, giving these institutions the responsibility of managing funds and making and receiving payments associated with proliferation-related procurement or other transactions. These subsidiaries may be engaged in both legitimate and illegitimate transactions.

# ANNEX 9-V Red Flag Indicators

*FATF's Trade-Based Money Laundering "Red Flag" Indicators*

The respondents to the FATF project team's questionnaire reported a number of red flag indicators that are routinely used to identify trade-based money laundering activities. These include situations in which:

- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities.
- The type of commodity being shipped is designated as "high risk" for money laundering.*
- The type of commodity being shipped appears inconsistent with the exporter's or importer's regular business activities.
- The shipment does not make economic sense.**
- The commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities.
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason.
- The method of payment appears inconsistent with the risk characteristics of the transaction***
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.
- The transaction involves the use of repeatedly amended or frequently extended letters of credit; and
- The transaction involves the use of front (or shell) companies.

[Customs agencies make use of more targeted information that relates to specific exporting, importing or shipping companies. In addition, red flag indicators that are used to detect other methods of money laundering could be useful in identifying potential trade-based money laundering cases.]

* For example, high-value, low volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.
** For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.
*** For example, the use of an advance payment for a shipment from a new supplier in a high-risk country.

In addition to the FATF Guidance, banks may also find some useful information in the public and private sector e.g. Wolfsberg Group guidance - Trade Finance Principles 2019, or guidance from (local) regulators.

# ANNEX 9-VI Proliferation financing – Risk assessment of customers and products

1. The purpose of a risk-based approach is not the elimination of risk but rather that banks involved in high risk activity understand the risks they face and have the appropriate policies, procedures and processes in place to manage such risk. Equally, even reasonably applied controls will not identify and detect all instances of proliferation.

2. It would be impractical for banks to be expected to develop a dedicated risk-assessment framework for assessing proliferation financing risks alone. It would be more proportionate to include proliferation considerations alongside the wider determination of risks factors. Moreover, established mechanisms to conduct risk assessment and to identify suspicious activity of wider criminal activity are, in many cases, likely to be applicable to proliferation considerations.

3. The application of a risk-based approach to proliferation financing has both similarities to, and differences from, money laundering. They both require a process for identifying and assessing risk, but the characteristics of proliferation financing – including the limited availability of accessible information to determine risk – result in a more restricted scope for the application of risk-based measures. In acknowledgement of such limitations this guidance seeks to identify potential areas where risk-based decisions could be applied in the area of proliferation financing.

4. Clearly, in some circumstances a risk-based approach will not apply, will be limited, or will be determined by the parameters set by international obligations, national law or regulation. Where particular individuals, organisations or countries are subject to proliferation sanctions, the obligations on banks to comply with certain actions are determined exclusively by national authorities and are therefore not a function of risk. A risk-based approach may, however, be appropriate for the purpose of identifying evasion of sanctions, for example, by directing resources to those areas identified as higher risk.

5. The inclusion of proliferation financing within current risk assessment practices should be proportionate to the overall proliferation risk associated with the activities undertaken by the bank. For example, a bank operating internationally and/or with an international customer base will generally be expected to assess a wider range of risks, including proliferation, than a smaller, domesticallyfocused one.

6. In the application of a risk-based approach, measures and controls implemented by banks may often address more than one identified risk, and it is not necessary that a bank introduce specific controls for each risk. For instance, risks associated with proliferation financing are likely to sit alongside other country, customer and product risks. Additional information that may be useful could include further information on the parties to a transaction, source of funds, beneficial ownership of the counterparty and purpose of the transactions or payment.

*Country/geographic risk*

7. The most immediate indicator in determining risk will be whether a country is subject to a relevant UN sanction; in these instances some element of mandatory legal obligation will be present, along with risks related to sanctions evasion by sanctioned entities, and proliferation financing by unsanctioned entities. Depending on the extent of risk assessment and business conducted, other factors that may be considered could include:

   • Countries with weak or non-existent export controls (the FATF Proliferation Financing report noted that only 80 jurisdictions have any exports controls related to WMD). Individual country compliance with export control obligations are not, however, currently published. In the absence of such information, banks will not be in a position to make an informed assessment and therefore will not be in a position to utilise this indicator. If, however, such information became forthcoming – either at an international or individual government level – it could provide an additional factor that could potentially inform country risk assessment.

*Customer risk*

8. Any assessment of the risks that a customer may pose will be underpinned by customer take-on procedures and developed further by ongoing monitoring. Specific categories of customer whose activities may indicate a higher proliferation financing risk could include:
   - Those on national lists concerning high-risk entities.
   - Whether the customer is a military or research body connected with a high-risk jurisdiction of proliferation concern.
   - Whether the customer is involved in the supply, purchase or sale of dual-use and sensitive goods. Banks rely on export control regimes and customs authorities to police the activities of exporters who are their customers. Among others, export control authorities and customs authorities ensure that licensing requirements for dual-use goods have been met. Therefore, the fact that a customer is involved in the supply, purchase or sale of dual-use goods is, of itself, not an indicator for a bank; this would result in a disproportionately large number of trading companies falling into this category. However, a wide range of industrial items and materials can assist WMD programmes and would-be proliferators. The most critical items normally appear on national strategic export control lists, although screening against controlled goods lists is not a practical solution for banks. The involvement in the supply, purchase or sale of dual-use goods may therefore be of some relevance if other risk factors have first been identified.

9. Mitigating factors should also be considered, for example whether the customer is itself aware of proliferation risks and has systems and processes to ensure its compliance with export control obligations.

*Transactions risk*

10. In determining whether the transaction presents an elevated risk, a number of factors should be considered:
    - Specific nature of the underlying transaction and whether it contains a valid and apparent commercial rationale
    - Terms of the underlying agreement
    - Relationship nature between the bank, customer and any potential 3rd party
    - A number of participants involved and consideration of potential fragmentation and complexity
    - Involvement of manual processing/screening of various paper instruments
    - Whether a transaction is conducted on an open account or credit instrument basis

*Delivery channels risk*

11. Customer relationship commenced without a face to face meeting may present a higher financial crime risk than a relationship commenced following a customer meeting. The risks could include:
    - Whether the customer legally exists i.e.shell or front company
    - Whether they operate from the stated location
    - Whether the nature of the business activity is as stated
    - Whether the size of the customer is as stated
    - Whether the representatives are the persons who own or control the customer
    - Any other information provided by the customer does not match information which could be obtained by a physical meeting at the place of business

*Product and Service Risks*

12. Determining the risk of products and services may include a consideration of factors such as:
    - Delivery of services to certain entities Project financing of sensitive industries in high-risk jurisdictions.
    - Trade finance services and transactions involving high-risk jurisdictions.

13. As is the case with anti-money laundering, any assessment of risk will need to take account of a number of variables specific to a particular customer or transaction. This will include duration of relationship, purpose of relationship and overall transparency of relationship and/or corporate structure. It would be disproportionate to assess a stable, known customer who has been identified as involved in the supply, purchase or sale of dual-use and sensitive goods as either moderate or high-risk for that reason alone. However, the overall assessment of risk may increase with the presence of other factors i.e., delivering high volumes of dual-use or sensitive goods to a high-risk country/complicated corporate structures/the type and nature of principal parties engaged in the transaction.

Consideration of these risks, including customer-specific information, and mitigating factors, will enable a bank to reach a graduated understanding of the degree of proliferation finance risk a particular customer poses.

14. Interpretation of “dual-use” requires a degree of technical knowledge that letter of credit document checkers cannot be expected to possess. In addition, the description of the goods may appear in the documents using a wording which does not allow the identification of such goods as “dual-use”. Regardless of the details in the information sources, however, without the necessary technical qualifications and knowledge across a wide range of products and goods, the ability of a bank to understand the varying applications of dual-use goods will be virtually impossible. It would be impracticable for banks to employ departments of specialists for this purpose.

15. Banks may nevertheless refer to sources of information that may be relevant to assessing the risk that particular goods may be ‘dual-use’, or otherwise subject to restrictions on their movement. For example, there are public resources (such as the EC's TARIC database) that can indicate which restrictions might apply to exports from the EU with specific tariff codes: it will show where trade in some types of good under that category might be licensable or prohibited. Exporters must already provide tariff codes to the customs authorities (who use them to calculate the tax levied on the trade), so should be able to provide them to their banks, insurers and their agents. These can be used to identify transactions that might present higher risk or require further due diligence checks, particularly in situations where the risks are perceived to be higher). For example, have issuing banks, applicants or beneficiaries of letters of credit, or freight companies and shipping lines moving the goods, been highlighted by national authorities as being of concern? (This information will often be recorded on commercially-available due diligence tools). Does the trade involve jurisdictions previously implicated in proliferation activity?

16. EU exporters seeking to send goods to countries subject to trade restrictions may also be in contact with relevant government authorities including customs to clarify whether their shipments will be affected. A bank financing trade with such countries may inquire whether such correspondence has been entered into, particularly if it appears that the goods in question may require an export licence.

# Chapter 10

# Correspondent Relationships

## Overview of the sector

10.1 Under the Wwft, all relationships with credit and financial institutions fall within the definition of correspondent relationships. For the purposes of this guidance, however, a distinction is drawn between banking and trading relationships, given the different risks and method of operation. This is reflected in the way that due diligence measures should be applied. Collectively, correspondent banking and correspondent trading relationships will be referred to as “correspondent relationships”.

*Wwft 1(1), FATF Guidance correspondent banking services (2016)*

10.2 Correspondent relationships covers:

- **A “correspondent trading relationship”** is a relationship between credit institutions or financial institutions for the provision of commercial or business products or services, which may include relationships established for securities transactions or funds transfers, including services within the scope of wholesale markets or syndicated lending, or which could simply be the provision of loan finance from one credit or financial services institution to another. Such relationships may be described as a bilateral commercial arrangement between two institutions, rather than the provision of “correspondent banking relationship”-related services from one institution to another (as defined above). These relationships do not have a traditional correspondent and a respondent since neither party is providing services on behalf of the other or for an underlying customer; accordingly, the degree of ML/TF risk in such relationships is different, generally lower, than it is with relationships that provide for banking-related services on behalf of that institution's customers. They are more similar to normal customer relationships.

A "**correspondent banking relationship"** is the provision of banking-related services by one bank (the 'correspondent bank') to another bank (the 'respondent bank'). Large international banks typically act as correspondents for many other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable through accounts and foreign exchange services. Correspondent banking does not include one-off transactions or the mere exchange of SWIFT RMA-keys in the context of non-customer relationships, but is rather characterized by its ongoing, repetitive nature. Correspondent banking services encompass a wide range of services that do not all carry the same level of ML/TF risks. Some correspondent banking services present a higher ML/TF risk because the correspondent institution processes or executes transactions for its customer's customers. Hence, the focus of the risk-based due diligence is on correspondent banking relationships that are higher risk, in particular cross-border correspondent banking relationships involving the execution of third party payments.

10.3 Generally, in a correspondent banking relationship, a correspondent is effectively an agent (intermediary) for the respondent and executes/processes payments or other transactions for customers of the respondent. The underlying customers may be individuals, corporates or even other financial services banks. Beneficiaries of transactions can be customers of the correspondent, the respondent itself or, in many cases, customers of other banks and therefore unknown.

## What are money laundering risks in correspondent relationships?

10.4 The correspondent often has no direct relationship with the underlying parties to a transaction and is therefore not in a position to verify their identities. Correspondents often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments or clearing cheques.

10.5 For these reasons, correspondent relationships are, in the main, non-face-to-face business and, when an unknown third party is

involved, must be regarded as potentially high risk from a ML/TF perspective.

10.6 Correspondent banking relationships, if poorly controlled, can allow other financial services institutions with inadequate AML/CTF systems and controls, and customers of those banks, direct access to international banking systems.

10.7 A correspondent handling transactions that represent the proceeds of criminal activity or terrorist financing risks regulatory fines and/or damage to its reputation.

10.8 The degree of ML/TF risk presented by different types of correspondent relationships between banks will vary, sometimes considerably – for example, some relationships cannot result in payments being made, which carries an almost non-existent degree of risk – and, therefore, the appropriate customer due diligence measures that should be applied will similarly vary, according to the assessed degree of risk.

10.9 The primary risk in correspondent relationships turns on whether a relationship or transaction is between financial or credit institutions as principal, where the risks are inherently low, especially where the counterparty is based in an assessed low risk jurisdiction. Where the transaction relates to an underlying customer or customers – if this is disclosed, the correspondent will know who it is dealing with, if undisclosed, this will heighten the risk.

### How to assess the elements of risk in correspondent trading relationships

10.10 The degree of risk in a correspondent trading relationship should be determined bearing in mind the risks inherent in the product and service, and the risks posed by the nature and jurisdictions of operation of the counterparty, in particular whether or not unknown third parties are involved. The risk assessment will essentially follow the bank's standard approach.

### How to assess the elements of risk in correspondent banking relationships

10.11 For any correspondent, the highest risk respondents are those that:

- Deal or trade on behalf of undisclosed customers; or

- Are offshore banks that are limited to conducting business with non-residents or in non-local currency, and are not subject to robust supervision by their AML/CTF controls; or

- Are domiciled in jurisdictions with weak regulatory/AML/CTF controls or other significant reputational risk factors e.g., corruption.

10.12 The following risk factors should be considered both when initiating a relationship, and on a continuing basis afterwards, to determine the levels of risk-based due diligence that should be undertaken. These risks are particularly relevant for correspondent banking relationships:

- **The respondent's domicile.** The jurisdiction where the respondent is based and/or where its ultimate parent is headquartered may present greater risk (or may mitigate the risk, depending on the circumstances). Certain jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Other jurisdictions, however, such as many members of the Financial Action Task Force (FATF), have more robust regulatory environments, representing lower risks. Correspondents should review statements by regulatory agencies and international bodies such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the respondent and/or its parent are based. Please refer also to the list of Recognised Regulators in Part I, annex II.

- **The respondent's ownership and management structures.** The location of owners, their corporate legal form and/or a lack of transparency of the ultimate beneficial ownership are indicative of the risk the respondent presents. Account should be taken of whether the respondent is publicly or privately owned; if publicly held, whether its shares are traded on a Recognised Exchange (refer to the list of Recognised Exchanges in Part I, annex I) or, if privately owned, the identity of any UBOs and controllers. Similarly, the location and experience of management may indicate additional concerns, as would unduly frequent management

turnover. The involvement of PEPs in the management or ownership of certain respondents may also increase the risk.

- **The respondent's business and customer base.** The type of business the respondent engages in, as well as the type of markets it serves, is indicative of the risk the respondent presents. Involvement in certain business fields that are internationally recognized as particularly vulnerable to money laundering, corruption or terrorist financing, may present additional concern. Consequently, a respondent that derives a substantial part of its business income from higher risk customers may present greater risk. Higher risk customers are those customers that may be involved in activities, or are connected to jurisdictions, that are identified by credible sources as activities or countries that are especially susceptible to ML/TF or corruption. Equally, a respondent that has a predominantly low risk customer base, and/or is based in a well-regulated jurisdiction with high AML/CTF standards, carries a lower risk. Please refer also to the list of Recognised Regulators in Part I, annex II.

- **Downstream correspondent clearing.** A downstream correspondent clearer is a respondent that receives correspondent banking services from a correspondent and itself provides correspondent banking services to other financial institutions in the same currency as the account it maintains with its correspondent. When these services are offered to a respondent that is itself a downstream correspondent clearer, a correspondent should, on a risk-based approach, take reasonable steps to understand the types and risks of financial institutions to whom the respondent offers such services. And specific care should be taken to ensure there are no shell bank customers, and consider the degree to which the respondent examines the AML/CTF controls of those financial institutions.

