MONEY LAUNDERING & THE FINANCING OF TERRORISM

GUIDELINES FOR FINANCIAL INSTITUTIONS

Update

[Published 12 June 2017]

The Supervisory Authority and
Director of the ONDCP
O.N.D.C.P. Headquarters
Camp Blizard
Antigua, West Indies
Telephone: 562-3255, (268) 462-5934
Fax: (268) 460-8818
Email: supervisory.authority@ondcp.gov.ag

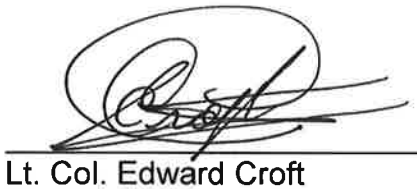
NOTICE

To All Financial Institutions:

TAKE NOTICE that pursuant to the powers of the Supervisory Authority under sections 11(vii) and (xiii) of the Money Laundering (Prevention) Act 1996 as amended, and the powers of the Director of ONDCP under section 43 of the Prevention of Terrorism Act 2005 as amended, the Money Laundering & the Financing of Terrorism Guidelines for Financial Institutions are hereby updated by the amendments annexed hereto.*

The amendments are general upgrades of the guidance to bring them into line with the new international standards. Also included is supplemental guidance on the risk based approach to AML/CFT.

12 June 2017



Lt. Col. Edward Croft
Director of ONDCP and
Supervisory Authority under the
Money Laundering (Prevention) Act 1996

* Financial institutions have 14 days from the date of publication in which to raise with the Supervisory Authority in writing any concerns about implementation or any other issue prompted by this amendment that may relate to its effective implementation.

AMENDMENT

The Money Laundering & Financing of Terrorism Guidelines for Financial Institutions (also referred to herein as "the MLFTG") are hereby amended as follows:

A. In Part I (Money Laundering Guidelines)

1. In Paragraph 1.1 of the MLFTG, the following subparagraphs are inserted after subparagraph 1.1(5):

"(6) assist management in making strategic decisions in relation to the implemention and effectiveness of its AML/CFT system. In so doing, the Compliance Officer should provide information to management on SARs (those that remain internal and those submitted to the Supervisory Authority); on the ML and FT risk assessment of the various areas of the institution's business, for example but not limited to, its departments, business categories, product lines, customer types, geographical areas of operation, etc., so as to assist management in managing the institution's ML/FT risks.

(7) submit an annual written report to the board and senior management ("the Compliance Officer's Annual Report"), which should give an account of the measures being taken to implement policy, controls and procedures relating to AML/CFT legal requirements. It should state the Compliance Officer's independent assessment of the effectiveness of the system. The report should be commensurate with the nature and size of the financial institution to which it relates.

(8) The job functions of a Compliance Officer should always be in operation. Where, for example, a Compliance Officer has reason to be out of office for an extended period, for example, because he has to travel abroad or to take a vacation, the functions of the Compliance Officer should continue to be carried out by someone competent to ensure the compliance function continues effectively and avoid a hiatus until the return of the person who holds the substantive position.

2. After paragraph 1.3 there is inserted paragraph 1.4 titled "1.4 The Risk Based Approach to AML/CFT (See Supplemental Guidance – Risk Based Approach)" at the end of these amendments.

3. Paragraph 2.1.14A(3) subparagraph (a) is repealed and replaced with the following:

"(a)(1) Life insurance business and investment related insurance policies in relation to identification of the beneficiary under the policy: Identification and verification should take place as soon as the beneficiary is identified or designated, and in all cases at or before the payout or the time when the beneficiary intends to exercise vested rights under the policy.

(2) Financial institutions should include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. If a beneficiary who is a legal person or legal arrangement presents a higher risk, enhanced measures should be taken, including reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout."

4. Paragraph 2.1.43 is amended by inserting after the word "owner" the words "or class of benficiaries".

5. After Paragraph 2.1 43, the following is inserted:

"2.1.43A(1) Verification of identity for trust, nominee and fiduciary accounts should include identifying the natural person exercising ultimate effective control (including through a chain of control/ownership).

