HANDBOOK

FOR THE PREVENTION AND DETECTION OF

MONEY LAUNDERING

AND

COMBATING THE FINANCING OF TERRORISM

FOR FINANCIAL AND TRUST SERVICE PROVIDERS

REGULATED BY

THE CENTRALE BANK VAN ARUBA

Statutory Requirements,
Regulatory Requirements
and Guidance Notes

June 1, 2011

CONTENTS

GLOSSARY

In the context of this Handbook the below abbreviations and references have the following meanings:

Furthermore, reference is made to the definitions contained in Article 1 of the AML/CFT State Ordinance.

AML:	Anti-money laundering.
CFT:	Combating financing of terrorism.
Amending State Ordinance:	State Ordinance amending the Sectoral Supervisory State Ordinances (*Landsverordening herziening sectorale toezichtswetgeving*).
AML/CFT State Ordinance:	State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (*Landsverordening voorkoming en bestrijding witwassen en terrorismefinanciering*, AB 2011, no. 28).
AML/CFT Laws and Regulations:	AML/CFT State Ordinance, State Decree Regulation Wire Transfers (*Landsbesluit regeling geldelijke overmakingen*, AB 2011, no. 30), Sanctions State Ordinance (*Sanctieverordening 2006*, AB 2007, no. 27), Sanctions State Decree Combating Terrorism and Financing of Terrorism (*Sanctiebesluit bestrijding terrorisme en terrorismefinanciering*, AB 2010, no. 27) and related laws and regulations in the area of AML/CFT.
Board:	The Executive Board and insofar applicable also the Supervisory Board of a Regulated Entity.
CBA:	Centrale Bank van Aruba.
CBCS:	Centrale Bank van Curaçao en Sint Maarten.
CDD:	Customer due diligence.
CFATF:	Caribbean Financial Action Task Force.
close associates:	A natural person (i) of whom it is known that this person is a joint ultimate beneficiary of legal entities or legal constructions together with a PEP, or has other close business relationships with said person; or (ii) who is the sole beneficiary of a legal entity or legal construction of which it is known that it was established for the factual benefit of a PEP.
direct family members:	Husband or wife or partner who under the relevant national law is considered equivalent to a husband or wife, the children and their husbands or wives or partners and parents.
DNB:	De Nederlandsche Bank.

Enactment State Ordinance:	Enactment Ordinance State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (*Invoeringsverordening Landsverordening voorkoming en bestrijding witwassen en terrorismefinanciering*, AB 2011, no. 29).
existing customer:	An existing customer as at the date that the AML/CFT State Ordinance came into force.
express trust:	A (Anglo-Saxon) trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangement (e.g. constructive trust).
EEA:	European Economic Area.
EU:	European Union.
FATF:	Financial Action Task Force on Money Laundering.
FATF Recommendations:	The FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing.
FT:	Financing of terrorism.
Guidance Notes:	Ways of complying with the Statutory Requirements or Regulatory Requirements presented in this Handbook.
Handbook:	Handbook for the prevention and detection of money laundering and combating the financing of terrorism for financial and trust services business regulated by the Centrale Bank van Aruba.
IMF:	International Monetary Fund.
ML:	Money laundering.
MLCO:	Money laundering compliance officer as meant in Article 47, paragraph 1, of the AML/CFT State Ordinance.
MLRO:	Money laundering reporting officer as meant in Article 47, paragraph 2, of the AML/CFT State Ordinance.
MOT:	Reporting Center Unusual Transactions (*Meldpunt Ongebruikelijke Transacties*), referred to in Article 20, paragraph 1, of the AML/CFT State Ordinance.
OFAC:	Office of Foreign Assets Control of the US Department of the Treasury.
PEP:	Politically exposed person as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance.

Regulated Entity:	Entity regulated according to the SOSCS, SOSIB, SOSMTC, SOSTSP and supervised by the CBA, which is also deemed a financial or designated non-financial service provider as mentioned in Article 1, paragraph 1, of the AML/CFT State Ordinance.
Regulatory Requirements:	Directives issued by the CBA that Regulated Entities must comply with.
Relevant Employee:	An employee whose duty relates to the provision of financial and trust services.
SOSCS:	State Ordinance on the Supervision of the Credit System (*Landsverordening toezicht kredietwezen*, AB 1998, no. 16).
SOSIB:	State Ordinance on the Supervision of Insurance Business (*Landsverordening toezicht verzekeringsbedrijf*, AB 2000, no. 82)).
SOSMTC:	State Ordinance Supervision Money Transfer Companies (*Landsverordening toezicht geldtransactiebedrijven*, AB 2003, no. 60).
SOSTSP:	State Ordinance on the Supervision of Trust Service Providers (*Landsverordening toezicht trustkantoren*, AB 2009, no. 13).
source of funds:	The origin of the customer's assets offered to the Regulated Entity or otherwise involved in the business relationship or the transaction, e.g. a customer's occupation or business activities. Information concerning the geographical sphere of the activities may also be relevant.
source of wealth:	The activities which have generated the total net worth of a customer (the customer's funds and other assets). Information concerning the geographical sphere of the activities may also be relevant.
Statutory Requirements:	Requirements as set by or by virtue of the AML/CFT State Ordinance.
Supervisory Laws:	SOSCS, SOSIB, SOSMTC and SOSTSP.
UBO:	Ultimate beneficial owner (or beneficiary).
UN:	United Nations.
US:	United States of America.

1. INTRODUCTION

1. Aruba has a strong commitment at political, government and industry level to play an active part in the international fight against ML and FT. Accordingly the authorities of Aruba will take a strong line toward any business that assists in ML or FT, whether it acts:

   - with knowledge or suspicion of the connection to crime; or
   - without proper regard to what it may be facilitating through the provision of its products or services.

   Such businesses will face the loss of their reputation, they will risk regulatory sanction including the loss of their license (where regulated and supervised). In addition to these substantial matters persons also risk prosecution for criminal offences.