10.13 Other factors that might affect the respondent's risk profile (non-exhaustive):

- The respondent, their parent or a bank belonging to the same group as the respondent has recently been the subject of any criminal case or regulatory enforcement for inadequate AML/CTF policies and procedures and/or breaches of AML/CTF obligations;

- The history of the customer relationship with the respondent gives rise to concern, for example because the number of transactions is not in line with what the correspondent would expect based on previous knowledge of the nature and size of the respondent;

- There is a suspicion of ML/TF in relation to the respondent;

- A SAR has been filed for the respondent (specific branch or subsidiary);

- Respondents operating under an offshore banking licence;

- There is adverse media by reputable sources in relation to the respondent;

- Sanctioned parties are involved;

- Respondents designated by the US Secretary of the Treasury as warranting special measures due to money laundering concerns, under section 311 of the U.S.A. Patriot Act;

- Respondents operating under a banking license issued by a country that has been designated by the Secreatry of the US Treasury, as warranting special measures due to money laundering concerns, under section 311 of the U.S.A. Patriot Act.

10.14 The following factors may indicate lower risk:

- The respondent is registered as a licensed bank in the EEA.

- The respondent is registered as a licensed bank in a third country that has AML/CTF requirements consistent with the 2012 FATF Recommendations and effectively implements those requirements. Please refer also to the list of Recognised Regulators in Part I, annex II.

- The relationship is limited to a SWIFT RMA plus capability, which is designed to manage communications between financial institutions. This means that the respondent, or counterparty, does not have a payment account relationship.

- The banks are acting in a principal-to-principal capacity, rather than processing transactions on behalf of their underlying customers, e.g. foreign exchange services between two banks where the business is transacted on a principal to principal basis and where the settlement of such a transaction does not involve a payment to an unknown third party.

10.15 Correspondent relationships with shell banks are prohibited in all circumstances and so the bank should satisfy itself that its counterparty is not a shell bank. Furthermore the bank must take appropriate measures to ensure that it does not enter into, or continue, a correspondent relationship with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank.

## Customer due diligence

### *Risk-based approach*

*Wwft 2b(2)*

10.16 A bank can take a risk-based approach, meaning that the AML/CTF measures may vary in view of specific risks the bank has identified, but must be commensurate to those risks in order to mitigate them effectively. The nature and the extent of the CDD measures depend on the risks involved, including the type of customer, product, service, transaction and distribution channel and geographies. The CDD measures to be carried out in relation to correspondent relationships depends on the particular type of relationship established, where the counterparty is based, and the degree of ML/TF risk presented by the relationship.

10.17 All correspondent relationships must be subject to an appropriate level of due diligence which:

- Meets the bank's standard due diligence requirements, reflecting the degree of risk determined in the relationship, and;
- Ensures that the bank is comfortable conducting business with/for a particular counterparty (and, if applicable, its underlying customers) given the counterparty's risk profile.

10.18 For counterparties based in an EEA member state, the bank will follow its standard due diligence procedures, based on its determination of the ML/TF risk presented following its risk assessment. This may lead the bank to apply CDD, SDD (adjusted due diligence) or EDD measures in accordance with the guidance in Part I, sections 1.5 and 2.5. In case of correspondent banking relationships banks should take into account the risk factors described in paragraphs 1.12 and 1.13.

10.19 Where a counterparty based in a third country is a branch or subsidiary undertaking of a credit or financial institution in an EEA state, the bank should on a risk-based approach consider the extent to which the specific EDD measures as mentioned in article 8(4) Wwft should be applied. The risk presented by such a customer may be mitigated where it is subject to group AML/CTF standards that are compliant with the EU Directive 2015/849 and the parent entity is EEA regulated.

10.20 The extent of the correspondent relationship should be factored into the level of due diligence undertaken. A bank, under its risk-based approach, may decide to lower its level of due diligence measures for limited correspondent banking relationships, such as those limited to a SWIFT RMA plus capability (the respondent does not have a payment account relationship), or for correspondent trading relationship transactions undertaken within the NL or the EEA on a bilateral basis. It will also be appropriate for a bank to take account of the fact that a counterparty bank is domiciled or operating in a regulatory environment that is recognised internationally as adequate in the fight against money laundering/terrorist financing and corruption (refer to the list of Recognised Regulators in Part I, annex II). See 10.14 for other factors that may decrease the risk.

10.21 In respect of correspondent banking relationships, the level and scope of due diligence undertaken should take account of the relationship between the respondent and its ultimate parent (if any). In general, for relationships maintained with branches, subsidiaries or affiliates, the status, reputation and controls of the parent entity should be considered in determining the extent of due diligence required on the respondent. Where the respondent is located in a high risk jurisdiction, correspondents may consider it appropriate to conduct additional due diligence on the

respondent as well as the parent. In instances when the respondent is an affiliate that is not substantively and effectively controlled by the parent, then the quality of the affiliate's AML/CTF controls should always be established.

The correspondent, in assessing the level of due diligence to be carried out in respect of a particular respondent, (in addition to the factors mentioned in the paragraphs 10.12 and 10.13) must consider:

- **Regulatory status and history.** The primary regulatory body responsible for overseeing or supervising the respondent and the quality of that supervision. If warranted by circumstances, a correspondent should also consider publicly available materials to ascertain whether the respondent has been the subject of any criminal case or adverse regulatory action in the recent past.

- **AML/CTF controls.** A correspondent should establish whether the respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the respondent is required to verify the identity of its customers and apply other AML/CTF controls to FATF standards/equivalent to those laid down in EU Directive2015/849. Where this is not the case, additional due diligence should be undertaken to ascertain and assess the effectiveness of the respondent's internal policy on money laundering/terrorist financing prevention and its 'know your customer' and activity monitoring controls and procedures. When undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to FATF standards/equivalent to those laid down in EU Directive 2015/849. If not, the extent to which the parent's controls meet FATF standards/equivalent to those laid down in the EU Directive 2015/849 and whether these are communicated and enforced 'effectively' throughout its network of international offices, should be ascertained.

10.21 To satify its due diligence requirements the bank may, depending on the risks involved, rely on:
- Publicly available information from reliable sources;
- Information obtained from the counterparty itself;

- Information obtained from other credible sources (e.g., regulators, exchanges);
- Information obtained from reputable information sources (e.g. SWIFT KYC Registry).

The Wolfsberg Group has developed questionnaires to support correspondents in meeting their due diligence requirements regarding correspondent relationships. Currently there are two different Wolfberg questionnaires available:

- The Financial Crime Questionnaire (FCCQ). Banks may consider using this questionnaire in case of lower risk situations such as SWIFT RMA plus capability and correspondent trading relationships.
- The Correspondent Banking Due Diligence Questionaire (CBDDQ), which is a considerably extended version. Banks may consider using this questionnaire in higher risk situations such as correspondent banking relationships with respondents established in non-EU member states (refer to 1.28-1.29).

Although these questionnaires are efficient tools a bank should always consider on a case-by-case basis whether the provided information is sufficient to mitigate the risks involved.

10.22 A bank's policies, controls and procedures should require the information, including due diligence, held relating to the counterparty to its correspondent relationship to be periodically reviewed and updated. The frequency of review should be tailored to the assessed degree of risk and updating should be undertaken as a result of trigger events e.g. an extension to the service/product range provided; a material change to the nature/scope of business undertaken by the respondent; or as a result of significant changes to its legal constitution, or its owners or controllers or negative regulatory statements and/or press coverage.

### Enhanced due diligence for correspondent relationships

*Wwft (8)(4), EBA The Risk Factors Guidelines paragraph 90*

10.23 When the respondent is not based in EEA member state correspondents are required to apply the specific EDD measures as mentioned in article 8(4) Wwft. However, correspondents can adjust the extent of these measures using a risk-based approach.

As a rule of thumb the due diligence must be sufficiently extensive for the correspondent to be able to form a reasonable belief and be confident that it knows on an ongoing basis which risks it runs in order to manage those risks effectively.

10.24 These specific EDD measures may also be carried out with respect to respondents based in EEA member states if the bank, based on its risk assessment, determines that the relationship presents a higher degree of ML/TF risk.

10.25 Banks need to ensure that the specific EDD requirements are applied to non-EEA counterparties. When considering whether a counterparty should be treated as an EEA institution or a non-EEA institution the relationship should be assessed at the regulated bank level, rather than at the legal entity level. Banks should ensure that they fully document their decision-making process.

10.26 When undertaking EDD banks should identify whether they are entering into a correspondent banking or correspondent trading relationship. A correspondent banking relationship presents by its nature a higher ML/TF risk to banks. By contrast, a correspondent trading relationship, and in particular that in which no unknown third party is involved, may be lower risk. In applying EDD measures, banks must decide on the precise measures to be applied on a risk sensitive basis.

*Enhanced due diligence for correspondent banking relationships*

10.27 The following EDD measures, as listed in article 8(4), should be considered for correspondent banking relationships using a risk-based approach and taking into account the paragraphs 10.24 to 10.27:

- **Nature of business**. Banks must gather sufficient information about the respondent to fully understand the nature of its business. The amount of information gathered on the customer may be on a risk-based approach and may take into consideration the following (non-exhaustive list):
    - Type of respondent – an assessment of the credit or financial institution type;
    - Business Model – the customer base of the respondent and the products and services it offers;

- Country of operations – is the respondent based in a non-EEA member state, which has AML/CTF requirements that are equivalent to the Wwft and/or EU Directive 2015/849. Refer to the list of Recognised Regulators in Part I, annex II.
- Does the respondent have operations in high risk jurisdictions?

- **Reputation and supervision**. Banks must determine using credible, publicly available information, the reputation and supervision of the respondent. Banks should consider the following:
  - The disciplinary record of the respondent – has the respondent been subject to recent regulatory enforcement for inadequate AML/CTF systems and controls?
  - Regulated status of the respondent – whether the respondent is regulated;
  - AML regime – is the respondent based in a non-EEA country with an effective AML/CTF regime? Please refer to the list of Recognised Regulators in Part I annex II.
  - Jurisdiction in which the respondent is regulated - whether the respondent is subject to adequate AML /CTF Supervision regime. Please refer to the list of Recognised Regulators in Part I annex II

- **Assessment of the bank's AML/CTF controls**. Banks must assess the respondent's AML/CTF framework. This may be applied on a risk-based approach, with a varying degree of scrutiny depending on the risks identified as part of the EDD process.

In meeting the above mentioned requirements banks may consider using the Wolfsberg Correspondent Banking Due Diligence Questionnaire (CBDDQ). See also 10.21. Additionally, based on the risks involved, the correspondent may wish to speak with representatives of the respondent to obtain comfort that the respondent's senior management recognises the importance of AML/CTF controls.

- **Senior management approval.** Banks must obtain senior management approval before establishing a new correspondent banking relationship. The bank should

determine who constitutes “senior management” for the purposes of the correspondent banking relationship approval process. However, the approver should have sufficient knowledge of the bank’s ML/TF risk exposure, and of sufficient authority to take decisions affecting the bank’s risk exposure. Banks should document internally their approach to customer relationship approvals and should have a graded scale of approvals depending on the risk of the customer relationship.

A new correspondent banking relationship refers to the initial onboarding of the customer. However, banks should consider, on a risk-based approach whether any further senior management approvals might be required by the risk profile of the new product and/or business line being offered and in accordance with the banks risk assessment of the business.

- **Responsibilities of the respondent and correspondent**. Banks must document the responsibilities of the respondent and correspondent. In some instances this information may be contained within contractual language (including terms of business) between the correspondent and respondent.

- **Direct access to correspondent accounts**. Banks must identify whether the respondent’s customers have access to their accounts. If the respondent’s customers have access, the correspondent must be satisfied that:
    - The respondent has verified the identity of, and conducts relevant CDD checks on, their customers on an ongoing basis;
    - The respondent is able to provide upon request the CDD data or information gathered.

- **SWIFT (RMA) relationships**[15]. Due diligence should take into account the message types being made available to the respondent bank. Message types Category 1 and Category 2 bring heightened risks and, therefore, EDD must be considered regarding respondents established in non-EEA member states.

.....

[15] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/7.%20SWIFT-RMA-Due-Diligence.pdf

- **Shell banks**. Whether the respondent has confirmed that it will not provide banking services to, or engage in business with, shell banks.

10.28 The EDD process for correspondent banking relationships should involve further consideration of the following elements designed to ensure that the correspondent has on a risk-based approach secured a greater level of understanding:

- **Respondent's ownership and management.** For all UBOs and controllers, the sources of wealth and background, including their reputation in the market place, as well as recent material ownership changes (e.g. in the last three years), and an understanding of the experience of each member of executive management.

- **PEP involvement**. If a PEP (see Part I, Chapter 1) appears to have a material interest or management role in a respondent then the correspondent should ensure it has an understanding of that person's role in the respondent.

*Enhanced due diligence for correspondent trading relationships*

10.29 In relation to correspondent trading relationships, a bank will apply its standard due diligence approach, based on its determination of the ML/TF risk presented following its risk assessment. This may lead the bank to apply CDD, SDD (adjusted due diligence) or EDD measures in accordance with the guidance in Part I, sections 1.5 and 2.5.

10.30 Due to the inherently lower risk profile of many correspondent trading relationships, a bank should take the following measures in order to meet the prescribed specific EDD requirements of the Wwft relating to correspondent trading relationships with non-EEA based respondents (in addition to its standard CDD approach, based on its determination of the ML/TF risk presented following its risk assessment):

- Ensure that the other institution is clearly identified in the bank's records as being the counterparty to the transaction;

- Gather information about the nature of the business of the other institution;

- Include relevant related parties of the institution in the bank's regular customer screening for PEPs, sanctions and other financial crime indicators and follow the same approach as for other customers in terms of assessing and applying the results of such screening within the bank's risk-based approach;

- Satisfy itself that the other institution is authorised and regulated in a non-EEA country, which has AML/CTF requirements which are equivalent to the Wwft and/or EU Directive 2015/849. Please refer to the list of Recognised Regulators in Part I, annex II;

- Or otherwise undertake an assessment of the other institution's AML/CTF framework. This may be applied on a risk-based approach, with a varying degree of scrutiny depending on the risks identified as part of the EDD process.

In meeting the requirements mentioned above, banks may consider, dependent on the risks involved, using one of the Wolfsberg Questionnaires. See also 10.21.

- Obtain the approval from senior management before establishing a new correspondent trading relationship. In this case, the level of seniority of the manager required to give such an approval should be commensurate with the risk, provided the approver has sufficient knowledge of the bank's AML/CTF risk exposure, and is of sufficient authority to take decisions affecting the bank's risk exposure. Senior management should not be understood as referring to persons identified as senior managers under the senior manager regime - banks may internally decide who is a "senior manager" for the purposes of approving correspondent trading relationships. For example, a relationship with an institution that is authorised and regulated in a non-EEA country, which has AML/CTF requirements equivalent to EU Directive 2015/849) (refer to the list of Recognised Regulators in Part I, annex II), could be approved by the senior manager of the desk in question;

- Where appropriate, retain a copy of the terms and conditions that govern the transactions between the bank and the other institution (as the only responsibilities between the two

institutions concern the execution of the transaction in accordance with its terms); and

- Ensure that the other institution is not entering into the correspondent trading relationship on behalf of, or as agent for, a shell bank (in this regard, transaction terms which clearly state that the institution is entering into the transaction as principal and not as agent would be sufficient).

10.31 Where a bank identifies additional risk(s) or is not able to satisfy the measures set out in 1.31, it should consider which enhanced due diligence measures would be appropriate to mitigate the additional risk.

## Monitoring of Correspondent Banking Relationships

10.32 Implementing appropriately documented monitoring procedures can help mitigate the money laundering risks for banks undertaking correspondent banking activities. General guidance on monitoring is set out in Part 1, section 2.8.

10.33 The level of monitoring undertaken by a correspondent on its respondent's activity should be commensurate with the risks posed by the respondent. Due to the significant volumes that correspondent banking activity can entail, in conjunction with the need to work within prescribed scheme settlement deadlines, electronic and/or post-execution monitoring processes are often the norm.

10.34 Where relevant, observation of the following in relation to correspondent banking relationships should lead to monitoring activity:

- Anomalies in behaviour

Monitoring for sudden and/or significant changes in transaction activity by value or volume.