(2) For other types of legal arrangements (for example, partnerships), paragraphs 2.1.42 to 2.1.43A(1) above should be applied to identifying the arrangements and persons in equivalent or similar positions."

6. Paragraphs 3.4 to 3.13 are repealed and replaced with the following:

"3.4 WIRE TRANSFERS

3.4.1 Wire transfers have been identified as particularly vulnerable to being used for terrorist financing and money laundering. Wire transfer and funds transfer refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may

be the same person. Originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

3.4.2 Wire transfers can be cross-border or domestic. Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element. Domestic transfer means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction,

3.4.3 *Financial institutions shall take measures to include full originator information, that is, accurate and meaningful originator information (name, address and account number) and beneficiary information on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain. Financial institutions shall conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information and beneficiary information. However, where there is a suspicion of ML or FT, the financial institution shall verify the information pertaining to its customer.*

3.5 Cross-*border Wire Transfers*

3.5.1 Cross-border transfers should be accompanied by accurate and meaningful originator information that must at a minimum include the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included. However, the financial institutions may in their discretion substitute the address with a national identity number, customer identification

number or date and place of birth. The accuracy of the information collected must also be verified.

3.5.2 Information must also be obtained on the beneficiary of the wire transfer and include:

(i) the name of the beneficiary;

(ii) the beneficiary account number where an account is used to process the transaction; or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

3.5.3 Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they shall be exempted from including full originator information, provided they include *the originator's account number or unique reference number, and the batch file contains full originator information that is fully traceable within the recipient country, However, financial institutions are required to ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.*

3.6 Domestic wire transfers

3.6.1 Information accompanying domestic wire transfers must also include the same originator information as indicated for cross-border wire transfers, unless the bank is satisfied that full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the financial institution need only include the account number or a unique identifier provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The information must be made available by the ordering financial institution within three (3) business days of receiving the request either from the beneficiary financial institution or from appropriate authorities.

3.7 *Exemptions*

3.7.1 The above guidelines regarding wire transfers do not cover any transfers that flow from a transaction carried out using a credit or debit card so long as the credit or debit card

number accompanies all transfers flowing from the transaction. They also do not apply to financial institution-to-financial institution transfers and settlements where both the originator and the beneficiary are financial institutions acting on their own behalf. However when credit or debit cards are used as a payment system to effect a money transfer, they are covered by these guidelines, and the necessary information should be included in the message.

3.8 Role of Ordering Financial Institutions

3.8.1 *The ordering financial institution must ensure that qualifying wire transfers contain* complete originator information, which must be verified for accuracy. It must also ensure that the wire transfer contains required beneficiary information.

3.8.2 The ordering financial institution should not execute a wire transfer that does not comply with the requirements in this section (paragraphs 3.4 to 3.11 above).

3.8.3 The ordering financial institution shall maintain all originator and beneficiary information collected *in accordance with record keeping requirements of the Regulations and these guidelines.*

3.9 Role of Intermediary Financial Institutions

3.9.1 For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

3.9.2 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution must keep a record, for the minimum period under the Act, of all the information received from the ordering financial institution or another intermediary financial institution.

3.9.3 Intermediary financial institutions should take reasonable measures, consistent with straight-through processing, to identify cross-border transfers that lack required originator information or required beneficiary information.

3.9.4 Intermediary financial institutions should have risk-based policies and procedures for determining (a) when to execute, reject or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow up action."

3.10 Role of Beneficiary Financial Institutions

3.10.1 Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the Supervisory Authority. Where necessary, the beneficiary financial institution must consider restricting or even terminating its business relationship with financial institutions that fail to meet these standards.

3.10.2 Beneficiary financial institutions are required to take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

3.10.3 For cross -border wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously identified, and keep a record of that information in accordance with the regulations.