2. Each Regulated Entity must recognize the role that it must play in protecting itself, and its employees, from involvement in ML and the FT, and also in protecting Aruba's reputation of probity.

3. The CBA strongly believes that the key to the prevention and detection of ML and FT lies in the implementation of, and strict adherence to, effective systems and controls, including sound CDD procedures based on international standards. This Handbook therefore sets standards which match international standards issued by the FATF. The Handbook also has regard to the standards promoted by the Basel Committee on Banking Supervision and the International Association of Insurance Supervisors. The Handbook takes account of the requirements of EU AML/CFT legislation, and its application of standards set by the FATF.

1.1 OBJECTIVES OF THE HANDBOOK

4. The objectives of the Handbook are as follows:

   - to outline the requirements of the AML/CFT State Ordinance and related legislation.
   - to outline the requirements of the AML/CFT State Ordinance which introduces additional obligations for those remitting or receiving fund transfers;
   - to set out the CBA's requirements to be followed by all Regulated Entities (Regulatory Requirements);
   - to assist a Regulated Entity to comply with the requirements of the legislation described above (Statutory Requirements) and the CBA's requirements (Regulatory Requirements) through practical interpretation;
   - to provide a base from which Regulated Entities can design, tailor and implement their own AML/CFT policies, procedures and measures;
   - to ensure that Aruba matches international AML/CFT standards;
   - to emphasize the responsibilities of the Board of the Regulated Entity;
   - to promote the use of a proportionate risk based approach to CDD measures, which directs resources towards higher risk customers;
   - to provide practical guidance on identification and verification of identity; and

- to emphasize the particular ML and FT risks of certain financial services and products.

5. The Handbook may be amended in light of experience, changes in legislation, and the development of international standards.

6. The Handbook is intended for use by senior management and compliance staff in the development of a Regulated Entity's policies, procedures and measures. The Handbook is not to be used by a Regulated Entity as an internal procedures manual.

1.2 STRUCTURE OF THE HANDBOOK

7. Part 1 of the Handbook is structured to take a three level approach.

   - Level one (**Statutory Requirements**) describes the statutory requirements set out in the AML/CFT State Ordinance that apply to Regulated Entities.

   - Level two (**Regulatory Requirements**) provides directives of the CBA regarding the application of the AML/CFT State Ordinance that apply to Regulated Entities.

   - Level three (**Guidance Notes**) presents ways of complying with the Statutory Requirements (level one) and Regulatory Requirements (level two) and must always be read in conjunction with these requirements. A Regulated Entity may adopt other appropriate measures to those set out in the Guidance Notes, including policies, procedures and measures established by the group, so long as it can demonstrate that such measures also achieve compliance with the Statutory and Regulatory Requirements. This allows a Regulated Entity discretion as to how to apply requirements in the particular circumstances of its business, products, services, transactions and customers. The soundly reasoned application of the provisions contained within the Guidance Notes will provide a good indication that a Regulated Entity is in compliance with the Statutory and Regulatory Requirements.

8. The provisions of the Statutory and Regulatory Requirements are described using the term **must** or **should**, indicating that these requirements are mandatory. In contrast, the Guidance Notes use the term **may**, indicating ways in which the Statutory and Regulatory Requirements may be satisfied, but allowing for alternative means of meeting the requirements. References to must, should and may elsewhere in the Handbook should be similarly construed.

9. Level one (Statutory Requirements) necessarily paraphrases provisions contained in the AML/CFT State Ordinance. Depending on the subject, these can be articles, sections of articles or a combination of articles or sections of articles of the AML/CFT State Ordinance. Level one should always be read and understood in conjunction with the full text of the AML/CFT State Ordinance and where applicable other AML/CFT Laws and Regulations. Such text is presented in italics.

10. Should discrepancies arise between the text of this Handbook and the text of the AML/CFT State Ordinance, the text of the latter always prevails.

11. Reference is also made to the Explanatory Memorandum to the AML/CFT State Ordinance, in which the provisions of the AML/CFT State Ordinance are further explained and interpreted.

1.3 LEGAL STATUS AND SANCTIONS FOR NON-COMPLIANCE

12. The Statutory Requirements described in this Handbook are statutory requirements prescribed by the AML/CFT State Ordinance.

13. The Regulatory Requirements that are introduced in this Handbook are directives of the CBA regarding the application of Chapters 2, 3, 4 and 6 of the AML/CFT State Ordinance, issued on the basis of Article 48, paragraph 1, of the AML/CFT State Ordinance. These directives are directed at Regulated Entities, being financial services providers or designated non-financial service providers as defined in Article 1, paragraph 1, of the AML/CFT State Ordinance State. In so far as the directives concern the application of Chapter 3 of the AML/CFT State Ordinance, the CBA has consulted with the MOT.

14. Pursuant to the AML/CFT State Ordinance, non-compliance with provisions set by or by virtue of the AML/CFT State Ordinance (i.e. Statutory and Regulatory Requirements) can be addressed with the following instruments:

- a direction (*aanwijzing*);
- a penalty charge order (*last onder dwangsom*);
- an administrative fine (*bestuurlijke boete*);
- criminal prosecution.

15. Moreover, the Supervisory Laws set out obligations for Regulated Entities regarding sound and controlled business operations, more specifically to pursue adequate policies and to have procedures and measures in place to, *inter alia*, ensure compliance with the AML/CFT Laws and Regulations.[1]

16. Compliance with the requirements of the AML/CFT State Ordinance and the Handbook will also be considered by the CBA in the execution of its supervisory tasks pursuant to the Supervisory Laws. Non-compliance with the Supervisory Laws can be addressed by the CBA with the following instruments:

- a direction;
- a penalty charge order;
- an administrative fine;
- publication of a direction, a penalty charge order or an administrative fine;
- silent receivership (*stille curatele*)
- revocation of the license or removal from the registry;
- criminal prosecution.