- Hidden relationships

Monitoring for activity between accounts, customers (including respondents and their underlying customers). Identifying common beneficiaries and remitters or both amongst apparently unconnected accounts/respondents. This is commonly known as link analysis.

- High risk geographies and entities

Monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher risk geographies and/or entities.

- Other money laundering behavioural patterns

Monitoring for activity that may, in the absence of other explanation, indicate possible money laundering, such as the structuring of transactions under reporting thresholds, or transactions in round amounts

- Other considerations

In addition to the monitoring techniques above, the monitoring system employed to monitor correspondent banking for AML/CTF purposes should make it possible to apply different thresholds against customers that are appropriate to their particular risk category.

10.35 In addition to monitoring account/transaction activities, a correspondent should monitor a respondent for changes in its nature and status. As such, information about the respondent collected during the customer acceptance and due diligence processes must be:

- Reviewed and updated on a periodic basis. (Periodic review of customers will occur on a risk-assessed basis), or
- Reviewed on an ad hoc basis as a result of changes to the customer's information identified during normal business practices, or
- Reviewed when external factors result in a material change in the risk profile of the customer.

10.36 Where such changes are identified, the respondent should be subject to an EDR. General guidance on monitoring is set out in Part 1, section 2.8. Where, as a result of the EDR, the risk categorisation is altered (either up or down) a bank should ensure that the due diligence standards for the respondent's new risk categorisation are complied with, by updating the due diligence already held. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk category.

10.37 Banks should consider terminating the accounts of respondents, and consider their obligation to report suspicious activity, for

respondents who fail to provide satisfactory answers to reasonable questions regarding transactions/activity passing through the correspondent relationship, including, where appropriate, the identity of their customers featuring in unusual or suspicious transactions or activities.

### Staff awareness, training and alertness in respect of correspondent banking relationships

10.38 Where the bank is a correspondent, the bank must train staff on how correspondent banking transactions may be used for ML/TF and in the bank's procedures for managing this risk. This training should be directed specifically at those staff directly involved in correspondent banking transactions and dealing with correspondent banking customers and should be tailored to the greater risks that this type of business represents.

10.39 Banks should provide "senior management" approving correspondent relationships with appropriate training to provide them with sufficient knowledge of the bank's money laundering and terrorist financing risk exposure.

Monitoring and staff awareness, training and alertness in respect of correspondent trading relationships.

10.40 The monitoring and staff awareness, training and alertness principles set out in Part I, chapter 5 of this Guidance would be applicable.

# Chapter 11

# Syndicated Lending

## Introduction

*Overview of the sector*

11.1 The syndicated loan market is an organised professional market, international in nature, providing much of the capital used by some of the largest companies in the world for a variety of purposes, ranging from working capital to acquisition financing. Banks and other financial institutions agree to grant term loans and revolving credit loans to companies and may syndicate (offer on), or sell off, parts of their commitments to other banks, financial institutions or other entities.

11.2 The following sets out the relationships that exist in loan syndications:

- Borrower. A corporate or other legal entity that seeks to borrow funds and/or arranger credit facilities through the international capital markets.
- Mandated Lead Manager/Arranger/Bookrunner. A mandated Lead Manager/Arranger/Bookrunner enters into an agreement to provide credit facilities to a borrower. By the very nature of this appointment, it is likely that the mandated Lead Manager/Arranger/Bookrunner will be a lender with which the Borrower already has an established relationship. A syndicated loan transaction typically may have one to four mandated Lead Managers/Arrangers/Bookrunners and many lenders. The Mandated Lead Manager/Arranger/Bookrunner is normally responsible for advising the Borrower as to the type of facilities it requires, negotiating the broad terms of those facilities and advising on roles, timetable and approach to the market. In some instances it will also underwrite the transaction.
- Lenders. The financial institutions that provide the funds that have been arranged for the Borrower by the Mandated Lead Manager/Arranger/Bookrunner.
- Agent. To facilitate the process of administering the loan an Agent is appointed. The Agent acts as the agent of the Lenders

not of the Borrower, although it is the Borrower that pays the Agent's fees and charges. The Agent acts as an intermediary between the Borrower and the Lenders, undertaking administrative functions, such as preparing documentation, servicing and acting as a channel for information between the Lenders and Borrower. One of the Lenders from the syndicate is normally appointed as the Agent.The Agent has a number of important functions:

- Point of contact (maintaining contact with the Borrower and representing the views of the syndicate);
- Monitor (monitoring the compliance of the Borrower with certain terms of the facility);
- Postman and record-keeper (it is the Agent to whom the Borrower is usually required to give notices); and
- Paying agent (the Borrower makes all payments of interest and repayments of principal and any other payments under the loan agreement to the Agent. The Agent passes these monies back to the Lenders to whom they are due. Similarly, the Lenders advance funds to the Borrower through the Agent).

- Guarantor. As part of the loan agreement, the Borrower may provide guarantors, who will guarantee repayment of the loan if the Borrower defaults on the loan, on a joint and several basis.

11.3 A bank often fulfils multiple roles in the syndicated loan market. Most commonly as Agent, Mandated Lead Manager, Lead Arranger, Bookrunner or Lender. Where mention is made of these roles, these will also be understood to apply to a bank dependent on the role(s) specified in the arrangement.

11.4 The cash flows arising from these arrangements are between the syndicate participants (lenders) and the Agent, and then on to the Borrower. Similarly, payments made by the Borrower to the Lenders take place via the Agent. The Lenders do not usually have any direct contact with the Borrower with respect to cash flows.

11.5 A secondary market also exists where banks and others buy and sell interests in these loans.

## Customer due diligence

### *The customer from an AML perspective*

11.6 The obligation on each party to a syndicated lending arrangement to verify the identity of the customer is as follows:

- Mandated Lead Manager/Arranger/Bookrunner: The Borrower and the agent are the mandated Lead Manager/Arranger/Bookrunner's customer.
- Lenders: The Borrower is also a customer of the syndicate participants.
- Agent: The Agent's customers are the Borrower, the Mandated Lead Manager/Arranger/Bookrunner and the Lenders.

### *Customer Due Diligence Process*

11.7 The Mandated Lead Manager/Arranger/Bookrunner must apply the guidance set out in Part I on the Borrower and the Agent.

11.8 The Agent must apply the guidance set out in Part I, in line with the firm's risk-based approach, to the Borrower, the Mandate Lead Manager/Arranger/Bookrunner and the Lenders. The Agent, when as part of its risk-based approach it feels it is appropriate to do so, may take into account the due diligence carried out by the Mandated Lead Manager/ Arranger/Bookrunner on the Borrower. It is often the case that the Lenders have pre-existing relationships with the Mandated Lead Manager/Arranger/Bookrunner and/or the Agent so that, in practice, little, if any, additional due diligence will need to be undertaken.

11.9 The Lender also has a responsibility to apply the guidance set out in Part I, subject to the firm's risk-based approach, to the Borrowers. The Mandated Lead Manager/Arranger/Bookrunner and Agent also have an obligation to conduct CDD on the Borrower, the Lender may, where as part of its risk-based approach it feels it is appropriate to do so, take account of the due diligence carried out by the Mandated Lead Manager/Arranger/Bookrunner and/or Agent on the borrower where they are in a comparable jurisdiction. In such instances it may be appropriate for the reliance arrangements to be confirmed in a certificate to the Lenders stating that the CDD has been undertaken and documentation is available on request. This

may be facilitated by the Borrower undertaking to provide all relevant CDD documentation.

11.10 It should be noted that when a bank in a syndicated loan arrangement takes account of due diligence done by another bank it remains ultimately responsible for compliance with Wwft as well as risk acceptance.
For this reason banks should therefore consider requesting the due diligence work done by the other party instead of relying on a request.

11.11 Where the Borrower has provided a guarantor as part of the loan agreement, all parties who have an obligation to identify the Borrower - Mandated Lead Manager/Arranger/Bookrunner, Lenders and Agent - should consider whether it is necessary, based upon their risk-based approach, to apply to the guarantor relevant CDD measures, but at least identification and screening against the applicable lists (e.g. sanctions).

11.12 The guarantor is not considered a customer of the bank. However, since the guarantee may be used to obscure the criminal origin of the funds, the relation between the Guarantor and the Borrower needs to be clarified. This means assessing whether the link between the Borrower and Guarantor is logical and has an economic rationale. In addition, the origin of the collateral also needs to be established.

11.13 The money laundering risk associated with a guarantor only becomes real, if a borrower defaults on a loan, and the guarantor is called upon to repay the loan. A bank may consider, subject to its risk-based approach, whether it should verify the identity of the guarantor at the same time as the Borrower, or only to identify the guarantor as and when the guarantor is called upon to fulfil their obligations under the loan agreement.

11.14 When considering the extent of the risk assessment appropriate for a particular borrower, any normal commercial credit analysis that has been undertaken on the Borrower should be taken into account, and should be factored into a bank’s risk-based approach.

*Secondary market in syndicated loans*

11.15 A Lender under a syndicated loan may decide to sell its participation in order to: realise capital; for risk management purposes, for example to re-weight its loan portfolio; meet regulatory capital requirements; or to crystallise a loss. The methods of transfer are usually specified in the Syndicated Loan Agreement.

11.16 The most common forms of transfer to enable a Lender to sell its loan commitment are: novation (the most common method used in transfer certificates to loan agreements); legal assignment; equitable assignment; fund participation and risk participation. Novation and legal assignment result in the Lender disposing of its loan commitment, with the new lender assuming a direct contractual relationship with the Borrower, whilst the other methods result in the Lender retaining a contractual relationship with the Borrower and standing between the purchaser in the secondary market and the Borrower. The transfer method should be taken into account by the purchasing firm when considering its customer due diligence requirements.

## Customer due diligence

11.17 A bank selling a participation in a loan should apply the guidance set out in Part I, in line with its risk-based approach, when identifying, and if necessary verifying the identity of, the purchaser.

11.18 A bank purchasing a participation in a loan should apply the guidance set out in Part I, in line with its risk-based approach, when identifying, and if necessary verifying the identity of, the seller.

11.19 The money flows are between the purchaser and seller of the loan. However, if a bank purchases a participation in an existing loan from another participant by way of novation or legal assignment, it will have a direct contractual relationship with the Borrower. As such the purchaser has an obligation to identify, and if appropriate as part of its risk-based approach, verify the identity of the Borrower, in accordance with the guidance set out in Part I.

11.20 Where a bank purchases a participation in an existing loan from another participant (the Lender) by way of equitable assignment, fund participation or risk participation the seller acts as intermediary between the purchaser and the Borrower for the life of the loan. Depending on the status of the Lender (seller), the purchaser should decide as part of its risk-based approach whether it has an obligation to identify, and verify the identity of, the Borrower.

11.21 In addition, a bank purchasing a loan in the secondary market must check the underlying Borrower against applicable lists (e.g. sanctions).

11.22 Whether the Agent is required to undertake customer due diligence on a secondary purchaser of a loan participation will depend upon how the transfer between the seller and the purchaser in the secondary market is made:

- Where the sale is by way of novation or legal assignment the Agent should, as part of its risk-based approach, identify, and verify the identity of, the purchaser, in accordance with the guidance set out in Part I, Chapter 5.
- Where the sale is by way of equitable assignment, the Agent may not have a direct relationship with the purchaser, even though funds may flow through the Agent from or to the purchaser (via the Lender), and therefore the Agent may not have an obligation to identify and/or verify the purchaser. However, the Agent should screen against applicable lists (e.g. sanctions) and consider, as part of its risk-based approach, whether it should identify, or verify the identity of, the purchaser in accordance with the guidance set out in Part I.
- Where the sale is by fund participation or risk participation, the Agent will not necessarily be aware of the transaction and therefore has no obligation to identify and/or verify the purchaser or check them against applicable lists (e.g. sanctions).

## Money Laundering risk

11.23 Syndicated loans tend to be made to large, often multi-national companies, many of which will have their securities listed, or are parts of corporate groups whose securities are listed on a recognized exchange (Part I, Annex I). As such, the money

laundering risk relating to syndicated loans for this type of customer should in general be regarded as low.

11.24 The features of all lending are generally that the initial monies advanced are paid into a bank account. In syndicated lending the monies are usually handled by the Agent making it unlikely that the transaction would be used by money launderers in the placement stage of money laundering. Syndicated facilities could, however, be used to layer and integrate criminal proceeds. Repayments are usually made from the Borrower's bank account to the Agent who administers the repayment from its bank accounts to the Lenders. Repayments in cash are unlikely and must be assessed when they occur.

11.25 Given that a syndicated loan results in the Borrower receiving funds from the Lender, the initial transaction is not very susceptible to money laundering. The main money laundering risk arises through variations in the loan arrangements such as the acceleration of an agreed repayment schedule, either by means of lump sum repayments, or early termination without good commercial rationale. When these circumstances occur they should be considered carefully and consideration must be given to the source of the money used to accelerate the repayment schedule, or terminate the loan early.

# Chapter 12

# Wholesale Markets

## Overview of the sector

12.1 Wholesale banking refers to banking services between merchant banks and other financial institutions. This type of banking deals with professional customers, such as large corporations and other banks.

12.2 Wholesale banking services include currency conversion, working capital financing, large trade transactions, and other types of specialized services for generally high net worth corporate entities. The wholesale markets comprise exchanges and dealing arrangements that facilitate the trading (buying and selling) of wholesale investment products, and hedging instruments ("traded products"), including, but not limited to:

- Securities: equities, fixed income, warrants and investment funds (Exchange Traded Funds – ETFs);
- Money market instruments: FX, interest rate products, term deposits;
- Financial derivatives: options, futures, swaps and warrants;
- Commodities: physical commodities and commodity derivatives, including exotic derivatives (e.g. weather derivatives); and
- Structured products (e.g. equity linked notes).

12.3 This chapter provides general guidance on assessing risks in wholesale markets, due diligence and monitoring. It then provides additional guidance on each of the product types referred to above. Reference should be made to both the general and the relevant product-specific guidance in this section, as well as to the general guidance in Part I.

12.4 Traded products confer 'rights' or 'obligations'; either between an investor and the issuer, or between parties engaged in the trading of the instruments. Traded products can be bought, sold,

borrowed or lent; as such, they facilitate the transfer of property or assets and usually represent an intrinsic value, which may be attractive to money launderers. Traded products can be bought or sold either on an exchange (“exchange traded products”), or between parties ‘over-the-counter’ ("OTC").

12.5 Some traded products or instruments, such as equities, are issued in a ‘primary’ market, and are traded in a ‘secondary’ market, allowing investors in the primary market to realise their investment. Other traded products are created to enable investors to manage assets and liabilities, exchange risks and exposure to assets, commodities or securities.

*Exchange-traded products*

12.6 Exchange-traded products are financial products that are traded on exchanges, which have standardised terms (e.g. amounts, delivery dates and terms) and settlement procedures and transparent pricing. Banks may deal in exchange-traded products as principals or as agents for their customers. In the financial and commodity derivatives markets, banks will typically deal as principals, and on certain exchanges (e.g. Euronext.LIFFE, ICE Futures, LME) must do so when dealing as a clearing member in relation to their customers’ transactions. In the securities markets, banks can deal as either principals or as agents for the banks’ underlying customers.

12.7 Most exchanges have a Central Counterparty (CCP) that stands between the exchange members that are buying and selling a product (becoming the buyer to the seller and the seller to the buyer). When an exchange or trading platform does not have a CCP, the members contract with each other.

The following are persons typically involved in wholesale market activities:

- Instructing Counterparty: The customer on whose behalf the transaction or trade is being conducted;
- Agent: An agent in the context of the wholesale markets is an entity that provides related financial services for or on behalf of a customer;
- Executing Broker: An executing broker is the broker or dealer that finalises and processes an order to transact/trade on behalf of a customer; Clearing Broker: A clearing broker settles transactions/trades on behalf of

the customer and as such will handle the movement of funds or assets for the customer in settlement of respective transactions and liabilities;

- Central Counterparty (CCP): A CCP is an organisation that exists to help facilitate trading activities on certain markets by providing efficiency and stability as a financial intermediary to a transaction/trade;
- Custodian: A custodian is a financial institution that holds a customer's securities for safekeeping and protection; and
- Investment Manager or Adviser: Funds are managed by an investment manager, which is a separate legal entity from the fund, and which is given authority to act as agent and manage the funds and investments held by the fund vehicle. It is often the investment manager that will make investment decisions and place transactions with the bank as agent of the fund. The investment manager may delegate certain activities to a separate Investment Adviser.