3.10.5 Beneficiary financial institutions should have risk-based policies and procedures for determining (a) when to execute, reject or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow up action.

3.11 Money Transmissions Services

3.11.1 Providers of money transmission services must comply with all the relevant provisions relating to the different types of wire transfers set out above in the countries in which they operate directly or through their agents.

3.11.2 Providers of money transmission services that control both the ordering and beneficiary side of a wire transfer should (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; (b) file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Supervisory Authority in this country, and to the Financial Intelligence Units in the other countries."

7. After Paragraph 4.6A, the following is inserted:

"4.6B Suspicious Activity Reports are to be sumbitted to the Supervisory Authority promptly upon detection of suspicious activity. Promptly means right away or if necessary, no later than 48 hours of becoming satisfied that the activity is suspicious. For that purpose, financial institutions should have in place systems that allow for prompt detection.Where there is a realistic chance that ML/FT is or is about to take place, or the matter can be seen as urgent, the report must be made right away, within hours if not minutes and verbally if necessary. Where the activity to be reported is complex or of a nature such that a proper report will take more that 48 hours to prepare, the Compliance Officer is nonetheless required to report the suspicion within the 48-hour period with any explanations or requests for extension of time to complete the full report. Note: This guideline supersedes all prior guidance, including the commentary contained in the standardized SAR reporting form in use on the date of publication where there are any conflicts.

8. After Paragraph 4.9, the following is inserted:

"4.9A Where a Compliance Officer, having reviewed a transaction report or the results from sample testing or the monitoring of an account or the activity of a customer, determines that the transaction or the way in which the account is being used or the customer activity is suspicious, the Compliance Officer should have a duty and be enabled to make recommendation where appropriate to management with documented reasons that the transaction should not be completed or that the account be

closed or that there should be no further business relationship with the customer. The management of the institution should give careful consideration to the recommendation and record its response to the recommendation with reasons.

4.9B It should be part of the functions of the Compliance Officer to review applications for the opening of accounts or the initiation of business relationships to assess whether or not the prospective or new customer has any association with criminal activity.

Should the Compliance Officer determine that a prospective or new customer ***is*** concerned with criminal activity that generates proceeds or benefits or relates to FT or proliferation of WMD, then the Compliance Officer, having reviewed all the circumstances, should be enabled to recommend in writing to management that the account not be opened. The management of the institution should give careful consideration to the recommendation and record its response to the recommendation with reasons.

If the Compliance Officer is of the opinion that a prospective or new customer ***may*** be concerned with criminal activity that generates proceeds or benefits or relates to FT or proliferation of WMD, the Compliance Officer may, after consideration of the financial institution's risk exposure, make appropriate recommendations, and be enabled so to do, in relation to whether an account should be opened or a business relationship entered into or continued. The management of the institution should pay careful attention to the concerns of the Compliance Officer and give them appropriate consideration."

9. After Paragraph 4.11, the following is inserted:

4.11A The Compliance Officer should be enabled to act independently in reaching determinations about the nature of transactions, the manner in which accounts are being utilised, and the extent to which the AML/CFT system is being effectively implemented throughout the financial institution, and also in making recommendations to management. The Compliance Officer should not be denied resources so as to prevent or forestall the possibility of a recommendation unfavourable to the pursuit or continued pursuit of business with a customer or potential customer."

B. In Part II (Financing of Terrorism Guidelines)

10. Section 2.6.3 is amended as follows:

(a) in paragraph 2.6.3(3) by inserting at the end on a new line, the following:

"name and address of any natural person exercising ultimate effective control (including through a chain of control/ownership);

name and address of beneficiaries, or beneficiaries identified by characteristics, class or other means".

(b) after paragraph 2.6.3(5), inserting the following:

"(5a) The financial institution should take reasonable steps to verify the identity of the beneficial owners.".

(c) subparagraph (8) is renumbered as (9), and after subparagraph (7) is inserted the following paragraph:

"(8) For other types of legal arrangements, paragraphs 2.6.3(1) to (7) above should be applied to identifying the arrangements and persons in equivalent or similar positions."