17. The AML/CFT State Ordinance and the Supervisory Laws[2] state that violations can be committed by natural persons and legal persons. Article 53, paragraph 1 and 2, of the Criminal Code of Aruba applies mutatis mutandis. This means that violations by a legal entity may be attributed to the

[1] After the Amending State Ordinance has entered into force.

[2] After the Amending State Ordinance has entered into force.

individuals who ordered the act constituting the violation or who were “de facto in charge” at the time when the violation occurred.

1.4 SCOPE OF THE STATUTORY AND REGULATORY REQUIREMENTS

1.4.1 FINANCIAL AND TRUST SERVICES CONDUCTED FROM ARUBA

18. The AML/CFT State Ordinance applies to many categories of persons carrying on business in or from Aruba. However, this Handbook focuses on Regulated Entities. This will include Aruban-based branches of companies incorporated outside Aruba conducting financial or trust services business in or from Aruba.

1.4.2 FINANCIAL AND TRUST SERVICES CONDUCTED OUTSIDE ARUBA

STATUTORY REQUIREMENTS

19. *Under Article 45, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity that has a branch or subsidiary outside Aruba must take care that the branch or subsidiary applies as much as possible the provisions set by or by virtue of the AML/CFT State Ordinance and the internationally accepted AML/CFT standards. According to Article 45, paragraph 2, of the AML/CFT State Ordinance, this applies in particular to branches and subsidiaries in countries and jurisdictions that do not or insufficiently apply the international accepted AML/CFT standards.*

20. *Where legislation of a foreign jurisdiction prohibits compliance with the AML/CFT State Ordinance, the Regulated Entity must, in accordance with Article 45, paragraph 3, of the AML/CFT State Ordinance, inform the CBA of this and take, if necessary in consultation with the CBA, measures to counter the ML and FT risks.*

REGULATORY REQUIREMENTS

21. If a Regulated Entity has a subsidiary or branch carrying on a financial or trust services business in a jurisdiction outside Aruba that has more stringent requirements than those set out in the AML/CFT State Ordinance, the Regulated Entity must ensure that, with regard to this subsidiary or branch, the more stringent requirements are complied with.

1.5 RISK BASED APPROACH

22. To assist the overall objective to prevent ML and FT, the Handbook adopts a risk based approach. Such an approach:

- recognizes that the ML and FT threat to a Regulated Entity varies across customers, jurisdictions, products and services and delivery channels;
- allows a Regulated Entity to differentiate between customers in a way that matches risk in a particular business;
- while establishing minimum standards, allows a Regulated Entity to apply its own approach to policies, procedures and measures in particular circumstances;
- directs resources towards higher risk customers; and
- helps to produce a more cost effective system.

23. Policies, procedures and measures will not detect and prevent all ML or FT. A risk based approach will, however, serve to balance the cost burden placed on individual Regulated Entities and on their customers with a realistic assessment of the threat of a Regulated Entity being used in connection with ML or the FT by focusing effort where it is needed and has most impact.

2. CORPORATE GOVERNANCE AND CONTROLLED BUSINESS OPERATIONS

2.1 OVERVIEW OF SECTION

1. Corporate governance is the system by which businesses are directed and controlled. The responsibilities of the Board include setting strategic aims, providing the leadership to put them into effect and supervising the management of the business. This chapter describes a Regulated Entity's general framework for an adequate corporate governance system and controlled business operations to combat ML and FT, including:

   - an ethical culture;
   - conducting a business risk assessment;
   - establishing and maintaining policies, procedures and measures,
   - ensuring compliance with policies, procedures and measures;
   - appointing a MLCO and MLRO;
   - ensuring effective policies, procedures and measures; and
   - outsourcing.

2. This Handbook does not distinguish between the executive board and the supervisory board. The structure of a two tier board (separate executive and supervisory boards) is required for banks and life insurance companies, but not for money transfer companies and trust service providers. Irrespective of the governance structure in place, the Handbook is equally applicable to all Regulated Entities. Each Regulated Entity is responsible for determining the relevant levels of responsibility for each body. Banks and life insurance companies are referred to the respective policy papers on corporate governance issued respectively for the banking and insurance sectors.

3. Where a Regulated Entity is not a legal person, but is, for example, a branch or partnership, references in this chapter to "the Board" should be read as meaning the senior management function of that business.

2.2 AN ETHICAL CULTURE

REGULATORY REQUIREMENTS

4. The Board must ensure an ethical corporate culture and lead accordingly by example and actions ('tone at the top').

5. The Board must actively promote risk and compliance awareness and the importance of AML/CFT and encourage ethical behavior.

6. The Board must ensure that the Regulated Entity's remuneration policy does not negatively impact the ethical corporate culture or compromises the operation of effective AML/CFT policies, procedures and measures.

2.3 CONDUCTING A BUSINESS RISK ASSESSMENT

STATUTORY REQUIREMENTS

7. *According to article 46, paragraph 3, of the AML/CFT State Ordinance, Regulated entities must carry out periodical evaluations in order to assess if and to what extent they are vulnerable to ML and FT because of their activities and operations.*

REGULATORY REQUIREMENTS

8. The Board must conduct and document a business risk assessment. In particular, the Board must consider, on an on-going basis, the extent of its exposure to risks by reference to its organizational structure, its corporate culture, its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services. The Board's assessment must be kept up to date.

9. On the basis of its business risk assessment, the Board must establish a formal AML/CFT strategy. For a Regulated Entity forming part of a group operating outside Aruba, that strategy must protect both its global reputation and its Aruba business.

10. The Board must consider what barriers (including cultural barriers) exist to prevent the operation of effective AML/CFT policies, procedures and measures, and must take effective measures to address them.

GUIDANCE NOTES

11. The Board may demonstrate that it has considered and addressed the Regulated Entity's exposure to ML and FT risks by:

- Involving all members of the Board and the MLCO and MLRO in determining the ML and FT risks within those areas for which they have responsibility.

- Considering organizational factors that may increase the level of exposure to the ML and FT risks, e.g. outsourced activities.