*OTC products*

12.8 OTC products are bilateral agreements between two parties (or may be multilateral agreements, depending on the settlement process) that are not traded or executed on an exchange. The terms of the agreement are tailored to meet the needs of the parties, i.e. they are not necessarily standardised terms, contract sizes or delivery dates. Where banks deal OTC, they usually deal as principals. Some OTC dealing is facilitated by brokers and, while settlement is normally affected directly between the parties, it is becoming increasingly common for exchanges and clearers to provide clearing facilities (i.e. the trades are executed as OTC but are then given up for clearing by a CCP).

## What are the money laundering and terrorist financing risks in Wholesale?

12.9 Traded products are usually traded on regulated markets, or between regulated parties, or with regulated parties involved acting as agent or principal.

12.10 In the Wholesale Markets most participants have no knowledge of their customer's customer or, for example, the UBO of the asset being traded. In the Wwft there is no obligation to know your customer's customer. This means it is important that each

financial institution in the chain is correctly fulfilling its obligations in relation to CDD for its own customer. While this is not unique to this sector, it is particularly important here, as trading chains often have multiple layers, involve complex products with many players and are often cross-border.

12.11 However, the characteristics of traded products, which facilitate the rapid and sometimes opaque transfer of ownership, and the ability to change the nature of an asset and market mechanisms that potentially complicate the audit trail, together with a diverse international customer base, present specific money laundering risks that need to be addressed and managed appropriately.

12.12 Given wholesale markets' global flows of funds, speed of transactions and potential ease of converting holdings to cash, they are capable of being used for money laundering, but it is important to recognise that these markets may be abused by criminals at different stages of the money laundering process and that the risks of money laundering in the wholesale markets may vary, depending on the products and services a bank offers to a customer. It is important for a bank to understand at which stage(s) risks may arise (and this may vary from bank to bank):

- Placement: It is unlikely that cash or bearer instruments could be placed into the wholesale financial markets, as the primary acceptance of such assets is not a service offered by banks carrying out business in the NL within this sector.
- Layering: The wholesale financial markets grant the means to execute and clear a chain of transactions that may be complex, involving a multitude of financial instruments and/or financial institutions. This environment may potentially be abused by a criminal to layer funds and/or asset ownership with an aim of obfuscating the illicit origin of such funds/assets. The bank should be aware of common methods that are highly suggestive of financial crime such as ‘mirror trading’, ‘wash trading’ or ‘offsetting transactions’. A bank should also consider whether it facilitates the electronic transfer of funds into the wholesale market sector from an outside source, particularly from a third party or jurisdiction considered to present a higher risk for money laundering.
- Integration: Some financial instruments transacted on the wholesale markets can be rapidly liquidated to cash or reinvested into other holdings. A bank may then facilitate the further integration of these funds through the purchase or

transfer of other existing assets. While these activities are generally legal and legitimate, banks should consider the associated and varied money laundering risks when a customer instructs the transfer of value (by payment or change of asset ownership) to an overseas jurisdiction, particularly where a third party is involved.

- Post-integration (use of criminal proceeds): It can be very difficult to identify proceeds of crime once they have been integrated and mixed with legitimate funds in wholesale market products. Once proceeds of crime have been integrated in this way, it is likely that only the bank whose customer is the end party (and which would therefore have carried out CDD on that party) would be in a position to potentially identify such proceeds, by identifying any irregularity/inconsistency between the value of the transaction and its customer's source of wealth or funds (although such inconsistencies may, even then, be difficult to identify). Where the end party already has significant legitimate wealth, the use by that party of the proceeds of crime for investment purposes (rather than further layering of funds) will, again, be difficult to identify, even by the bank that has conducted CDD on that party as its customer.

12.13 Banks dealing in traded products in the wholesale markets do not generally accept cash deposits or provide personal accounts that facilitate money transmission and/or third-party funding that is not related to specific underlying investment transactions. Third party payments may, however, be used in relation to particular products, such as FX and/or commodities. Banks should consider whether third party payments are possible and whether the ability to make such payments presents additional money laundering risks and should into account the product specific guidance in this chapter where relevant.

12.14 OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in assessed lower risk jurisdictions, are transparent and have a CCP to clear trades, can ordinarily be carrying a lower generic money laundering risk. OTC business will, generally, be less transparent, and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. For example, exchanges often impose specific requirements on position transfers, which have the effect of reducing the level of money laundering risk. These

procedures will not apply in the OTC markets, where banks will need to consider the approach they will adopt in relation to any such requests in respect of customers dealing OTC. Trades that are executed as OTC but are then centrally cleared may have a different risk profile to trades that are executed and settled OTC. Hence, when dealing in the OTC markets banks will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

### Risk assessment

12.15 The main factors to consider in assessing the risk when undertaking business in the wholesale markets are: the nature of the customer; the market participants; the financial products and services involved; and whether the products are exchange traded or OTC.

12.16 When implementing a risk-based approach, producing or reviewing risk assessments, or assessing the risk profile of a prospective customer, there are several areas that banks may want to consider in addition to the more general matters set out in Part I.

- Wholesale markets are populated by customers with a wide range of different business interests. The types of participants present might typically include, but are not limited to:
    - Sovereign governments;
    - Local authorities;
    - Regulated financial firms (e.g. banks, brokers, investment managers and funds);
    - Unregulated financial entities (e.g. off-shore funds);
    - Corporations (e.g. listed companies, private companies); or
    - Trusts and partnerships.

- A customer’s nature, status, and the degree of independent regulation to which it is subject may affect the bank’s assessment of risk for the customer or for the bank's business.

- The instruments traded in the wholesale markets can allow for long-term investment, speculative trading, hedging and physical delivery of certain financial instruments and commodities. Understanding the role of a prospective customer in the market, and the customer's reasons for

trading, will help to reach informed decisions on the risk profile the customer presents.

- The way that a bank addresses the jurisdictional risk posed by a customer will depend on several factors. Jurisdictional risk should be considered but may, in relevant cases, be mitigated by the rationale for the customer being located or operating in a particular jurisdiction; customers located in potentially higher risk jurisdictions may have legitimate commercial interests which can mitigate the perceived risk, and presence in a higher risk jurisdiction does not necessarily render a customer high risk for AML/CTF purposes. For example, an oil producer in a higher risk territory may seek to use derivative instruments to hedge price risks and this does not necessarily present a high money laundering risk.

- Banks should ensure that any factors mitigating jurisdictional or other risks of a customer are adequately documented and periodically reviewed in the light of international findings or developments, and due diligence gathered as part of ongoing monitoring.

- Banks should take a holistic view of the risk associated with a given situation and note that the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

- For discussion of other risk areas banks may need to consider, such as corruption risk, see paragraph 12.19.

12.17 When dealing on an exchange or trading platform, a bank needs to identify its counterparty (paragraph 12.20-12.41 below describes who should be subject to CDD) and consider any associated risks:

- Where there is a CCP, a bank must assess the risks associated with the exchange.

- If there is no CCP, a bank will need to perform due diligence on the party with whom it deals - even if their name is not known until after the trade - before the trade is settled.

- While trading on an exchange or trading platform, a bank may execute a trade with a member who does not have an account with the bank. A bank should consider obtaining,

from the exchange or trading platform, a list of members and either identify and verify them upfront (to avoid possible delays in settlement) or on a case-by-case basis.

12.18 Product risk should also be taken into consideration. Transactions that give rise to cash movements (such as those associated with structured products) may present an increased money laundering risk, although this risk may be mitigated by the nature and status of the customer and the depth of the relationship the customer has with the bank. For example, if the use of a product (or service) is part of a wider business relationship and is compatible with other activity between the bank and the customer, the risk may be reduced.

12.19 While assessing ML/TF risks, banks will also wish to assess other factors such as reputational risk, sanctions risks and bribery and corruption risks. For example:

- New customers and payments on behalf of customers to third parties will typically need to be screened for sanctions purposes, and new additions to sanctions lists checked against existing customers, in line with the bank's approach to sanctions compliance.

- Banks should assess whether they have a due diligence requirement with respect to any introducing brokers who introduce new customers or other intermediaries and consider whether there are any red flags in relation to corruption risks.

## Customer due diligence

### *About the customer*

12.20 The bank should ensure that it fully understands the customer's legal form, structure and ownership, and must obtain sufficient additional information on the nature of its business, and the reasons for seeking the product or service from the bank.

12.21 It is important to know and understand any associations the customer may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries etc.) and the individuals who may influence its operations (political connections

etc.).

12.22 It is important to distinguish the relationships that exist between the various parties associated with the transaction. The bank should be clear whether it is acting as principal, or agent on behalf of the customer, and whether the bank has a responsibility, on a risk-based approach, to verify the identity of any underlying customers of parties involved in transactions.

12.23 Where the bank's customer qualifies for simplified due diligence see Part I, Chapter 2. Therefore, from an AML/CTF perspective, as a rule of thumb please refer to Part I, Chapter 2

- If the bank is acting as principal with another exchange member, the exchange member is the bank's customer.

- As discussed in paragraph 12.17 above, where an exchange-based trade is randomly and automatically matched with an equal and opposite exchange-based trade, it is recognised that, due to market mechanisms, the name of the other exchange member(s) may not be known. In these situations, where all the parties are members of the exchange and there is a CCP to match and settle the trades, the bank cannot know and therefore does not need to identify the other exchange member. Banks should, however, include the money laundering risk involved in the participation in any exchange or centralised clearing, as part of their overall risk-based approach. Participation in any exchange or centralised clearing system does not remove the need to adequately verify its own customer if the bank is dealing as agent for a customer.

- Where a bank is acting as principal with a non-exchange member, the non-exchange member is the bank's customer.

- Where a bank executes a trade OTC with a customer, which is then centrally cleared, and settled by the CCP, the bank has visibility of the customer and may need to verify the identity of the customer with whom they contract. By contrast, the CCP would not be a customer of the bank, and as such the bank would not be required to conduct due diligence on the CCP from an AML/CTF perspective. In certain situations, the bank may open customer accounts at the request of a CCP, in which case due diligence obligations would arise.

However, this would only occur in a default management scenario, and such arrangements would be documented in a separate customer agreement with the CCP.

- Where a bank is acting as agent for another party, the party for whom the bank is acting will be the bank's customer.

- Where the bank is transacting with a counterparty trading as agent for underlying entities, the counterparty will be the customer of the bank.

- Where the bank is performing services on behalf of an investment manager, the investment manager is the bank's customer. An investment manager may itself be acting on behalf of an underlying entity, such as a fund, to whom it may provide advisory or discretionary investment management services. Whether CDD is performed on the underlying entity will depend on the bank's customer relationship with both entities and the nature and status of the investment manager. Where a bank takes instruction from an underlying entity, or where the bank acts on the underlying entity's behalf (e.g. as a custodian), the bank then has an obligation to carry out CDD measures in respect of that underlying entity.

12.24 Accordingly, when determining whether CDD should be performed on the underlying entity, banks may wish to undertake a risk assessment that includes consideration of whether:

- The investment manager or the underlying entity is the instructing party (e.g. does the investment adviser/manager have discretionary trading authority and full control to instruct transactions);

- The investment manager is incorporated in a jurisdiction assessed by the bank as lower risk;

- The investment manager is subject to and supervised for compliance with equivalent AML/CTF system to the EU (please refer to the list of recognised regulators in Annex II in Part I); and/or

- The product or service is assessed, by the bank, as lower risk.

12.25 In circumstances where the bank determines that CDD should be performed on the underlying entity, the bank may consider reliance with regards to CDD on the underlying entity.

12.26 Where a bank is receiving services from a counter-party broker, the bank is the customer of the counter-party broker and it is not required to conduct CDD on that broker (although it may decide, on a risk-based approach, that some form of due diligence is appropriate).

12.27 An introducing broker may “introduce”, or a Receiver and Transmitter of orders may pass orders from, his customers to a bank to execute trades. This introducing broker may possibly perform related requirements in connection with the customers’ trades and bookkeeping and record keeping functions. The bank pays a fee to the introducing broker, usually based on the transactions undertaken. A customer often has no say in which bank the introducing broker selects to execute a trade. As such, the customer being introduced is a customer of both the introducing broker and the bank.

12.28 A non-clearing member of an exchange may maintain one or several accounts with a clearing member. Where a non-clearing member deals as agent for a customer, this may be through an omnibus account with the clearing member on behalf of all the non-clearing member’s underlying customers, who often have no say in the non-clearing member’s selection of a clearing member.

- Where a non-clearing member deals on a proprietary basis as principal, it will generally operate a separate account for such business. In that case the non-clearing member will be the customer of the clearing member.

- The clearing member may, based upon his risk-based approach and/or the status of the non-clearing member, consider that the non-clearing member’s underlying customer or customers are also his customers.

12.29 Customers wishing to execute and clear transactions on regulated markets may do so using separate executing and clearing brokers. To complete such a trade, the executing broker will execute the order and then ‘give-up’ that transaction to the clearing broker for it to be cleared through the relevant exchange or clearing house. This arrangement may commonly take the

form of a tri-party agreement between the customer, the executing broker and the clearing broker. However, give-up arrangements can extend to cover several different types of relationships.

12.30 Where a bank acts as executing broker, the party placing the order is the customer for AML/CTF purposes.

12.31 Where a bank acts as clearing broker, the customer on whose behalf the transaction is cleared is the customer for AML/CTF purposes. A clearing broker typically has a more extensive relationship with the customer as they may also act as custodian.

12.32 Where an executing broker and a clearing broker are involved in a 'give up' arrangement, the executing broker may, as part of its risk-based assessment, consider it appropriate to place reliance on the clearing broker.

12.33 In some cases, other parties, who are not customers, may be linked to a transaction. A bank may, however, still wish to assess them as part of its own due diligence and to guard against reputation, sanctions and bribery and corruption risks (e.g., introducing brokers, particularly in higher risk jurisdictions, for the reasons described above in paragraph 12.27).

*Distributors*

12.34 Banks who use third party distributors to distribute, sell and/or market products will generally have a customer relationship with the distributor, rather than the underlying entity (who is the customer of the distributor).

12.35 Banks must carry out CDD on the distributor in accordance with the provisions of Part I and should consider seeking information and/or assurances about the distributor's own AML/CTF procedures. The bank can also seek contractual protections in the distribution agreement.

*Arranger of structured products contracting via custodians*

12.36 In one scenario, an arranger (who may also be described as an "introducer" or "retrocession agent") may approach a bank to request, on behalf of an undisclosed customer, a quote for a structured product with a set of features (e.g. reference

assets/indices, capital guarantee, maximum upside, etc.). If this quote is acceptable, the arranger will then recommend the structured product to their customer. The arranger's customer will typically instruct their custodian bank to purchase the structured product from the bank. The custodian bank will purchase, on an execution-only basis, the structured product as principal, settling directly with the bank. The bank then pays the arranger a fee, which is non-standardised and negotiated on a transaction by transaction basis. Alternatively, the bank may approach the arranger with a structured product that the arranger's customers may be interested in (although transaction flows remain the same as above).

12.37 In some cases, the arranger may act with a power of attorney from their customer and thus have authority to purchase the structured product on behalf of the customer. The bank should ascertain whether the arranger is acting under a power of attorney or not. Settlement of the transaction will be affected, by the bank, with the custodian bank of the undisclosed customer, as outlined above.

12.38 In NL, an arranger is required to be regulated and registered. However, depending on local legislation, an arranger may or may not be required to be regulated in their country of domicile or of main operation, which may be different.