C. Miscellaneous

11. References to "bank": These guidelines in both Parts I and II should be assumed to be generic, applying across all categories of business activities listed in the First Schedule to the MLPA, whether or not they are financial institutions in the traditional sense, unless there are clear indications that the guidance is specific to a particular category of financial institution.

In this regard the following references in the guidelines to "banks" should be read generically rather than specifically. In other words, "bank" should be read to mean "bank or other business activity" and "banking" read likewise in the following sections:

Part I of the MLFTG
Paragraphs:
2.1.4B – under Know Your Customer
2.1.5A
2.1.5B
2.1.5C
2.1.7A – under What is identity?
4.3A – under Recognition of Suspicious Activities

Part II of the MLFTG:
Paragraphs:
5.3 under Responsibilities of financial institution and its staff

SUPPLEMENTAL GUIDANCE – Risk Based Approach

1.4 The Risk-Based Approach to AML/CFT

1.4.1 Overview
1.4.2 Advantages of the risk-based approach
1.4.3 How to carry out a risk assessment
1.4.4 Identifying ML/FT risks
- **1.4.4.1 Customers that might pose a risk**
- **1.4.42 Customer behaviours that might suggest a risk**
- **1.4.4.3 When to check source of funds in one-off transactions below $25,000**
  - **Example 1**
  - **Example 2**
  - **Example 3**
- **1.4.4.4 Risks associated with your products and services**

1.4.5 What to do when you have carried out your risk assessment
1.4.6 Mitigation of ML/FT risks
1.4.7 Governance and effective implementation of RBA

Legal framework

Regulations
MLPR 2007 as amended
definition of:
"customer due diligence"
"enhanced due diligence"

reg. 3(1)(b)(i) and (ii)
reg. 4(2)(d)
reg. 4(3)(d)(i)
reg. 4(3a)
reg. 6(1a)

Guidelines
MLFTG as amended
Part I, paragraphs:

2.1.14A(3)(a)(2)	3.10.1
1.1(6)	3.10.5
3.9.4	4.9B

Part II, paragraphs:

1.1.2	1.1.21
1.1.3	1.1.22
1.1.4	1.2.3
1.1.5	1.2.4
1.1.6	1.3.1

1.3.2
1.3.4
1.3.5
1.3.6

4.2.4(2)
5.1
5.3

1.4.1 Overview

(1) Businesses listed in the First Schedule to the Money Laundering (Prevention) Act and therefore regulated by the Money Laundering (Prevention) Regulations (MLPR) must assess the risk that they could be used for money laundering, including terrorist financing and the financing of the proliferation of weapons of mass destruction.

(2) You should decide which areas of your business are at risk and put in place measures to prevent money laundering occurring by using what's known as a 'risk-based' approach.

(3) This section gives an overview of the risk-based approach and helps you to carry out a risk assessment of your business.

(4) Financial institutions must adopt a risk-based approach (RBA) for dealing with money laundering threats. RBA means that you are expected to identify, assess and understand the ML/FT risks to which you are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively.

(5) The RBA is not optional, but a prerequisite for the effective implementation of the AML/CFT requirements. For that reason, the risk assessment must be subject to ongoing monitoring and kept up-to-date.

(6) Where ML/FT risks are higher, FIs have to take enhanced measures to mitigate the higher risk. The range, degree, frequency or intensity of controls used will be stronger. Where the ML/FT risk is identified as lower, standard AML/CFT measures may under certain conditions be reduced, which means that each of the required measures has to be applied, but the degree, frequency or the intensity of the controls used will be lighter or simplified. This may be done where the financial institution has controls in place that reflect the degree of risk of ML identified, and measures to monitor the effectiveness of implementation of those controls to the standard required.