- Considering the risk that cultural barriers might prevent the operation of effective AML/CFT policies, procedures and measures. Human and organizational/hierarchical factors, such as the inter-relationships between different employees within a Regulated Entity, the inter-relationships between employees and customers, insufficient room for dissenting opinions, lack of transparent decision making, can result in the creation of damaging barriers. Unlike policies procedures and measures, the prevailing culture of an organization is intangible. As a result, its impact can sometimes be difficult to measure. The risk that cultural barriers might prevent the operation of effective AML/CFT policies, procedures and measures may be minimized by the Board considering the prevalence of the following factors:

    - An assumption on the part of more junior employees that their concerns or suspicions are of no consequence.

    - Negative handling by managerial staff of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions.

    - An unwillingness on the part of employees to subject high value (and therefore important) customers to effective CDD checks.

- Pressure applied by management or customer relationship managers outside Aruba upon employees in Aruba to transact without first conducting all relevant CDD.

- Excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management remuneration or bonus schemes are primarily linked to revenue-based targets.

- The familiarity of employees with certain customers resulting in unusual or higher risk activity and transactions within such relationships not being identified as such.

- The inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential ML and FT activity.

- A tendency for line managers to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily.

- An excessive desire on the part of employees to provide a confidential and efficient customer service.

- Non-attendance of senior employees at AML/CFT training sessions on the basis of mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

- Considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each area of its operation.

- Considering who its customers are and what they do.

- Considering whether any additional risks are posed by the jurisdictions with which its customers, and introducers are connected. Factors such as high levels of organized crime, increased vulnerabilities to corruption and inadequate AML/CFT frameworks will impact the risk posed by relationships connected with such jurisdictions.

- Considering the characteristics of the products and services that it offers and assessing the associated vulnerabilities posed by each product and service, including delivery channels. For example:

  - The use of third parties such as group entities and other introducers to conduct elements of the CDD process.

  - Pooled relationships will tend to be more vulnerable - because of the anonymity provided by the co-mingling of assets or funds belonging to several underlying customers.

- Considering how it establishes and delivers products and services to its customers. For example, risks are high when relationships are established remotely (non-face to face), or are controlled remotely by the customer (straight-through processing of transactions).

2.4 POLICIES, PROCEDURES AND MEASURES

STATUTORY REQUIREMENTS

12. *In accordance with article 46, paragraph 1, of the AML/CFT State Ordinance, Regulated Entities must pursue adequate policies and must have in place written procedures and measures, in particular for the application of the Chapters 2, 3 and 4 of the AML/CFT State Ordinance.*

13. *In accordance with article 46, paragraph 2, of the AML/CFT State Ordinance, the procedures and measures must in any case regard the internal organization and internal control of the Regulated Entity, the recruitment, change of position, background, education, guidance and on-going training of the relevant staff, the application of the CDD, record keeping, the internal decision making process for the reporting of unusual transactions, as well as the periodical evaluation of the effectiveness of those procedures and measures.*

REGULATORY REQUIREMENTS

14. Taking into account the conclusions of the business risk assessment and AML/CFT strategy, the Board must organize and control its affairs effectively and be able to demonstrate the existence of adequate AML/CFT policies, procedures and measures.

2.5 APPOINTING A MLCO AND MLRO

STATUTORY REQUIREMENTS

15. *According to article 47, paragraph 1, of the AML/CFT State Ordinance, Regulated Entities must employ a person in charge with the compliance with the laws and regulations in the area of AML/CFT (the MLCO).*

16. *According to article 47, paragraph 2, of the AML/CFT State Ordinance, Regulated Entities must employ at least one person in charge with the internal receipt and assessment of potential unusual transaction reports and the reporting of unusual transactions to the MOT (the MLRO).*

17. *According to article 47, paragraph 3, of the AML/CFT State Ordinance, a Regulated Entity must inform the MOT and the CBA of the appointment of the MLCO and the MLRO, within a month after the appointment took place.*

REGULATORY REQUIREMENTS

18. A Regulated Entity must appoint a MLCO that:

- has sufficient knowledge, experience and skills;
- has appropriate independence and authority;
- has direct access to the Board (i.e. operates at management level);
- has sufficient resources, including sufficient time and (if appropriate) a deputy MLCO and support staff;
- has unfettered and timely access to all business lines, support departments and information necessary to appropriately perform the function.

19. A Regulated Entity must appoint a MLRO that:

- is employed by the Regulated Entity or an entity in the same group as the Regulated Entity;
- is based in Aruba;
- has sufficient knowledge, experience and skills;
- has appropriate independence and authority;
- has direct access to the Board;
- has sufficient resources including sufficient time and (if appropriate) a deputy MLRO and support staff;
- has unfettered and timely access to all business lines, support departments and information necessary to appropriately perform the function.

20. In the event that the position of MLCO or MLRO is expected to fall vacant, a Regulated Entity must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

21. Where temporary circumstances arise where the Regulated Entity has a limited or inexperienced compliance or reporting resource, the Regulated Entity must ensure that this resource is supported and temporary replaced as necessary.

22. When considering whether it is appropriate to appoint the same person as MLCO and MLRO, a Regulated Entity must have regard to:

- the respective demands of the two roles, taking into account the size and nature of the Regulated Entity's activities; and
- whether the individual will have sufficient time and resources to fulfill both roles effectively.