12.39 In each of the scenarios outlined above, the arranger must be subject to CDD. The bank should check that the arranger satisfies the authorisation requirements (if any) of the arranger's country of domicile or of main operation. The bank should also consider obtaining details of the career in the financial services industry of each of the main employees or principals of the arranger.

12.40 In addition, if the custodian bank cannot be subject to simplified due diligence or is not otherwise regarded as posing a lower risk, the bank will also have to look through to the custodian's underlying customers (the UBOs).

12.41 Banks should consider, if an arranger requests that his fee be paid to a bank account held in the name of an apparently unrelated third party or to an account at a bank in a country with no obvious connection to his country of domicile or of main operation, whether such requests give rise to suspicions of

bribery, corruption or tax evasion. Banks may wish to consider introducing a policy of paying fees only to a bank account in the name of the arranger that is held at a bank in the country of the arranger's domicile or a country of main operation. Banks may also wish to confirm that there is full disclosure of any fees on relevant documentation for each transaction.

12.42 Banks should also be alert to the risk that an arranger who is an individual may be carrying on their own personal business while still employed by, and managing the affairs of customers of, another financial institution such as a bank, asset manager or wealth manager. The arranger may be acting in their own name or via a corporate entity that they control. If, because of its CDD, the bank has suspicions that an arranger may be currently employed by a financial institution, the bank should contact the financial institution concerned to ascertain whether the individual is employed by them and, if so, that they are content with the proposed relationship between the bank and their employee. Similar suspicions may also arise where all of an arranger's customers use the same custodian bank.

*Expected activity*

12.43 A bank will, as part of CDD, assess, and where appropriate obtain information on, the purpose and intended nature of the customer relationship and/or transaction. This information will assist banks when assessing whether the proposed relationship is in line with expectations and will support ongoing monitoring. The key consideration is being able to identify whether the customer's activity (for example: transaction size and frequency) is in line with the bank's knowledge of the customer. The bank will, in many cases, be able to infer the customer's expected activity from the nature of the customer itself (e.g. regulated financial institutions can generally be expected to trade products consistent with the typical operating model of such an institution).

12.44 Customers will typically have multiple brokers and deal in a multitude of products and asset classes and their strategy may be dependent on market conditions, which may influence changes in activity.

*Source of funds*

12.45 A bank should, where appropriate, identify and verify the source of funds to understand the origin of the funds involved in the business relationship and/or occasional transaction. Whether the identification and verification of a customer's source of funds is required will depend on the nature and status of the entity wishing to execute and clear wholesale markets transactions. The bank may decide, on a risk-based approach, to obtain specific evidence of the source of funds.

12.46 In situations where the customer takes the form of a privately-controlled, unregulated entity (including, in particular a private investment company, SPV or family office) the risk is likely to be assessed as higher, and in cases which present a higher ML/TF risk, the source of funds for a business relationship or occasional transaction should be identified and, on a risk-based approach, verified by the bank in order to reasonably satisfy itself that the origin of the funds is legitimate.

*Monitoring and surveillance*

12.47 Guidance on general monitoring requirements is set out in Part I. Monitoring in wholesale markets will be affected by the fact that banks may only have access to part of the overall picture of their customer's trading activities. The fact that many customers spread their activities over several financial firms will mean that many banks will have a limited view of the entirety of a customer's trading activities. Extreme market conditions may also impact a customer's trading strategy and the commercial rationale for a particular transaction will often be linked to market conditions. There are, however, specific characteristics of the wholesale market sector that will impact a bank involved in the wholesale markets monitoring activity. These include:

- Scale of activity: Wholesale markets involve very high volumes of transactions being executed by large numbers of customers. The monitoring activity undertaken should therefore be adequate to handle the volumes undertaken by the bank.
- Use of multiple brokers: Customers may choose to split execution and clearing services between different financial firms and many customers may use more than one execution broker on the same market. The customer's reasons for this include ensuring that they obtain best execution, competitive rates, or to

gain access to a specialism within one financial firm. This will restrict a bank's ability to monitor a customer, as they may not be aware of all activity or even contingent activity associated with the transactions they are undertaking.

- Electronic execution: Increasingly, electronic order routing is used where customers access markets directly and there is little or no personal contact between the bank and the customer in the day-to-day execution of the customer's business. This means that the bank may not know the rationale for transactions.

12.48 The nature and extent of any monitoring activity will therefore need to be determined by a bank based on an assessment of its business profile. This will vary for each bank and may include an assessment of the following matters:

- Extent of execution vs clearing business undertaken;
- Nature of customer base (geographic location, regulated or unregulated);
- Number of customers and volume of transactions;
- Types of products traded and complexity of those products; and/or
- Payment processes (including payments to third parties, if permitted).

12.49 Banks should ensure that any relevant factors are considered in determining their monitoring activities, and that the programme is adequately documented and subject to periodic review on an ongoing basis.

12.50 Banks may wish to leverage existing surveillance frameworks established for the purposes of compliance with the Market Abuse Regulation (MAR), to assist in monitoring certain wholesale markets activities for unusual transactions that may constitute financial crime.

## Guidance on specific products Securities

### *General guidance for Securities*

#### *Product specific risks*

12.51 Securities are typically regarded as a lower risk asset class and are a typical product traded on the wholesale markets. Banks should, however, be aware of the risk of insider dealing and market abuse (and the subsequent laundering of the proceeds of

such offences) in the context of securities trading.

*Who is and is not the customer?*

12.52 Customers wishing to transact securities on a Delivery vs. Payment (DVP) basis may do so through an executing broker that will generally settle with the customer's settlement agent/custodian. Under this arrangement, the customer elects to execute transactions through an executing broker and to clear the transaction through a separate settlement agent/custodian. The orders can either be placed directly by the customer or by an agent on behalf of the customer. Once the transaction is executed, the executing broker will settle with the settlement agent/custodian simultaneously once payment is received.

12.53 Both the executing broker and the settlement agent/custodian will have a relationship with the customer.

12.54 It is usually (but not always) the customer that elects to execute transactions through one or more brokers and to clear such transactions through a settlement agent/custodian and, to that end, selects both parties.

12.55 Where a bank acts as executing broker, the party placing the order is the customer for AML/CTF purposes. Where the party placing the order is acting as agent for underlying entities, they, too, may be customers for AML/CTF purposes. In this context, banks should have consider paragraphs 12.23 to 12.26 of this chapter.

12.56 Where a bank acts as settlement agent/custodian, the customer on whose behalf the transaction is executed is the customer for AML/CTF purposes.

12.57 A common additional participant in a DVP arrangement is the customer's investment adviser or manager, to whom the customer has granted discretionary trading authority. Where a bank is acting as executing broker and an investment adviser or manager is acting for an underlying entity, the type of/or level of CDD measures performed, and whether there is an obligation to identify the underlying entity, will depend upon the regulatory status and location of the adviser or manager. When considering whether it is necessary to undertake CDD on the underlying entity, banks should consider paragraphs 12.24 and 12.25 of this

chapter.

*Customer due diligence*

12.58 Where the underlying entity is considered to be subject to CDD by the executing broker, a risk-based approach to CDD can take into account the investment manager and/or the settlement agent/custodian supervised by a regulator from the EEA or countries having an equivalent AML/CTF system to the EU. This may reduce the identity information or evidence requested and what the bank verifies. Banks should take the relationship with the Investment Manager and settlement agent/custodian into account in their own CDD on customers, rather than place full reliance on the settlement agent/custodian.

12.59 Given the information asymmetries likely to exist between an executing broker and settlement agent/custodian, when a bank is acting as settlement agent/custodian it would not be appropriate, from a risk-based perspective, to rely on an executing broker. Settlement agents/custodians should undertake the CDD measures as set out in Part I.

12.60 Where transactions are settled on a free of payment basis (e.g. non-DVP), banks should ensure that they understand the commercial rationale for this arrangement.

12.61 Where suspicion of market abuse behavior needs to be checked, it might well be the case that these transactions are not only manipulating the market but also used for ML reasons. Therefore banks should also ensure that measures are taken and transactions/ financial instruments are checked against potential ML related pourposes and in the event of findings the local conduct regulator (in NL AFM) is informed and a STOR (Suspicious Transaction Order Report) is duly filled out.

## *Money market instruments*

*Product specific risks*

12.62 "Money Market Instruments" is the term used to collectively cover foreign exchange (FX), interest rate products and term deposits. These instruments will typically be traded in the wholesale market between regulated financial institutions and large corporates (listed and private) and the money laundering risk may therefore

be viewed as generally lower. However, this risk may be increased by matters such as:

- The nature of the customer (e.g. the customer's business);
- The customer's regulatory status (e.g. a sophisticated private investor);
- The purpose of the trading (e.g. hedging may be regarded as lower risk than speculative transactions);
- Requests for payments to be made to third parties: for example, customers, particularly corporates that need to make FX payments to suppliers and overseas affiliates.

12.63 When assessing the money laundering risk in such circumstances, a bank may want to consider the nature of the customer's business and the frequency and type of third party payments that are likely to result from such business.

*Customer due diligence*

12.64 FX (as well as many other traded products) is commonly traded on electronic trading systems. Such systems may be set up by brokers or independent providers. When a bank executes a transaction in these systems the counterparty's identity is not usually known until the transaction is executed. The counterparty could be any one of the members who have signed up to the system. Banks should examine the admission policy of the platform before signing up to the system, to ensure that the platform only admits regulated financial institutions as members, or that the rules of the electronic trading system entail that all members are subject to satisfactory anti-money laundering checks, and identify its counterparty and any associated risks.

## *Financial derivatives*

*Product specific risks*

12.65 Financial products are used for a wide range of reasons, and market participants can be located anywhere within the world; banks will need to consider these issues when developing an appropriate and holistic risk-based approach. The nature, volume and frequency of trading, and whether these make sense in the context of the customer's and bank's corporate and financial status, will be key relevant factors that a bank needs to consider when developing an appropriate risk-based approach. Banks should also consider whether the derivative to be traded is

consistent with its understanding of the customer's expected activity.

12.66 Where banks are trading commodity futures, they should be mindful of the fact that physical delivery may be required.

12.67 Some derivative products may be complex in nature and linked to a chain of underlying assets. On this basis, where the bank is facilitating the trade of a derivative product, it is not expected to have knowledge of the specific asset underlying the derivative.

## Commodities

### *Product specific risks*

12.68 Banks that, in addition to physical commodity activity, undertake any business with a customer, which amounts to a regulated activity (including business associated with physical commodities) will be subject to CDD on the customer.

12.69 When implementing a risk-based approach and performing a risk assessment on a (prospective) customer, there are several areas that commodity market banks may want to consider in addition to the more general matters set out in Part I. These will include, but are not be limited to:

- The wide range of different business interests that populate the commodity markets. The types of participants may typically include:
    - Producers (e.g. oil producers and mining firms);
    - Users (e.g. refiners and smelters);
    - Wholesalers (e.g. utility firms);
    - Commercial merchants, traders and agents; and
    - Financial institutions (e.g. banks and funds).

- The above-mentioned types of firms are illustrative and widely drawn and can be present in more than one category (for example, a refiner will be both a user of crude oil and a producer of oil products).
- The instruments traded in the wholesale commodity markets can allow for the speculative trading, hedging and physical delivery of commodities.
- There may be third party funding of transactions in the commodities markets. Also, where a bank is transferring funds to a customer to purchase a physical commodity

and the customer hedges the risks associated with the transaction in the derivatives market through a broker, the bank may guarantee the payment of margin to that broker; this results in a flow of money between the broker and the bank on the customer's behalf. However, both the party making the payment on behalf of the customer, and the party receiving the funds, will be regulated financial institutions.

- Banks should also consider whether it is necessary to assess the potential higher risk of corruption, money laundering, fraud or sanctions issues associated with extractive industries or governmental licences in higher risk jurisdictions through its CDD processes.

12.70 The risks and potentially mitigating factors should be considered. The global nature of the commodity markets means that customers from potentially higher risk jurisdictions with a perceived higher money laundering risk are likely to have legitimate commercial interests. Understanding the role of a prospective customer in the market, and their reasons for trading, will help to reach informed decisions on the risk profile they present.

12.71 When undertaking commodities business, banks should take into account any relevant trade sanctions.

*Who is and is not the customer?*

12.72 Where business does not fall within the scope of the AML/CTF regulations, e.g. shipping and chartering, it is entirely a matter for the banks to decide what commercial due diligence they perform on their counterparties, and what due diligence they may wish to undertake to mitigate ML/TF and other financial crime risks (e.g. for the purposes of complying with applicable sanctions regimes).

## Structured products

*Product specific risks*

12.73 Structured products are financial instruments specifically constructed to suit the needs of a particular customer or a group of customers. They are generally more complex than securities and are traded predominantly OTC, although some structured notes are also listed on exchanges.

12.74 There is a wide range of users of structured products. Typically, they will include:

- Corporates;
- Private banks;
- Government agencies; and
- Financial institutions.

12.75 The money laundering risk associated with structured products is not generally considered to be high, because of the involvement of regulated parties and because trading in structured products is unlikely to be a particularly effective way to launder criminal proceeds. However, because of the sometimes-complex nature of the products, they may generally be more difficult to value than cash securities. This complexity may make it easier for money launderers, for example, to disguise the true value of their investments. Banks should therefore remain mindful of their obligations when trading in structured products and ensure that they carry out EDD where red flags are identified.

12.76 The complexity of the structure can also obscure the actual cash flows in the transaction, enabling customers to carry out circular transactions. Understanding the reason behind a customer's request for a product will help banks to assess the money laundering risk inherent in the structure.

*Who is and is not the customer?*

12.77 Transactions are usually undertaken on a principal basis between the provider (normally a financial institution) and the customer. Some structured products are also sold through banks and third-party distributors (arrangers). In the latter circumstances, it is important to clarify where the customer relationships and responsibilities lie (e.g. are the third parties introducing the customer to the bank or distributing products on behalf of the bank) and to set out each party's responsibilities in relation to AML/CTF.

# Chapter 13

# Brokerage Services

## Introduction

For the following guidance in relation of Brokerage Services whenever the term “Bank” is used it should be understood that this activity is performed by an authorised regulated broker dealer.

### *Overview of the sector*

13.1 A fund is a vehicle established to hold and manage investments and assets. A fund usually has a stated purpose and/or set of investment objectives. Funds may be regulated or unregulated, listed or unlisted, open or closed-ended, and targeted at retail, an eligible counterparty or other investors. The provision of brokerage services to funds may therefore pose a wide spectrum of money laundering risks, from low to high, see section ML/TF risks associated with funds 1.2 below. It is important to draw a distinction between funds that are personal investment vehicles (which may be set up and/or managed by private wealth managers) and those set up for a commercial purpose with, usually, unrelated investors (e.g. hedge funds) although, as both types of funds can use the same structures, the line between the two may sometimes be hard to distinguish.

13.2 Funds will normally be separate legal entities, formed as limited companies, limited partnerships or trusts (or the equivalent in civil law jurisdictions), so that the assets and liabilities may be restricted to the fund itself. Sub-funds of an umbrella fund typically take the form of different classes of shares, fund allocations to separately incorporated trading vehicles or legally ring-fenced portfolios. Sub-funds may or may not be separate legal entities from their umbrella fund. The investors in the funds are the UBOs of the fund and its source of funds.

13.3 Funds may also operate a “master/feeder” arrangement, whereby investors, typically from different tax jurisdictions, invest via separate feeder funds that hold shares only in the master fund.

The most common set up is to have an onshore feeder for taxable investors and an offshore feeder for foreign or tax-exempt investors. Feeder funds may also on occasion invest/deal directly and therefore a bank may provide services to a fund that is acting on its own behalf while at the same time being a feeder fund of another (master) fund.