(7) In assessing it owns risk, a financial institution should take into account:

- the results of the National Risk Assessment (NRA) of Antigua and Barbuda and any other jurisdiction in which it operates, take account of

the legal requirements in place, note any legally prescribed areas of high or significant risk, and legally permitted mitigation measures for low risk;
- Complement this information with relevant internal and external information
- Mutual evaluation reports;
- Typologies;

(8) Where risks are high, financial institution should always use enhanced due diligence, even if mitigation measures are not set out in law.

(9) Simplified measures may not be used by a financial institution where a suspicion of ML/FT exists.

(10) Assessing and understanding risk requires skilled and trusted staff. Where appropriate they should be assigned fit and proper tests. They should be technically equipped to carry out their tasks, commensurate with the complexity of the operations.

1.4.2 Advantages of the risk-based approach

You're able to decide on the most cost-effective way to control the risks of money laundering when you follow the steps involved in the risk-based approach. This allows you to focus your efforts and resources where the risks are highest.

1.4.3 The risk-based approach

(1) Businesses that are regulated by the MLPR have to use a risk-based approach to prevent money laundering. This involves following a number of steps.

You have to:

(a) identify the money laundering risks that are relevant to your business;

(b) □carry out a detailed risk assessment of your business, focusing on customer behaviour, delivery channels and so on;

(c) assess the levels of bribery and corruption affecting the business;

(d) design and put in place controls to manage and reduce the impact of these risks;

(e) monitor implementation of the controls and improve their efficiency;

(f) □keep records of what you did and why you did it;

(g) carry out re-assessments at appropriate intervals. Some FIs will refresh their risk assessments annually, however, if there are no

material changes to the risk environment, some may choose to undertake their risk assessments less frequently. In exceptional circumstances, such as regulatory intervention for example, a risk assessment may be conducted more frequently than annually;

(2) Your risk assessment should always be properly documented, maintained and communicated to relevant personnel.

(3) The risk assessment must be approved by senior management.

(4) The risk assessment must always be available to the Supervisory Authority, Regulators and other Competent Authorities upon request.

1.4.4 How to carry out a risk assessment

(1) You can decide for yourself how to carry out your risk assessment. It might be quite simple or very sophisticated depending on:

- the size and structure of your business
- □the range of activities your business carries out and
- the nature of the products and services it supplies.

(2) When you assess the risks of money laundering that apply to your business you need to consider:

- the types of customer you have;
- □where you and your customers are based;
- □your customers' behavior;
- □how customers come to your business;
- □the products you sell or the services you offer;
- □your delivery channels and payment processes, for example cash over the counter, cheques, electronic transfers or wire transfers;
- □where your customers' funds come from or go to.

(3) Things conventionally taken into consideration are (a) Inherent Risk (b) Control Effectiveness, and (c) Residual Risk. Inherent Risk are the risks normally associated with the product, service etc. Control Effectiveness refer to the types of mitigating controls. Residual Risk is the risk remaining after the inherent risks are mitigated by applying controls. Some things that might be considered are as follows:

Inherent risk	Control effectiveness	Residual risk
Clients	Governance	Strategic actions
Products and services	Policies & procedures	Tactical actions
Countries	KYC/Due diligence	Risk appetite
Channels	Other risk assessments	
Other	Management information	
	Record keeping/retention	
	AML unit	
	SAR filings	
	Monitoring and controls	
	Training	
	Independent testing	

1.4.5 Identifying ML/FT risks

(1) Start by checking the results of the NRA and what it says in relation to the country, financial institutions and the financial sector of which your business is a part.

(2) In identifying the ML/FT risks to which they are exposed, a financial institutions should consider a range of factors, including:

- Nature, scale, diversity and complexity of the business;
- Target markets;
- Number of customers already identified as high risk;
- The jurisdictions it is exposed to either through its own activities or the activities of customers, especially jurisdictions that are subject to advisories for being high risk or having strategic AML/CFT deficiencies or for which countermeasures have been called for my the international or regional oversight bodies;
- Degree to which it relies on third parties to conduct elements of CDD;
- Distribution channels;
- Use of technology.