GUIDANCE NOTES

23. A Regulated Entity may demonstrate that it has clearly apportioned AML/CFT responsibilities, where the MLCO:

- develops and maintains policies, procedures and measures in line with evolving requirements;
- undertakes regular reviews (including testing) of compliance with AML/CFT policies, procedures and measures;
- advises the Board on AML/CFT compliance issues that need to be brought to its attention;
- reports periodically, as appropriate, to the Board on compliance with the Regulated Entity's policies, procedures and measures;
- responds promptly to requests for information made by the CBA and the MOT;
- acts as the liaison point with the CBA and in any other third party enquiries in relation to ML or FT;

24. A Regulated Entity may demonstrate that it has clearly apportioned AML/CFT responsibilities, where the MLRO:

- maintains a record of all enquiries received from law enforcement authorities and records relating to all internal and external unusual transaction reports (Section 8);
- manages relationships effectively post disclosure to avoid tipping off any third parties;
- acts as the liaison point with the CBA and the MOT and in any other third party enquiries in relation to ML or FT;

25. A Regulated Entity may demonstrate that the MLCO and MLRO have sufficient knowledge, experience and skills where an MLCO or MLRO:

- completed at least secondary education (HAVO/VWO), or higher, and ideally would have attained, or be studying for, a higher level of professional qualification which are provided by a range of academic and professional bodies.
- has 3 to 5 years relevant industry experience, at least one of which to evidence some management responsibilities – team leader or above – in a regulated financial services environment;
- has undertaken some compliance specific study – ideally resulting in formal qualifications;
- is a person of high integrity and highly analytical, critical and persistent.

26. Larger Regulated Entities with more complex AML/CFT requirements may need to employ senior compliance staff with a greater degree of experience and professional qualifications.

2.6 ENSURING COMPLIANCE WITH POLICIES, PROCEDURES AND MEASURES

REGULATORY REQUIREMENTS

27. The Board must assess compliance with policies, procedures and measures. It periodically must commission and consider a report from the MLCO that covers compliance, and it must sign off and retain the report. The frequency and content of such reports must be determined by its business risk assessment, including consideration of cultural barriers.

28. The Board must notify the CBA immediately in writing of any material failures to comply with the requirements of the AML/CFT State Ordinance or of the Handbook.

GUIDANCE NOTES

29. Areas which the periodic report may cover include:

- The means by which compliance with the Regulated Entity's policies, procedures and measures have been monitored and tested.
- Compliance deficiencies identified and details of action taken or proposed to address any such deficiencies.
- The number and scope of the unusual transaction reports made to the MOT based on the objective indicators.

- The number and scope of the internal potential unusual transaction based on the subjective indicators received and the number and scope of subsequent external unusual transaction reports submitted to the MOT.

- Information concerning the training program: which employees have received training, the methods of training and the nature of any significant issues arising from the training.

- Action taken in response to FATF statements (circulated by the CBA) highlighting jurisdictions which do not or insufficiently apply the FATF Recommendations or which are the subject of international countermeasures.

- Action taken to comply with AML/CFT Laws and Regulations.

2.7 ENSURING EFFECTIVENESS OF POLICIES, PROCEDURES AND MEASURES

STATUTORY REQUIREMENTS

30. *According to article 46, paragraph 3, of the AML/CFT State Ordinance, Regulated Entities must carry out periodical evaluations in order to assess if and to what extent they are vulnerable to ML and FT because of their activities and operations.*

31. *According to article 46, paragraph 3, of the AML/CFT State Ordinance, the findings of the periodical evaluations must be recorded in writing.*

REGULATORY REQUIREMENTS

32. Regulated Entities must conduct independent assessments of the effectiveness of its policies, procedures and measures on a periodic basis.

33. From time to time an assessment of the effectiveness of the Regulated Entity's policies, procedures and measures is to be conducted by a dedicated, independent and adequately resourced internal audit function. The frequency and scope of such an assessment must be determined by the Regulated Entity's business risk assessment.

34. The Board must reach an independent conclusion as to the effectiveness of the Regulated Entity's policies, procedures and measures and monitor adequate follow up action.

GUIDANCE NOTES

35. The Board may wish to use the MLCO and MLRO to provide information and advice to assist the Board to assess the effectiveness of the Regulated Entity's policies, procedures and measures. Larger and more complex Regulated Entities may require separate dedicated risk management and internal audit functions to assist in the assessment of effectiveness.

36. The Board may demonstrate that it has adequately assessed the effectiveness of a Regulated Entity's policies, procedures and measures where it, for example:

- Maintains an internal audit function that is conducted under the responsibility of an experienced auditor, being RA, AA or CPA, with at least 5 years of relevant experience in audit field.

- Ensures that the internal audit function is not combined with an operational function.

- Receives regular and timely information relevant to the management of the ML and FT risks, including information on any branches and subsidiaries.

- Considers the adequacy of the management information received by the Board relevant to the management of ML and FT risks.

- Monitors the on-going competence and effectiveness of the MLCO and the MLRO.

- Considers the adequacy of resources to comply with the AML/CFT State Ordinance, (and by extension, also the Handbook) as well as other AML/CFT Laws and Regulations.

- Considers the adequacy of its approach to the management of ML and FT risks posed by its existing customer base (see Section 9).

- Considers whether the incidence of unusual transaction reports (or absence of such reports) has highlighted any deficiencies in the Regulated Entity's CDD or reporting policies, procedures and measures, and whether changes are required to address any such deficiencies.

- Considers whether inquiries have been made by the MOT or law enforcement, without issues having previously being identified by CDD or reporting policies, procedures and measures.

- Considers changes made or proposed in respect of new legislation, regulatory requirements or guidance, or as a result of changes in business activities.

2.8 OUTSOURCING

REGULATORY REQUIREMENTS

37. In case of outsourcing, the ultimate responsibility for the outsourced activities and compliance with the AML/CFT Laws and Regulations, including this Handbook, remains with the Regulated Entity.

38. The outsourcing of activities should not hinder compliance with the AML/CFT Laws and Regulations.

39. The outsourcing of activities should not hinder the CBA's adequate supervision of the Regulated Entity's compliance with the AML/CFT Laws and Regulations.

40. A Regulated Entity must consider the effect that outsourcing has on the ML and FT risk, in particular where a MLCO or MLRO is provided with additional support from third parties, either from within the group or externally.

41. A Regulated Entity must assess possible ML or FT risks associated with outsourced activities, record its assessment, and monitor any risk on an on-going basis.

42. A Regulated Entity must be satisfied with the policies, procedures and measures that are put in place by the third party. In particular, a Regulated Entity must be satisfied that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of ML or FT activity will be reported by the third party to the MLRO of the Regulated Entity.