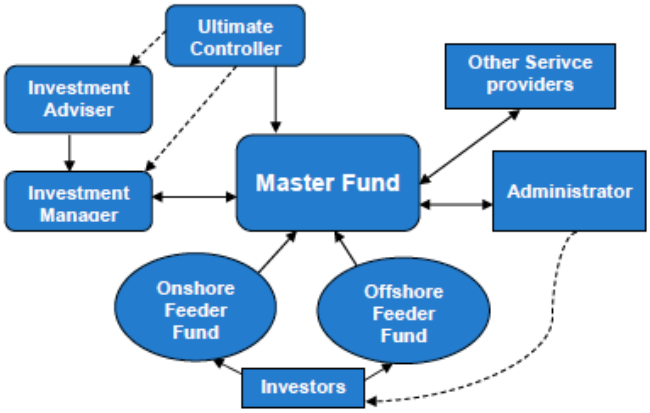
13.4 Dependent upon a fund's structure and legal form, the power to make decisions and provide instructions on behalf of a fund may rest with its directors, partners or trustees. However, in most instances the powers of the directors, partners or trustees will be delegated to the investment manager. It is not unusual to find that the key staff members of a fund are also the key staff members of the investment manager.

13.5 The complexity of the structures and multiple relationships associated with funds can often give rise to uncertainty. It is, therefore, critical that a bank establishes who it is dealing with, establishes whether that party is acting on its own behalf or on behalf of an underlying customer, and generally understands which parties may present a ML/TF risk in the relationship. Once these questions have been answered, the precise steps to identify and verify the relevant parties will vary in each case.

13.6 The following diagram illustrates some of the key players in a fund, specifically a master feeder fund structure.

13.7 The fund’s prospectus, offering memorandum or other document will set out the details of the fund structure, appointed service providers - the investment manager, administrator, prime broker, lawyers and auditors - together with a summary of the material contracts such as the administration, investment management and prime brokerage agreements.

13.8 Note that the precise structure in each case will vary and some of the responsibilities of each function outlined below may sometimes be amalgamated.




Note: both the administrator and investment manager will usually act for the underlying feeder funds.

*Ultimate controllers*

13.9 Funds may or may not have an "ultimate controller". In terms of day to day control, as explained above, the power to make decisions and provide instructions on behalf of a fund may rest with its directors, partners or trustees; and in most instances will be delegated to the investment manager (see below) who will take investment decisions with respect to the assets of the fund and place orders with the bank on behalf of the fund.

13.10 The investors in the fund (who are the UBOs of the assets within the fund) will not usually have control over the fund or its decision-making. However, in some cases, there may be one or more individuals who ultimately exercise control over the fund or its management (for example, having the right to replace its management or to direct the sale or purchase of assets). In personal investment vehicles in particular there may be voting shareholders, directors or holders of founding shares with such powers. The place to look for those who are the ultimate controllers is usually the fund's offering memorandum. Banks should, where appropriate, also consider relevant legal agreements and ask who has control: any ambiguity suggests further due diligence is necessary.

*Investment manager*

13.11 Funds are managed by an investment manager, who is a separate legal entity to the fund, and who is typically given authority to act as agent and manage the funds and investments held by the fund vehicle. It is often the investment manager that will take investment decisions and place transactions with the bank on behalf of the fund.

13.12 The investment manager plays a pivotal role in establishing and maintaining the relationships with the prime broker and the clearing and executing brokers and will, in most cases, be the direct contact with the bank on behalf of the fund. A bank may also act as investment manager to a fund in addition to providing other services.

13.13 The bank must review the investment management agreement to understand the scope of the manager's authority/control.

13.14 Investment managers will usually be regulated but, depending upon the jurisdiction they are registered in or operate from, they may be subject to varying degrees of regulatory oversight. Banks must, therefore, satisfy themselves of the regulatory status and responsibilities of investment managers, in particular with respect to AML/CTF.

13.15 "Recognised Regulated Investment Manager" refers to an investment manager who is regulated by a regulator from the EEA or country with an equivalent AML/CTF system (see Recognised Regulators List in Part I, Annex II).

13.16 The relationship the investment manager has with investment advisers, with the directors (or equivalent) of the fund, and with the ultimate controllers of the fund (if any), will vary depending upon the degree of control the investment manager has over the:

- Selection of investors (including compliance functions e.g. CDD or related checks);
- Investment strategy of the fund; and
- Placement of orders.

13.17 A fund may have more than one investment manager, known as sub-managers. Sub-managers are responsible for

managing/investing part of the fund, and, depending on the structure of the fund, there may be more than one sub-manager. Where investment management making decisions are delegated to sub-manager(s), depending on the nature of the bank's interactions with the sub-manager, CDD measures may be required to be performed on the sub-manager as well as on the investment manager (subject to the possibility of relying on the investment manager, in appropriate cases, as explained more fully in Reliance on third parties section 13.81).

*Investment adviser*

13.18 Some funds appoint separate investment advisers who will advise the investment manager with regard to investment decisions undertaken in relation to specific financial instruments or markets, and on occasion, depending on the delegated duties, may place orders with the bank. Depending on the nature of the bank's interactions with the investment advisor (in particular, if they have authority to place orders on behalf of the fund), CDD measures may be required on the investment adviser.

*Administrator*

13.19 Administrative services such as the day-to-day operation of the fund (e.g. valuations) and routine tasks associated with managing investments on behalf of investors (e.g. managing subscriptions and redemptions) will ordinarily be undertaken by a separate entity known as the fund administrator. Fund administrators may also perform the role of transfer agent and registrar. An administrator may also be responsible for performing CDD on the investors.

13.20 Fund administrators are often regulated / licensed but their responsibilities may vary (e.g. depending on the domicile of the fund). The responsibilities of the administrator are normally outlined in the offering memorandum/prospectus.

13.21 The regulatory status and responsibilities of the administrator, in particular with respect to AML/CTF compliance, may be relevant to the bank's assessment of ML/TF risk. In some cases, however, the investment manager may be responsible for the appointment of the administrator and may retain responsibility for compliance with AML/CTF laws and regulations, being required to provide oversight of the outsourcing arrangement with the administrator

to ensure that the manager's regulatory standards are applied. In such cases, the regulatory status of the investment manager and oversight arrangements may be more relevant to AML/CTF risk than the regulatory status of the administrator.

*Distributors*

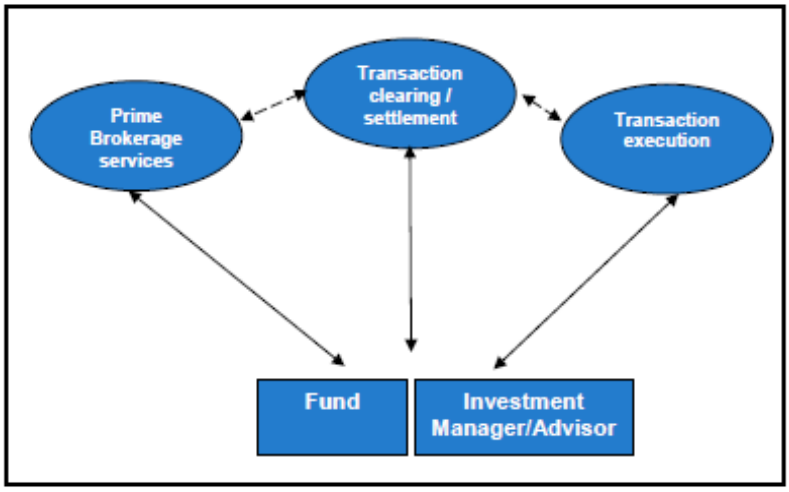
13.22 Some funds (and their managers on their behalf) may use third party distributors to distribute, sell and/or market their shares/units, particularly where the fund is marketed to retail investors. In some cases, the fund may have a customer relationship with the distributor, rather than the underlying investor (who is the customer of the distributor) or may rely on the CDD undertaken by the distributor.

13.23 From the perspective of banks providing brokerage services to the fund, understanding the nature of its distribution arrangements may be relevant in understanding its AML/CTF risk profile – for example, understanding the geographies of its operations or the type of distributors to which the fund is marketed may provide relevant information about the investor base.

*Other relationships*

13.24 In addition to the above-mentioned entities, who are involved with the operation and management of the fund, other parties may also be involved, such as auditors, law firms, trustees, and custodians. Diligence on these parties may not be necessary for a bank to meet its AML/CTF and sanctions-related obligations. On a risk-based approach a further understanding of the roles and identities may give a more complete picture of the fund set-up.

13.25 The following diagram sets out the likely services a bank may provide to a fund (although, as discussed above, the bank could deal with the fund via a number of entities).




*Transaction Execution*

13.26 Transactions or trading are undertaken for a fund by an executing broker. A fund may elect to execute transactions through one or more brokers. The executing broker takes instructions from the fund or its appointed agent (usually the investment manager), but passes the transactions/trades to a clearing broker for clearing and settlement.

- An executing broker may give up a transaction to a clearing broker for settlement.
- In transactions that involve delivery vs payment (DVP), cash or securities are swapped between the executing broker and settlement/clearing agent or, on occasion, the custodian.

13.27 An executing broker should be clear with whom they are interacting (i.e. who gives the orders) and in what capacity, in order to determine whom they are facing.

13.28 The executing broker typically provides execution-only services to the investment manager and settles with a regulated prime broker(s). The AML/CTF risk for the executing broker in these scenarios will be with the fund or its appointed agent (usually the investment manager).

*Clearing/Settlement*

13.29 A fund may elect to execute transactions through one or more brokers and elect to settle or clear such transactions through another broker, known as the clearing broker. The clearing broker will settle the transaction/trades on behalf of the fund.

*Prime brokerage services*

13.30 Prime brokerage is the term used to describe the provision of a tailored package of markets products and services to a fund. Services offered by prime brokers include custody, reporting, securities lending, cash lending and pricing (i.e. valuation services). Some prime brokers provide capital introduction, start-up services, credit intermediation, straight-through processing, futures and options clearing, research, contracts for difference and credit default swaps. Although prime brokers can offer an array of services, it is not uncommon for funds to appoint more than one prime broker as they see fit and for those prime brokers to be involved in transactions together on behalf of the fund. The precise relationship will depend on the products and circumstances.

## ML/TF risks associated with funds

13.31 It is common, when providing brokerage services to funds in capital markets, for the funds to be managed on a discretionary basis by an Appropriately Regulated Investment Manager. In practice, this means that the party making investment decisions on behalf of the fund is subject to AML/CTF legislation equivalent to that applying in the EU.

13.32 However, certain characteristics of funds render them susceptible to money laundering and therefore a potentially attractive vehicle to place, layer and/or integrate criminal funds into the legitimate financial system. A fund may be established in various legal forms (including but not limited to: private companies, partnerships or legal arrangements) and may have a complex beneficial ownership structure. Consequently, a fund may appear to lack transparency of ownership and/or control, which may be attractive to a money launderer wishing to obfuscate identification.

13.33 Funds are often established on a global basis, processing cross-border money flows in and out of the fund, generally through subscriptions and redemptions. At times, these cross-border transactions may involve countries assessed to have a weaker AML/CTF framework and those associated with heightened secrecy laws, creating barriers for relevant authorities to trace and freeze criminal assets. Furthermore, the volume, size and strategy of a fund's trading activity may be complex and may therefore potentially be abused by a criminal to layer funds and/or asset ownership with the aim of concealing the illicit origin of such funds/assets.

13.34 A fund will typically utilise legitimate professional intermediaries to perform certain services for or on its behalf, to assist with market operations and/or general administration. A money launderer may echo this practice, employing corrupt professional intermediaries, nominees and/or corporate shell companies, with the aim of concealing criminal actor(s) and the origin of illicit gains.

*Risk assessment*

13.35 A fund's nature, status, and the degree of independent oversight to which it is subject should influence the bank's assessment of risk.

13.36 The risks can be determined through gathering information and undertaking appropriate CDD on the investment manager and, where applicable, the fund (as set out in  section below -Who is the customer from AML/CTF perspective?), and in particular through understanding to whom the fund is marketed and its structure and objectives, as well as the regulatory status, track record and reputation/standing of the investment manager and/or other relevant parties in control of the fund.

13.37 A bank should also consider, as part of its wider obligations with respect to financial crime and to mitigate reputational risk, whether there are any risk indicators that warrant further investigation. As part of this consideration, banks may wish to include, where relevant, whether the size and reputation of the service providers (administrator, investment manager, auditor, lawyers etc.) match the fund's profile.

13.38 While structures associated with funds are often complex and involve a number of jurisdictions, an important question is whether the structure makes sense. For example, determining if the fund has an unusual cross-border structure. Also, where an administrator is located in a jurisdiction not assessed as lower risk, or specific concerns have been identified, closer inspection of the administrator's due diligence activities and background should be considered.

13.39 A bank should take a holistic view of the risks associated with a given situation and note that the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category (See Part 1 Chapter 4).

13.40 Certain factors may be considered indicators that a fund may present a higher money laundering risk. The following is a non-exhaustive list of factors that may be considered indicators of higher risk:

- Investment managers, funds, investors or other relevant parties located in jurisdictions assessed as higher risk by the bank;
- Where there is an increased risk of sanctions exposure, for example funds with investors or investments in sanctioned jurisdictions;
- A stand-alone, self-managed or managed fund with the investment manager not being an Appropriately Regulated Investment Manager. This may make it more difficult to ensure that the AML/CTF requirements applied to investors are of an appropriate standard, as such the bank may not rely on third party CDD assesment and must perform their own CDD on the fund and the investment manager;
- Funds whose ownership structure is unduly complex as determined by the bank;
- Where there is doubt as to the identity of underlying parties. This includes cases in which an investment manager is unwilling to disclose a fund's legal name to the bank. This would also include cases in which the bank considers it appropriate, on a risk-based approach, to obtain information about the UBOs of the fund, but such information is withheld;
- Where a UBO or ultimate controller of a fund is disclosed and that person resides in a jurisdiction assessed as higher risk by the bank;

- Where the fund is formed for the benefit of a Politically Exposed Person (PEP) or relative or close associate, in particular when assessed by the bank as a higher PEP risk;
- If, during the course of conducting CDD, the bank uncovers adverse media relating to the fund or the investment manager, this may be an indicator of higher risk. Banks want to ensure they identify and are comfortable with, any potential risks relating to the adverse media, taking mitigating steps to address such risks where appropriate;
- If the fund takes the form of a privately-controlled entity (including, in particular, a personal investment vehicle, private investment fund or SPV) and there are doubts as to its source(s) of funds and/or a UBOs source of wealth;
- The investment strategy is unclear or too good to be true (in terms of growth);
- The type of investors the fund solicits raises questions;
- The fund allows redemption without limitation of time and amounts;
- The manner in which the interest/shares/units in the fund are being distributed raises questions;
- There is a small number of investors relative to the size of the fund;
- The investment of the fund has an innovative character;
- The investment object raises questions.

13.41 In addition to customer and jurisdictional risk factors, banks should consider product risk factors. The product risk will vary depending on the nature of activities carried out on behalf of the customer. For example, services where customer instructions are passed on, on a principal basis, to regulated institutions or exchanges may be considered lower risk from an AML/CTF perspective than services that require settlement of funds and/or financial instruments, or from services that require custody of securities and/or cash assets by the bank.

13.42 In particular, where a bank agrees to undertake third party payments on behalf of a fund, the risks of money laundering and fraud are increased. A bank should therefore ensure it has adequate procedures, systems and controls to manage the risk associated with those types of payments and receipts. A bank may wish to consider monitoring and/or undertaking periodic reviews of these types of payments and receipts, as well as ensuring appropriate levels of sign-off within the bank.

13.43 Generally, the status and reputation of other third parties associated with a fund (including service providers, such as other executing, clearing or prime brokers, administrators, trust and company service providers, auditors and/or law firms) may contribute to the risk assessment of the fund. The level of comfort and elements of risk will differ depending on the identity of the third party and its role; for example, whether the nature of its relationship would require the third party to undertake CDD measures on the fund.