(3) It helps to categorize risks to better understand and prioritize them. Categorization is usually on a scale of High – Medium – Low.

1.4.4.1 Customers that might pose a risk

(1) Your business might be at risk of money laundering from:

- new customers carrying out large, one-off transactions;
- □a customer who has been introduced to you - because the person who introduced them to you may not have carried out 'due diligence' thoroughly;
- □customers who aren't local to your business□;
- customers involved in a business that handles large amounts of cash;
- □businesses with a complicated ownership structure that could conceal underlying beneficiaries□;
- a customer - or group of customers - who makes regular transactions with the same individual or group of individuals

1.4.4.2 Customer behaviours that might suggest a risk

Behaviour that may indicate a potential risk could be when a customer:

- doesn't want to give you identification, or gives you identification that isn't satisfactory;
- doesn't want to reveal the name of a person they represent□;
- agrees to bear very high or uncommercial penalties or charges;
- □enters into transactions that don't make commercial sense;
- is involved in transactions where you cannot easily check where funds have come from

1.4.4.3 When to check source of funds in one-off transactions below $25,000

(1) The way customers present themselves and the source of their funds are key indicators of potential risk.

(2) You should be able to show, through your risk-based approach, that you have taken all reasonable steps to satisfy yourself that the transaction is not suspicious, including, where appropriate, identifying the source of funds or wealth.

(3) This is best done through independent documents or data provided by the customer, for example, a payslip or bank statement. The documentation

required and the level of checks will depend on the risks to your business.

(4) Where a person is sending money for someone else and information such as a wage slip or bank statement is not available you should consider obtaining and keeping a signed certificate/declaration by the customer about the source of funds – checked against a proof of ID document, such as a passport.

Example 1

(1) A customer claims they are transmitting money on behalf of a group of friends. You should write down details of the names and addresses of the friends and the amounts to be transmitted.

(2) Where you have to accept a declaration, it is sensible to include details of something that can itself be checked. This could be contact details for each person named in the declaration, but every case will be different.

Example 2

(1) A customer claims the cash is from the sale of a car. You should include details of the car, its registration number and the date of sale. This will provide you with protection, as you'll be able to show that you have undertaken sufficient checks and will allow law enforcement agencies who can use such details to follow up on transactions after the event if they need to.

(2) The essential point is that the customer has provided you with information that can be checked. Whether you do any additional checks on that information will depend on your view of the risk.

(3) Businesses should have an operating risk based system in place, which is fully documented. If a business doesn't apply its own risk based approach to 'source of funds' checks, then the Supervisory Authority will expect that you seek additional verification on payments below $25,000 when:

- the customer has presented cash in payment for the transaction, which is five times the size of an average transaction for your business;
- □the customer has paid for the transaction by cheque or debit card, which is ten times the size of an average transaction.

(4) 'Average transaction' means the total value divided by the number of transactions over a given period. 'Your business' means calculated by each branch (where your business has more than one premises including the premises of any agents who act on your behalf).

Example 3

(1) You have transmitted $100,000 over 100 transactions in the given period, so the average value of your transactions is $1,000. You should check the source of funds on any cash transaction for $5,000 or more and any non-cash transaction for $10,000 or more.

(2) The length of time you use to decide the size of an average transaction for your business isn't fixed, although it should be at least one month. Ideally, the average transaction value will relate to a single set of premises. If you have more than one set of premises within your registration you may decide to fix the transaction level either by individual location or by reference to all the transactions across the whole of your business, being aware of the transaction levels between different locations.

(3) You may limit the source of funds checks to the top 5% of transactions by value if the number of transactions to be checked exceeds 5% of your total transactions.

(4) Where funds have come from a bank account, you can take some re-assurance that the customer's identity and personal details may have been checked by another regulated business in Antigua and Barbuda or another country which is prepared to provide the customer with account facilities. However, you should not be satisfied just because the money has come from the customer's bank account that the source of funds is lawful.