43. If activities are outsourced on a structural basis, the agreement between the Regulated Entity and the third party must be recorded in writing. The Regulated Entity must submit the draft outsourcing agreement to the CBA for prior approval.

44. A Regulated Entity must in any case regulate the following in the outsourcing agreement:

- the mutual exchange of information, including agreements about providing information requested by the CBA in connection with the execution of its supervisory tasks;

- the possibility for the Regulated Entity to at all times make changes in the manner in which the activities are carried out by the third party;

- the obligation of the third party to enable the Regulated Entity to continue to comply with the AML/CFT Laws and Regulations;

- the possibility for the CBA to carry out or have carried out an investigation at the third party's premises; and

- the manner in which the agreement is terminated, and the manner in which it is ensured that the Regulated Entity is able, after the termination of the agreement, to carry out the activities again itself or have another third party carry out these activities.

3. CDD REQUIREMENTS

3.1 OVERVIEW

1. This section establishes the minimum CDD requirements, and sets out a framework by which a Regulated Entity is required to develop a risk based approach to determining the type and extent of measures to apply to different types of customers, products and services. For example, the type and extent of customer identification and relationship information, the nature of verification of information obtained, and the level of business relationship monitoring activity.

2. The basic CDD measures required by the Statutory Requirements and Regulatory Requirements involve:

   - Identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information.

   - Identifying the UBO and taking reasonable measures to verify the identity of the UBO such that a Regulated Entity is satisfied that it knows who the UBOs are.

   - Identifying any third parties on whose behalf the customer is acting.

   - Determining the purpose and intended nature of the business relationship.

   - Keeping the above information up to date, and monitoring the business relationship and transactions undertaken throughout the course of the relationship to determine whether they are consistent with the Regulated Entity's knowledge of the customer and the UBO.

3. Sound CDD measures are vital because they:

   - help to protect the Regulated Entity and the integrity of the financial sector in which it operates by reducing the likelihood of the Regulated Entity becoming a vehicle for, or a victim of, financial crime;

   - assist law enforcement, by providing available information on customers or activities and transactions being investigated - following a unusual transaction report to the MOT;

   - constitute an essential part of sound risk management, e.g. by providing the basis for identifying, limiting and controlling risk, including reputational, operational, legal and concentration risk; and

   - help to guard against identity fraud.

4. The inadequacy or absence of satisfactory CDD measures can subject a Regulated Entity to serious customer and counterparty risks, as well as reputational, operational, legal, regulatory and concentration risks, any of which can result in significant financial cost to the Regulated Entity. CDD information is also a vital tool for the MLRO and business employees when examining unusual or higher risk activity or transactions, in order to determine whether an unusual transaction report is appropriate.

5. This section (Section 3) of the Handbook describes the CDD requirements, except for on-going monitoring and scrutiny of activity and transactions which is separately described in Section 4. Accordingly, this section should be read and understood in conjunction with Section 4.

6. A customer may be a natural person or a legal person or arrangement seeking to enter into a business relationship or conduct an occasional transaction.

3.2 RISK BASED APPROACH

7. Policies procedures and measures will not detect and prevent all instances of ML or FT. A risk based approach will, however, serve to balance the cost burden placed on a Regulated Entity and on their customers with the risk that the Regulated Entity may be used in ML or to FT by focusing resources on higher risk areas.

STATUTORY REQUIREMENTS

8. *Pursuant to Article 6, paragraph 3, of the AML/CFT State Ordinance, a Regulated Entity must tailor the CDD measures to the risk-sensitiveness for ML or FT in relation to the type of customer, business relationship, product, or transaction. To that effect, a Regulated Entity must establish a risk profile of the customer and the UBO*.

REGULATORY REQUIREMENTS

9. A Regulated Entity's business risk assessment (see Section 2.3) should enable the Regulated Entity to determine its initial approach to performing the CDD process, depending on the type of customer, business relationship, product or transaction involved.

10. The customer risk assessment must determine a risk profile of the customer and the UBO and the extent of CDD information that will be obtained, how that information will be verified, and the extent to which the resulting business relationship will be monitored.

11. Care must be exercised under a risk based approach. Being identified as carrying a higher risk of ML or FT does not automatically mean that a customer is a money launderer or is financing terrorism. Similarly, identifying a customer as carrying a lower risk of ML or FT does not mean that the customer is not a money launderer or financing terrorism.

3.3 SITUATIONS IN WHICH CDD MEASURES MUST BE APPLIED

STATUTORY REQUIREMENTS

12. *Article 6, paragraph 1 and 2, of the AML/CFT State Ordinance prescribes that Regulated Entities must apply CDD measures in the following cases:*

- *All Regulated Entities,*
  - *when entering into a business relationship in or from Aruba;*
  - *if there are indications that the client is involved in ML or FT;*
  - *if it doubts the soundness or reliability of data obtained from the client previously, or*
  - *if the risk of involvement of an existing client in ML or FT gives reason to do so.*
- *Regulated Entities, except for trust service providers:*
  - *when carrying out an occasional transaction in or from Aruba for the benefit of a customer of at least Afl. 25,000.-, or of two or more transactions related to each other with a combined value of at least Afl. 25,000.-;*

- *when carrying out a money transfer as meant in Article 1 of the SOSMTC in or from Aruba;*

- *Trust service providers, when carrying out the following activities:*

  - *to act as a founder of legal persons;*

  - *to provide a domicile, a business address or an accommodation, a postal or an administrative address to a company, corporation, or partnership, or another legal person of arrangement;*

  - *to act or have someone else act as manager or representative of a trust;*

  - *to act or have someone else act in the name of a shareholder.*

REGULATORY REQUIREMENTS

13. In particular, CDD measures must be applied when there is a:

- change in CDD information of a customer;

- change of UBO; or

- change in the third parties (or UBO of third parties) on whose behalf a customer acts.