13.44 Funds may also raise concerns regarding possible investment fraud and subsequent general duty of care obligations. Fraudsters may use investment funds to deceive third party investors. A well-known form of investment fraud is the so-called Ponzi scheme where investments are (partly) fictitious and dividend payments to or redemptions of existing investors are financed by deposits or subscriptions of new investors, rather than by profits obtained through real investment activities. Proceeds of these crimes may subsequently be laundered through bank accounts in the name of the funds involved. When dealing with a fund that turns out to be fraudulent there is also the legal risk that the bank may be (partly) held responsible for the losses of defrauded investors, even if those investors are not customers of the bank. This civil liability of the bank is based on a special duty of care that aims to protect the interests of third parties that may be harmed by a fraudulent fund when offering banking or other services to such a customer. Based on this duty of care the bank may be obliged to investigate signs of irregularities that may become evident when servicing a fund and to warn involved third parties of any knowledge it may have indicating possible fraud or deception. The bank may be deemed to have knowledge, if staff knows, or at least ought to know, that these transactions occur, also those that may harm the interest of third parties. Staff involved in servicing such customers thus needs sufficient ongoing awareness of fraud and money laundering risks, including third party liabilities (the burden of knowledge).

## Customer Due Diligence

### *Who is the customer from AML/CTF perspective?*

13.45 Who a bank should view as its customer, and to whom CDD measures should be applied, may vary according to the business

undertaken for a fund, the nature of the bank's relationship with the investment manager, and whether the investment manager is Appropriately Regulated.

13.46 A bank taking instructions from an investment manager will always be required to undertake CDD on the investment manager. Whether CDD measures must also be applied to the fund will depend on the nature of the bank's interaction with the fund. Where the fund is the bank's customer (e.g. where the bank takes instructions from it or holds its assets – see 13.50 customer relationship with the fund), the fund should be subject to CDD. Where the fund is not the bank's customer, CDD on the fund is not required, however identification and screening of the fund, its main principals, and if known to the bank, its beneficiaries is advised. Further enquiries may however be made and additional information sought on the underlying fund depending on the bank's assessment of the AML/CTF risk posed by the investment manager; depending on the level of risk assessed in relation to the investment manager, CDD on the fund may be advisable. The regulatory status of the investment manager will be a significant factor in that risk assessment. Therefore, where the investment manager is not Appropriately Regulated, banks will need to 'look through' and conduct due diligence on the underlying fund. Please see 13.53 table related to parties in respect of whom CDD measures are required to be carried out by the bank.

13.47 Regarding the assessment of ML/TF risk, it is common, when providing brokerage services to funds in capital markets, for the funds to be managed on a discretionary basis by an Appropriately Regulated Investment Manager. In such cases, it is customary that a contractual relationship exists between the bank and the investment manager and that the bank will receive instructions from the investment manager.

- Where the bank is providing brokerage services to an investment manager, the investment manager is the bank’s customer for AML/CTF purposes.
- Where an investment manager contractually delegates discretionary authority to act on behalf of a fund to a sub-manager, the sub-manager is a customer for AML/CTF purposes.

- In this context, whether CDD measures should also be applied to the underlying fund will depend on the nature of the bank's relationship with both entities, as explained below.

13.48 Wwft defines "correspondent relationships" as including relationships between and among credit and financial institutions, including where certain services are provided by a correspondent to a respondent, and including relationships established for securities transactions or funds transfers. The Wwft and the FATF recognise that correspondent relationships in the securities sector may include a relationship whereby a securities provider (correspondent) executing securities transactions on behalf of a cross-border intermediary acting as respondent for its underlying customers this is also known as "correspondent securities relationship".

13.49 Correspondent securities relationships exist in the context of providing brokerage services to funds; the broker (correspondent securities provider) may provide services to a domestic or cross-border intermediary, such as an Appropriately Regulated Investment Manager (respondent). Subject to compliance with applicable requirements relating to due diligence on the respondent/intermediary, a correspondent securities provider is not required to undertake CDD measures on the customers of the respondent/intermediary.

*Customer relationship with the fund*

13.50 Accordingly, in situations where a correspondent securities relationship exists within the context of providing brokerage services to funds, the underlying fund does not need to be treated as a customer for AML/CTF purposes unless:

- Otherwise determined by the bank on a risk-based approach;
- The bank takes instructions to execute and/or clear transactions from the underlying fund, either directly, or indirectly through an appointed third party agent (where the agent is not the investment manager) such as an attorney; or,
- The bank is contracting with and holding assets for safekeeping on behalf of the fund (e.g. as a custodian).

13.51 For the avoidance of doubt, apart from the scenarios identified at sub-paragraphs 13.45 – 13.49 above, the bank may (in line with the FATF guidance) treat the investment manager and not the fund as a customer, even if the investment manager is (for credit

risk purposes, for example) contracting with the firm as agent for its underlying fund customers.

13.52 Where the fund is not required to be treated as a customer for AML/CTF purposes, the bank should nonetheless consider obtaining, at a minimum, the fund's name, its main principals and any other information, on a risk-based approach, it considers necessary to support effective screening to comply with applicable international sanctions regimes.

13.53 For illustrative purposes, the following table sets forth the parties in respect of whom CDD measures are required to be carried out by the bank where it has (1) a correspondent securities relationship with the investment manager only, or (2) a customer relationship with both the investment manager and the fund for AML/CTF purposes:

| | **Correspondent securities relationship between bank and investment manager only** | **Customer relationship between bank and fund (refer sec. 1.3.6)** |
|---|---|---|
| **Appropiately Regulated Investment Manager** | 1. The investment manager is a customer requiring CDD.<br>2. The fund in not a customer and therefore CDD is not required. The bank should nontheless obtain, at a minimum, the fund's name and any other information, on a risk-based approach, it considers necessary to support effective screening to comply with applicable intenational sanctions regimes. | 1. The investment manager is a customer requiring CDD.<br>2. The fund is also a customer requiring CDD. |
| **Any other investment manager** | 1. The investment manager is a customer requiring CDD.<br>2. The fund in not a customer and therefore CDD is not required. The bank should nonetheless obtain, at a minimum, the fund's name and any other information, on a risk-based approach, it considers necessary to support effective screening to comply with applicable intenational sanctions regimes.<br>3. In the context of the correspodent securities relationship, the bank may consider undertaking risk-based due-dilligence on the underlying fund. | |

*Variations of customer due diligence*

13.54 As illustrated in the table above, when there is a correspondent securities relationship between the bank and the investment manager, the investment manager is a customer requiring CDD. If the investment manager is Appropriately Regulated, the relationship may be considered by the bank as lower risk (in the absence of other risk factors). However, due to the nature of a correspondent securities relationship, enhanced customer due diligence (EDD) will be required by the bank for investment managers who do not reside in an EEA jurisdiction.

13.55 When there is a customer relationship between the bank and the fund, and the investment manager is Appropriately Regulated, it may in some cases (e.g. for listed or regulated funds assessed as presenting a lower risk), be possible to apply CDD, adjusting the extent, timing or type of CDD evidence obtained. Otherwise, the fund can be identified by obtaining independent documentation, and/or the bank may satisfy elements of its CDD obligations by obtaining a signed form from the investment manager. Partial or full reliance on the investment manager may be permitted in certain situations.

13.56 In certain cases where there is a customer relationship between the bank and an assessed lower risk listed/regulated fund, if the investment manager is not Appropriately Regulated, it is not appropriate for the fund to be considered lower risk when it is managed by a higher risk investment manager. More commonly in this scenario, CDD on the investment manager is advisable, and EDD will be required on a risk-based approach.

*Customer Due Diligence: investment managers*

13.57 When the bank determines that a customer relationship exists with an investment manager, the identity of the investment manager must be verified, in accordance with the guidance relevant to their entity type, set out in Part I, Chapter 5.

13.58 When the bank establishes a correspondent securities relationship with an Appropriately Regulated Investment Manager who does not reside in an EEA member state, the bank should consider how to satisfy the specific EDD obligations arising under the Wwft. As noted above, section 13.50 – 13.53: Customer relationship with the fund explains that within the scope of

correspondent relationships there are relationships representing different types of risks, which necessitate various levels of controls, and different ways of satisfying the requirements of the Wwft in lower risk cases.

13.59 In cases in which the bank establishes a correspondent securities relationship with an investment manager who is subject to a regulatory regime but is not established in EEA jurisdiction or is not regulated at all, a bank may satisfy the relevant requirements by adopting a similar approach to EDD, which includes an assessment of the investment manager's AML/CTF controls. In the context of providing brokerage services to funds, further consideration should be given to undertaking risk-based due diligence on the underlying fund, to obtain a more comprehensive view of the risks posed by the relationship as a whole.

*Customer Due Diligence: Funds*

13.60 Where the bank is required to conduct CDD on the fund, in appropriate circumstances of assessed lower risk, and depending on whether the investment manager is Appropriately Regulated, and whether the fund itself is Appropriately Regulated, partial or full reliance may be permitted (see Reliance on third parties section 13.81.

13.61 When carrying out CDD on the fund, the identity of the fund must be verified, in accordance with the relevant guidance set out in Part I, Chapter 5. Banks should be satisfied when performing CDD that they understand the nature of the fund, including information related to the fund’s strategy, its target objectives and investor base. This information may also help banks satisfy requirements related to establishing the nature and purpose of the proposed customer relationship (see Part I, Chapter 5). On a risk-based approach, depending on the circumstances of the fund and its relationship with the bank, it may be relevant for the bank to consider some or all of following aspects of CDD on the fund.

13.62 Where the fund ownership and control structure is comprised of numerous fund entities or portfolios, to the extent practical and on the basis of a bank’s risk-based approach, banks should establish and document the structure of the fund.

13.63 Master-feeder fund structures allow feeder funds using the same investment strategy to pool their capital and be managed as part

of a bigger master fund investment pool. Where the bank's customer is a master fund within a master/feeder structure, the feeder funds should be identified. A bank should consider whether, based upon its risk-based approach, the identity of the investors in the feeder funds needs to be obtained and verified, as UBOs.

13.64 On a risk-based approach, the entity responsible for CDD of the feeder funds (ordinarily the administrator, registrar or transfer agent) should also be identified, as a bank may consider it necessary to place reliance on this entity pursuant to Reliance on third parties section 13.81

13.65 Umbrella fund structures allow separate portfolios that provide different strategies or rights to investors within an overarching fund structure. The sub-funds under the umbrella fund structure are separate portfolios and may or may not be separate legal entities. Where the bank's customer is a sub-fund, the bank should consider whether, on a risk-based approach, the umbrella funds should be identified.

13.66 Depending on the fund ownership and control structure, the ultimate control may be exercised, for example, by individuals at the fund (including directors or trustees), or through a chain of entities between the fund and the ultimate controller. Banks should satisfy themselves that they have established any other parties who ultimately control the fund, and who need to be identified as controlling "UBOs" (see Part I, Chapter 5). In the context of a personal investment vehicle, for example, there may be founder shareholders or others with specified control rights.

13.67 Standard identity information as regards the fund's ultimate controller(s) where they are not the investment manager should be obtained, and the identity of the ultimate controller(s) should be verified in accordance with the guidance set out in Part I, Chapter 5.

13.68 Individual investors that have a relevant interest in a fund are its UBOs (Relevant Investors); what constitutes a relevant interest will depend on the form of the fund (e.g. where the fund is in the form of a legal entity (e.g. a company), individual investors that have more than 25% interest in the fund are its UBOs). Subject to 13.70 below, such Relevant Investors should be identified and

verified in accordance with the guidance set out in Part I, Chapter 5.

13.69 The distribution of the fund may have a bearing on its type of investors, likely number of investors and how investments are made. Shares or units in funds may be open to general subscription, including on a stock exchange, or to purchase by any qualifying investors. Alternatively, funds may be established for the exclusive use of a closed group of private investors including hedge funds established for high net worth investors. The investors are also ultimately the fund entity's source of funds/wealth.

13.70 The distribution of the fund, together with the regulatory status of the fund and its related parties, may impact the approach to identification and verification of Relevant Investors, on a risk-based approach.

- When the fund is publicly traded on a Recognised Exchange (see Part I, Annex I) there is no requirement (subject to the bank's risk-based approach) to establish whether there are any Relevant Investors.
- For open-ended funds (whether unlisted or listed on an unregulated market), based on the size of the fund and nature of investor base and/or additional information from the investment manager, banks may be able to satisfy themselves that there are no Relevant Investors within the fund.
- Where the fund is itself Appropriately Regulated but unlisted, reliance measures to assess lower risk funds may impact the bank's approach to the identification or verification of Relevant Investors.
- For other unlisted and unregulated funds, it is likely to be necessary to identify any Relevant Investors, or to take steps to confirm there are no such investors.

13.71 As noted above in section 13.66, banks should be aware of the involvement of third party distributors. In such circumstances and on a risk-based approach, banks may wish to obtain further information on the underlying investor base. Establishing the nature of distribution arrangements may itself assist in understanding the fund’s investor base. Where the distributor itself is a Relevant Investor, it should be

identified and verified in accordance with the guidance set out in Part I, Chapter 5.

13.72 On occasion, a bank may offer services to, or establish a relationship with, a fund that is in the process of formation or a start-up. Start-up funds are funds that are in the pre-investor phase, and as such it is not appropriate to consider undertaking due diligence on the Relevant Investors; until the start-up phase is complete the investors and their status (as relevant or not) may change, depending on who else invests in the fund. In these circumstances, a bank should review the Relevant Investor situation and undertake, when appropriate to do so, due diligence on Relevant Investors, however, prior to executing any transactions.

13.73 For information and start-up funds, if any documents required to complete CDD on the fund are not final at the account opening stage, confirmation can be sought from an independent and reliable source attesting that key information will not change in the final version (i.e. details of administrators, investment managers) or, in the event they may change, that the bank will be informed as soon as reasonably practicable. In this situation, a bank might decide, on a risk sensitive basis, to accept such confirmation. Final versions of the documentation should, however, be obtained and reviewed prior to executing any transactions.

*Enhanced Due Diligence*

13.74 When higher AML/CTF risk factors are present, including those highlighted above and in Part I, as part of a bank's risk-based approach, the bank may feel it necessary to undertake EDD on the fund. Banks should seek to apply EDD measures that address the specific increased risk factors. In addition to the measures in Part I, Chapter 5, banks may wish to apply the following EDD measures as relevant:

- Establishing in greater detail the purpose of the fund, for example the nature and location of the fund's investments;
- Obtaining further information on the investor base to better document the source of funds for the fund;
- Increased quantity and source of verification on Relevant Investors; and
- Increased due diligence to establish commercial rationale for complex ownership and control fund structures.

*Reliance on third parties*

13.75 In assessing the involvement of other regulated firms in a fund structure, it may be relevant to consider the jurisdiction where the other firm is based, its regulated status, and also, where the other firm is part of a group, whether it applies relevant group-wide AML/CTF policies and procedures that are equivalent to those required by the Wwft.

13.76 Wwft sets out the parties on whom reliance can be placed (see Part I, Chapter 2).

13.77 Where an executing broker and a clearing broker are undertaking elements of the same exchange transaction on behalf of the same customer, and the clearing broker has conducted CDD on the customer, the executing broker may be able to rely upon the clearing broker (see Part I, Chapter 5).

*Monitoring*

13.78 There is a requirement to conduct ongoing monitoring. Guidance on the general monitoring requirements is set out in Part I. The implementation of such monitoring procedures can mitigate ML/TF risks to banks offering services to funds. There are, however, also specific characteristics of funds that will be relevant to banks' consideration of appropriate monitoring procedures, in particular the use of multiple brokers.

13.79 Customers may choose to allocate execution, clearing and prime brokerage to different banks and there are many customers who may use more than one execution broker. The reasons for this include ensuring that they obtain best execution, competitive rates, or gain access to a particular specialisation within one bank. Monitoring funds’ activity will be affected by the fact that banks may only have access to a part of the overall picture of their customer’s trading activities. This means that many banks will have a limited view of a customer’s trading activities. It may be difficult to assess the commercial rationale of certain transactions and possible involved ML/TF risks.

13.80 The nature and extent of any monitoring activity will therefore need to be determined by the bank. This will vary for each bank and may include an assessment of the following matters:

- Extent of business undertaken (executing, clearing, prime brokerage or a mixture of all three);
- Nature of funds that are customers (e.g. geographic location);
- Number of customers and volume of transactions;
- Types of products traded and complexity of those products; and
- Payment procedures.