(5) You should take a risk based approach, so that you're content with and establish how the money got into the bank and where the money came from, such as:

- wages;
- □a cheque from a family member;
- payment from the sale of personal items.

(6) An indication of higher risk might be if funds in the bank account had been paid in cash shortly before the transaction. Just because the funds have been through a bank doesn't mean that you can always assume that you don't need to check the source for them, especially if they seem unusual.

(7) You must send a Suspicious Activity Report (SAR) to the Supervisory Authority if you have any suspicion that the transaction relates to money laundering and/or terrorist financing, and get consent from them to continue with the transaction. You should always report before a transaction is made where possible. If your suspicion is raised after the transaction is completed you must send a SAR at the earliest opportunity.

1.4.4.4 Risks associated with your products and services

(1) Depending on your business type there may be a risk:

- that inappropriate assets could be placed in your business, or moved from or through it from a product or service which allows the ownership of assets to be disguised□;
- when you supply services without meeting your customer face to face.

(2) The types of risk you need to identify will depend on the nature of your business. For example, high value goods such a precious metal, art or jewellery need to be aware of the risk associated with cash sales of high value goods that can be either:

- sold through the black market - these are generally luxury items returned to the retailer in exchange for a legitimate cheque from them.

1.4.5 What to do when you have carried out your risk assessment

(1) Once you've completed your risk assessment you need to:

- put in place controls and systems to reduce any risks of money laundering that you identified;
- monitor your business on an ongoing basis to make sure your controls are effective;
- □identify and report any suspicious transactions or activities.

1.4.6 Mitigation of ML/FT Risks

(1) You are required to develop preventative and mitigation measures commensurate with the ML/FT risks identified. This relates to the way you allocate your compliance resources, organize your internal controls and internal structures, and implement policies and procedures to deter and detect ML/FT, including at the group level.

(2) You should decide on the most appropriate and effective means to mitigate the ML/FT risk.

1.4.7 Governance and effective implementation of RBA

(1) The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership and oversight of the development and implementation of the RBA across the business.

(2) Senior management should consider various ways to support AML/CFT

initiatives:

- promote compliance as a core value of the business by sending a clear message that the business will not enter into, or maintain, business relationships that are associated with excessive ML/TF risks which cannot be mitigated effectively. Senior management, together with the board, are responsible for setting up robust risk management and controls adapted to the business' stated, sound risk-taking policy;
- implement adequate mechanisms of internal communication related to the actual or potential ML/TF risks faced by the business. These mechanisms should link the board of directors, the AML/CFT Compliance Officer, the IT division and each of the business areas;
- decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the business is prepared to accept; and
- adequately resource the AML/CFT unit.

(3) This implies that senior management should not only know about the ML/TF risks to which the business is exposed but also understand how its AML/CFT control framework operates to mitigate those risks. This would require that senior management:

- receives sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the business is exposed through its activities and individual business relationships;
- receives sufficient and objective information to understand whether the business' AML/CFT controls are effective (for example information from the Chief Compliance Officer on the effectiveness of control, or audit reports);
- and that processes are in place to escalate important decisions that directly impact the ability of the business to address and control risks.

(4) It is important that responsibility for the consistency and effectiveness of AML/CFT controls be clearly allocated to an individual of sufficient seniority within the business to signal the importance of ML/TF risk management and compliance, and that ML/TF issues are brought to senior management's attention. This includes, but is not restricted to, the appointment of a skilled compliance officer at management level.

(5) The Supervisory Authority expects financial institutions to meet their AML/CFT legal obligations in a risk-sensitive way. The assessment of an effective RBA will depend on a common understanding by the Supervisory Authority and the financial institutions of what the RBA entails, how it should be applied and how ML/FT risks should be addressed. The Supervisory

Authority should be consulted if there are queries.

12 June 2017

Lt. Col. Edward Croft
Supervisory Authority and
Director of the ONDCP