3.4 TIMING OF INITIAL IDENTIFICATION AND VERIFICATION OF IDENTITY

STATUTORY REQUIREMENTS

14. *Pursuant to Article 8, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must apply CDD measures before entering into a business relationship or before carrying out an occasional transaction*. *However, Article 8, paragraph 2, of the AML/CFT State Ordinance provides the following exceptions:*

- *A Regulated Entity may verify the identity of the customer and the UBO during the establishment of the business relationship, if this is necessary not to disrupt the normal conduct of business, and there is little risk of ML or FT; in this case, the Regulated Entity must verify the identity as soon as practicable after the first contact with the customer;*

- *a Regulated Entity being a life insurer may identify the beneficiary of a policy and verify the identity, after the business relationship has been entered into; in this case, the identification and the verification of the identity must take place on or before the date of payment, or on or before the date on which the beneficiary wants to exercise his rights arising from the policy;*

- *a Regulated Entity being a bank can open an account, before the identity of the customer has been verified, provided it guarantees that this account cannot be used before verification has taken place.*

REGULATORY REQUIREMENTS

15. If a Regulated Entity completes verification of identity after the initial establishment of a business relationship, the following conditions must be met:

- all required CDD information (including information on identity) has been obtained;

- the need to perform verification of identity at a later stage is essential not to interrupt the normal conduct of business;

- it highlights to its customer its obligation to terminate the relationship in case the customer is not able to provide the information necessary to meet the verification requirements within a reasonable period of time; and

- ML/FT risk is effectively managed.

16. In case the customer is not able to provide the information necessary to meet the verification requirements, a Regulated Entity must terminate the relationship (See Section 3.5).

GUIDANCE NOTES

17. A Regulated Entity may demonstrate that it has a right to terminate a relationship where terms of business which govern its relationships with its customers encompass the termination of relationships in case the customer is not able to provide the information necessary to meet the verification requirements. Terms and conditions could clearly state that termination may lead to a customer suffering losses – where for example funds have been invested in a collective investment fund.

18. ML risk may be effectively managed where:

- policies, procedures and measures establish timeframes for the completion of verification measures; and

- the establishment of any business relationship benefiting from this concession has received appropriate authorization and such relationships are appropriately monitored so that verification of identity is carried out as soon as is practicable.

3.5 FAILURE TO COMPLETE CDD MEASURES

STATUTORY REQUIREMENTS

19. *According to Article 9, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must not enter into a business relationship or carry out a transaction, if it has not applied CDD measures, if it is not able to apply CDD measures or if the CDD measures did not lead to the result envisaged by Article 3, 4 and 5 of the AML/CFT State Ordinance*.

20. *According to Article 9, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity must end the business relationship promptly, if it is no longer able to comply with Article 3, 4 or 5 of the AML/CFT State Ordinance*.

REGULATORY REQUIREMENTS

21. Wherever possible, when terminating a relationship where customer money or other assets have been received, a Regulated Entity should return the assets directly to the customer, for example by returning money to the account from which it was received.

22. Where the customer requests that money or other assets be transferred to third parties, or to a different account in the customer's name, the Regulated Entity must assess whether this provides grounds for knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of ML or FT.

3.6 IDENTIFICATION AND VERIFICATION OF IDENTITY

23. This section describes the basic requirements regarding identification of customers and UBOs and the verification of their identity. Refer to Sections 3.11 and 3.12 for situations in which simplified CDD will be allowed or enhanced CDD will be required.

STATUTORY REQUIREMENTS

24. *Pursuant to Article 3, paragraph 1, subsection a, of the AML/CFT State Ordinance, a Regulated Entity must identify the customer and verify the customer's identity*.

25. *Pursuant to Article 3, paragraph 1, subsection b, of the AML/CFT State Ordinance, a Regulated Entity must identify the UBO and the take reasonable measures to verify the UBO's identity in such way that the Regulated Entity is convinced of the UBO's identity.*

26. *According to Article 4 of the AML/CFT State Ordinance, a Regulated Entity must ascertain whether a customer is acting for himself or on behalf of a third party and take reasonable measures to find out the identity of that third party en to verify that third party's identity*.

27. *According to Article 5, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must, if a customer is a legal person or arrangement, (i) verify that a natural person purporting to act on behalf of the customer is authorized to do so; (ii) identify that natural person and verify that natural person's identify; and (iii) record information on the legal status and provisions regulating the power to bind the legal person or arrangement*.

28. *According to Article 5, paragraph 3, of the AML/CFT State Ordinance, a Regulated Entity must, if a customer is acting as a trustee of a trust or if the business relationship is entered into or if the transaction is performed in connection with the management of a trust, take reasonable measures that lead to the settlor of the trust and the UBO to the assets of the trust being identified and their identity being verified*.

29. *Pursuant to Article 19, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must verify the identity of a customer being a natural person, using documents, data or information from a reliable and independent source*.

30. *Pursuant to Article 19, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity must verify the identity of a customer being a legal person which is domiciled in Aruba, using documents, data or information from a reliable and independent source*.

31. *Pursuant to Article 19, paragraph 3, of the AML/CFT State Ordinance, a Regulated Entity must verify the identity of a customer being a foreign legal person which is not domiciled in Aruba, using reliable and internationally accepted documents, data, or information, or documents, data, or information that have been recognized by law in the state of origin of the customer as a valid means of identification*.

32. *Pursuant to Article 19, paragraph 4, of the AML/CFT State Ordinance, a Regulated Entity must verify the identify of a trustee and the person who otherwise exercises effective control, the settlor of the trust and the UBO with regard to the assets in the trust, using reliable and internationally accepted documents, data, or information, or documents, data, or information that have been recognized by law in the state of origin of these persons as a valid means of identification*.

33. *Pursuant to Article 19, paragraph 5, of the AML/CFT State Ordinance, a Regulated Entity must verify the identity of the UBO using reliable and internationally accepted documents, data, or information or on the basis of documents, data, or information that have been recognized by law in*

the state of origin of the UBO as a valid means of identification, in such manner that it is convinced of the identity of the UBO.