13.81 Banks should ensure that any relevant factors taken into account in determining their monitoring activities are adequately documented and are subject to appropriate periodic review.

13.82 Banks relying on third parties under the Wwft to apply CDD measures cannot rely on the third party with respect to monitoring.

# Chapter 14

# Invoice Finance

## Introduction and description of product

*General*

14.1 Invoice finance products are used to fund the working capital requirements of customers; these generally fall into two categories:

- Factoring agreements; and,
- Invoice Discounting agreements.

These can be operated on a Recourse or Non Recourse basis, and with or without disclosure of the assignment of the sales invoice to the customer's customers, the debtors.

14.2 Invoice finance products can be offered by banks, subsidiaries of banks or independent factoring or invoice finance companies. For this purpose the term financial institution used in this chapter should be understood to refer to all of the above.

14.3 Factoring is a contract between a financial institution and their customer where revolving finance is provided against the value of the customer's sales ledger that is sold to the invoice financier. The invoice finance company will manage the customer's sales ledger and will normally provide the credit control and collection services. The customer assigns all their invoices, as usually a whole turnover contract is used, after the goods or service have been delivered or performed. The financial institution will then typically advance up to 85% of the invoiced amount – the gross amount including VAT. The balance, less charges, is then paid to the customer once the debtor makes full payment to the financial institution.

14.4 Invoice Discounting is a contract between the financial institution and their customer where revolving finance is provided against the value of the customer's sales ledger. The customer will manage the sales ledger and will normally continue to provide credit control and collection services. The customer assigns all

invoices, as usually a whole turnover contract is used, after the goods or service have been delivered or performed. The financial institution records and monitors this on a bulk sales ledger basis rather than retaining the individual invoice detail. The financial institution will then typically advance up to 85% of the invoiced amount. The balance, less any charges, is then paid to the customer once the debtor makes full payment to the financial institution. The customer undertakes the collection of the debt under an agency agreement within the contract. The customer is obliged to ensure that the payments from debtors are passed to the financial institution.

14.5 Asset-Based Lending in the Invoice Finance industry would usually have the customer's sales ledger at the core of the facility. It is a contract between the financial institution and their customer where revolving finance and/or fixed amortising finance is provided against a 'basket' of assets – accounts receivables, inventory, plant machinery, property, etc.

*Recourse and Non-Recourse agreements*

14.6 Recourse agreements can apply to factoring or invoice discounting agreements. If the debtor fails to pay the amount due to the customer, then the financial institution will look to the customer for reimbursement of any money they have advanced against that invoice.

14.7 Non-Recourse agreements can apply to factoring or invoice discounting facilities. The financial institution effectively offers a bad debt protection service to the customer. If the customer fails to pay the amount due to the customer, due to insolvency, the financial institution stands the credit loss up to the protected amount, which is the value of the credit limit provided against the particular customer, less any agreed first loss amount.

*International Collection Services*

14.8 Assigned sales invoices may include overseas sales that require international collection services. When the financial institution is not able to undertake this cross border activity, it may partner with a collection company in the appropriate country. Different types of institutions can fulfil a role as collection company, dependent on the jurisdiction and their role.

14.9 The activities and associated risks are considered to be similar to correspondent banking albeit considered to be a lower risk, the financial institution being fully aware of the underlying transaction and the purpose of payment.

## Customer Due Diligence

*Who is the customer from AML perspective?*

14.10 In the invoice finance provision the party with whom the financial institution holds a contract to provide finance is usually referred to as a 'customer' and the customer's customers as 'debtors'.

14.11 The identification requirements on which guidance is given in Part I, will apply to a financial institution's customers (i.e. the parties with whom it has a customer relationship). The customer will be a business entity; a public limited company, private limited company, partnership or sole trader.

*Customer Due Diligence measures.*

14.12 The CDD measures carried out at the commencement of the customer relationship and the ongoing due diligence are some of the primary controls for preventing criminals using invoice finance facilities. Financial institutions must carry out risk-based CDD measures to gain a full understanding of the customer and their business before opening a facility. This must include establishing expected activity patterns of customers and their business activities to meet the requirements set out in Part I.

14.13 The identity of the customer's debtors will normally only be obtained from the customer, as part of the understanding of that customer, without verification being required. The financial institutions risk appetite could determine that verification of the identity of some or all of the customer's debtors and subsequent filtering against applicable (e.g sanctions, internal, adverse media) lists will also be required under circumstances considered to be of increased risk.

14.14 In terms of money laundering, some invoice finance products are considered higher risk than others; in these cases, enhanced due diligence measures as explained in Part I are required.

14.15 Enhanced due diligence is appropriate in the following, but not exhaustive, list of situations:

- Where any party connected to the customer is a PEP. (See Part I);
- When the customer is involved in a business that is considered to present higher risk of money laundering;
- A customer who carries a higher risk of money laundering by virtue of their business or occupation. Examples in the context of invoice financing could be;
  - A business with a high level of cash sales.
  - A business with a high level of cross border sales, including Import-Export companies.
  - A business selling small high value goods that are easily disposed of.

14.16 To assess whether transactions or activities meet expected or historic expectations, a financial institution could take into consideration the following elements:

- Size – monetary, frequency, etc.;
- Pattern – cyclical, logical, frequency, amount, etc.;
- Location – cross border, rationale, etc.;
- Goods / Service – Type, Use, Payment norms, etc.

14.17 Monitoring aspects of enhanced due diligence should be set out in the financial institutions's risk-based approach. It is likely they will include the following:

- More frequent and on-site inspections of the customer's books and records, frequently called an 'Audit', with appropriate management oversight and action of any significant deficiencies.
- More frequent and extensive verification, usually by telephone contact with the debtor, of the validity of the sale and invoice values.
- Greater management supervision of these facilities.
- Extended KYC.

## Money Laundering Risk

### *Factors of increased and decreased ML risk*

14.18 As with any financial service activity, invoice finance products are susceptible to use by criminals to launder money. Both Factoring and Invoice Discounting products facilitate third party payments

and may therefore be used by criminals for money laundering activity. The different invoice finance products available vary greatly and the degree of risk is directly related to the product offering.

14.19 The susceptibility of the invoice finance sector at the traditional placement stage is very low. This is due to the low level of physical cash receipts in the invoice finance sector, as the vast majority of debtors settle outstanding invoices by way of cheque or electronic payment methods.

14.20 The main money laundering risks within the invoice finance sector are payments against invoices where there is no actual movement of goods or services provided, or the value of goods is overstated to facilitate the laundering of funds. As stated, the level of risk will depend on the nature of the product. Factoring should be considered to be a lower risk than invoice discounting, in view of the fact that direct contact is maintained with the debtor. Invoice discounting would represent an increased risk of money laundering due to the 'hands off' nature of the product.

14.21 The following factors will generally increase the risk of money laundering for invoice finance products:

- Cross border transactions;
- Products with reduced paper trails;
- Products where the invoice financier allows the customer to collect the debt;
- Confidential products;
- Bulk products.

14.22 The following will generally be considered good practice to decrease the risk of money laundering for invoice finance products:

- Individual items (invoices, customers, receipts) being recorded and managed by the financial institution;
- Collections activity being undertaken by the financial institution;
- Non-recourse facilities;
- Regular ongoing due diligence and monitoring including on-site inspections and verification of balances;
- Regular transaction monitoring to detect unusual transactions.

*Risk assessment*

14.23 It is important that a financial institution within its control framework has developed robust procedures to monitor the money laundering risks. In particular, the financial institution must have proper procedures in place to establish the source of funds, for which regular credit risk checks will generally not suffice. (See Part I)

14.24 With extremely low levels of cash being transacted the susceptibility of the invoice finance sector at the traditional placement stage is very low.

14.25 Invoice finance products may be used to launder money at the layering and integration stages. However, there are a number of factors that make the invoice finance facility less attractive to the money launderer, they are:

- The high levels of contact between the financial institution and the customer, in terms of physical audits and visits, and of transaction monitoring;
- The sophisticated IT monitoring techniques used to detect issues with the quality of the underlying security, consisting of the quality of the goods and the customers (debtors);
- In the case of factoring the item by item accounting and regular direct contact with the debtors;
- Focus on the debtors in terms of creditworthiness and assessment of risk.

14.26 A financial institution operating a full factoring agreement, with regular contact, monitoring and review of the third party transactions, may determine that the risk level of Factoring Agreements, due to the level and frequency of the mitigating controls is low.

14.27 The risks related to invoice discounting facilities, while generally considered higher risk than factoring facilities may also be mitigated through regular due diligence by the financial institution. A financial institution must consider the risk level based on its own risk assessment and risk appetite.

14.28 Cross border transactions represent an increased risk of money laundering. The nature of the agreement will lead to these transactions being managed in different ways. A financial institution may consider reducing the risk by working with

reputable collection companies and performing adverse news and sanction checks.

14.29 In general, the normally low to medium risk of money laundering will increase with the reduction of the levels of intervention by the financial institution and the increase in size of foreign transactions through the account.

# Chapter 15

# Escrow accounts (‘derdengeldenrekeningen’)

## Legal framwork

*Wft 3:5*

15.1 According to article 3:5 Wft it is prohibited to raise, acquire or have at one’s disposal repayable funds from parties other than professional market operators, unless one is licensed by the proper authorities or granted with an exemption by such authorities. This prohibition does not apply to banks, regional/local authorities and those raising repayable funds by providing securities (for instance, by means of a bond issue).

*Wft 1:1*

15.2 Article 1:1 Wft (Financial Supervision Act) defines repayable funds as funds that must be repaid at a certain point in time, for any reason whatsoever, and of which it is clear in advance what nominal amount must be repaid. Examples are savings and deposits but also borrowing money and issuing bonds. Funds raised by issuing shares are not repayable, as shares do not entail the obligation to repay the nominal amount. The term is used in the definition of 'bank' and in the prohibition on raising repayable or redeemable funds, outside a restricted circle, from parties other than professional market operators.

15.3 Whether funds qualify as repayable is further specified in the Explanatory Memorandum to Article 3:5 of the Wft, which excludes a number of categories. Excluded funds are:

- Paper vouchers and casino chips;
- Advance payments on specific purchase transactions;
- Postponement of payment for specific purchase transactions;
- Funds given within the framework of a specific instruction for 'onward payment' (doorbetaling) to a third party. Examples of agencies that fall outside the scope are injury desks (letselschade bureau’s), collection agencies

(incassobureau's) and child minding (gastouderbureau's). The reason for this is that funds paid by debtors to these agencies, usually do not need to be repaid to a debtor at a certain point in time. Therefore these funds, usually, are not 'repayable funds'. This could, however, be different if the debtor keeps a right to be repaid as long as the agency has not yet transferred the funds to the creditor. In that case it should be checked whether the agency meets the requirements for 'onward payment'. This is the case if the party receives the amounts with the sole purpose of paying onward to a third-party pursuant to a previously given mandate under the condition that:

- The payment and the mandate must be connected, and
- The Bank keeps the money no longer than technically and organisationally necessary. The common practice is a maximum of 5 calendar days, but a deviation may be permitted.

15.4 Administrators for debt restructuring, in particular curators offering debt restructurings in accordance with the Dutch Bankruptcy Act are also exempted parties. The exemption is only applicable to curators registered in the national register held by the Legal Aid Board. The following are also exempted: certain MSBs (under strict conditions), TCSPs, issuers of bearer shares and PSPs.

## Safekeepers

15.5 Notaries, bailiffs and attorneys are safekeeping repayable funds for their customers (escrow services). These profesionals are exempted parties by law. To prevent customers losing their funds in case of bankruptcy of these safekeepers a proprietary segregation of the funds of the customers and those of the safekeepers must be created. Therefore these parties make use of escrow accounts ('derdengeldenrekeningen'). Notaries and bailiffs have a legal obligation to hold an escrow account ('kwaliteitsrekening'). This obligation is regulated respectively by the 'Wet op het Notarisambt' and the 'Gerechtsdeurwaarderswet'. Attorneys are obliged to have an escrow foundation ('stichting derdengelden') in case they are safekeeping funds for their customers based on the 'Verordening op de Advocatuur'.

15.6 The 'kwaliteitsrekening' and the escrow foundation may only be used for the safekeeping of customer property. It is not allowed to

use the accounts for other purposes. No parties are entitled to the funds in the account other than the customers whose funds are being administrated. In order to guarantee this notaries, bailiffs and attorneys are subject to strict rules and supervision.

### What are the ML/TF and other relevant risks?

15.7 The risks escrow services pose to the bank depend, amongst others, on the extent to which these parties are regulated, supervised and/or are an obliged entity under the Wwft.

15.8 The bank has no direct relationship with the underlying customers of the counterparty (the bank's customer) operating the escrow account. The bank is neither in the position nor does it have the obligation to undertake CDD on the underlying customers. The degree of ML/TF risk presented by escrow accounts partly depends on whether the customer itself is subject to Wwft-regulation and supervision or is subject to AML/CTF requirements that are equivalent to the Wwft or the EU 4AMLD. The ML/TF risks involved in these kind of customer relationships may be considered lower than the risks involved in customers requiring an escrow account that are not subject to adequate AML/CTFregulation and supervision.

15.9 The bank runs a liability risk, if it knows that a customer operates an escrow account without the required license (or falls under an exemption). There is a risk that the customers of the counterparty may hold the bank liable in case the counterparty cannot fulfil its obligations under the escrow agreement.

15.10 Banks must be aware of the fact that escrow accounts/foundations may be misused by fraudsters. Since these accounts/foundations are being used by the group of professionals mentioned above, the accounts/foundations create a certain confidence amongst the public. Even using the word 'escrow' or 'derdengelden' in the name of an account can give the impression of confidence to third parties and may give the impression that asset segregation is in place. However, contrary to the escrow accounts/foundations being used by notaries, baillifs and attorneys there is no adequate regulation and supervision in place for escrow accounts/foundations used by other parties. This is why the ML/TF risks related to customer

relationships with an escrow foundation and other entities operating an escrow account that are not subject to adequate regulation and supervision are higher.

### Who is the customer for CDD purposes?

15.11 If the customer requiring an escrow account belongs to the group of professionals as mentioned above (see x.4) the CDD related to the escrow account may be limited to the fact that it is indeed an account operated by a customer belonging to this group of professionals. The CDD undertaken on the customer must be in line with the requirements described in paragraph 2.5 of Part I.

15.12 In all other cases, including those where a 'Stichting Derdengelden' is involved that is not operated by an attorney, enhanced due diligence must be undertaken.

15.13 EDD may include the following measures:

- Gathering sufficient information about the customer to fully understand the nature of its business. The amount of information gathered depends on the risks involved and may take into consideration the type of customers, its business model, products and services being offered, country of operation, size and nature of the transactions that will be carried out on the escrow account;
- Assessing the customer's AML/CTF policy/processes/procedures;
- Undertaking, depending on the ML/TF risks involved, applicable due diligence measures on the customers of the counterparty, including when needed, assessing their source of wealth.

### Escrow services related to a single specific transaction

15.14 Banks may provide escrow and settlement services to third parties themselves as a product. The nature of the ML/TF risk involved in escrow and settlement contracts/agreements is the fact that the customer relationship is predominantly governed by the underlying transaction rather than by the contracting parties that are considered to be the customer. Therefore, additional due diligence (EDD) should focus on the plausibility of the underlying transaction including the source of funds.
EDD may include the following measures:

- Assessing the background, purpose and legitimacy of the underlying transaction(s). For the purpose of this assessment the following factors need to be taken into account:
    - The nature and the duration of the contract/agreement;
    - The size of the transaction(s) under the contract/agreement (amount(s) involved);
    - The simplicity or the complexity of the operational execution of the contract/agreement;
    - The legitimate source and destination of the underlying assets involved, including when needed an assessment of the source of wealth from which the assets originate.

The bank must substantiate why it is comfortable to provide the product or service requested by the customer. If the customer's explanation of a request for particular products or services is inconclusive or otherwise unacceptable and remains so after EDD, the bank must refuse the customer's request.