REGULATORY REQUIREMENTS

34. When, as part of the identification and verification process, determining that a customer is the person that he, she, or it claims to be, a Regulated must be satisfied that:

    - a person exists - on the basis of appropriate identification information; and
    - the customer or UBO is that person - by verifying from reliable, independent source documents, data or information, satisfactory confirmatory evidence of appropriate components of the customer's or UBO's identity.

35. The extent of identification information to be obtained, what to verify, and how to verify it in order to be satisfied as to a customer's or UBO's identity, must depend on the risk assessment for that customer or UBO (refer to Section 3.8).

36. All key documents (or parts thereof) used to verify the identity must be understandable (i.e. in a language understood by the employees of the Regulated Entity), and must be translated into English or Dutch at the request of the CBA or other relevant authorities, including the MOT.

3.6.1 IDENTIFICATION AND VERIFICATION: NATURAL PERSONS

37. The following requirements are relevant to situations where the person to be identified is a natural person.

3.6.1.1 Identification

REGULATORY REQUIREMENTS

38. A Regulated Entity must collect relevant identification information on a natural person.

GUIDANCE NOTES

39. A Regulated Entity may demonstrate collection of relevant identification information where it requests, receives, and keeps up to date the following information:

All Customers
• Legal name, any former names (such as maiden name) and any other names used. • Principal residential address. • Date of birth.
Additional information for standard and higher risk customers
• Place of birth. • Nationality. • Sex. • Government issued personal identification number or other government issued unique identifier such as a passport.

3.6.1.2 Verifying identity

REGULATORY REQUIREMENTS

40. Where a particular aspect of a natural person's identity subsequently changes (such as following marriage, change of nationality, or change of address), a Regulated Entity must take reasonable measures to re-verify that particular aspect of identity of the natural person.

GUIDANCE NOTES

41. A Regulated Entity may demonstrate that it has verified the identity of a natural person where it verifies the following components:

Lower risk – information to be verified
• Legal name, any former names (such as maiden name) and any other names used. • Principal residential address or date of birth. using at least one identification verification method.
Standard risk – information to be verified
• Legal name, any former names (such as maiden name) and any other names used; • Principal residential address; • Date of birth; • Place of birth; • Nationality; and • Sex. using at least two identification verification methods.
Higher risk – information to be verified
• Legal name, any former names (such as maiden name) and any other names used; • Principal residential address; • Date of birth; • Place of birth; • Nationality; • Sex; and • Government issued personal identification number or other government issued unique identifier. using at least two identification verification methods. Refer to Section 3.12 for enhanced CDD requirements for higher risk relationships

42. Components of identity may be verified using the following methods:

General identification information:

I. Dutch nationals whether or not residing in Aruba – identification verification methods:

- A valid travel document in the sense of the Passport Act (*Paspoortwet*, Stb. 1991, 498; AB, 121);
- A valid driver's license as referred to in Article 10, first or second section, of the State Ordinance on Road Traffic (*Landsverordening wegverkeer*, AB 1997, no. 18);
- A valid identity card as referred to in the Identity Cards Ordinance (*Landsverordening identiteitskaarten*, AB 2001, no. 8).

II. Non-Dutch nationals residing in Aruba:

- A travel document issued by a competent agency in the country of origin of the holder for the purposes of identification at home and abroad. This travel document must be authenticated and be provided with a registration number, photograph, and a signature of the holder and shall at least contain the following additional data:
  a. the surname and the given name(s);
  b. the date and place of birth;
  c. the gender;
  d. the issuing country and the name and capacity of the agency of this issuing country;
  e. the date and place of issue;
  f. the expiry date;
  g. the territorial validity of the document;
- A valid driver's license as referred to in Article 10, first or second section, of the State Ordinance on Road Traffic (AB 1997, no. 18);
- A valid identity card as referred to in the Identity Cards Ordinance (AB 2001, no. 8).

III. Non-Dutch nationals not residing in Aruba:

- A travel document issued by a competent agency in the country of origin of the holder for the purposes of identification at home and abroad. This travel document must be authenticated and be provided with a registration number, photograph, and a signature of the holder and shall at least contain the following additional data:
  a. the surname and the given name(s);
  b. the date and place of birth;
  c. the gender;
  d. the issuing country and the name and capacity of the agency of this issuing country;
  e. the date and place of issue;
  f. the expiry date;
  g. the territorial validity of the document.

Residential address:
• Correspondence from a central or local government department or agency. • A letter of introduction confirming residential address from a service provider as meant in Article 15 or 16 of the AML/CFT State Ordinance. • Personal visit to the residential address. • A bank statement or utility bill. • One of the general identification information sources listed above. • Independent data sources (including electronic sources).

43. Where a Regulated Entity is not familiar with the form of the evidence obtained to verify the identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

44. When applying reasonable measures to the re-verification of identity following a change in a particular aspect of identity, e.g. a change of address, or following the expiration of an identification document a Regulated Entity may apply a risk based approach which focuses on higher risk customers.

45. Independent data sources can provide a wide range of confirmatory material on a customer insofar it concerns other data (not including verification of identity). These are becoming increasingly accessible, for example, through improved availability of public information and the emergence of commercially available data sources such as electronic databases and research firms. Sources include:

    - Telephone directories.
    - Credit reference agency checks.
    - Business information services.
    - Electronic checks provided by commercial agencies.

3.6.1.3 Verification of residential address of overseas residents

OVERVIEW

46. On occasions, a natural person that resides abroad may be unable to provide evidence of his principal residential address using the verification methods set out at Section 3.6.1.2. Examples of such natural persons include residents of countries without postal deliveries and few street addresses, who rely upon post office boxes or employers for delivery of mail, and residents of countries where, due to social restraints, private addresses may not be verified by personal visits.

47. It is essential for law enforcement purposes that a record of a residential address (or details of how that natural person's place of residence may be reached) be recorded.

REGULATORY REQUIREMENTS

48. A Regulated Entity must determine that there is a valid reason for a customer being unable to satisfy its more usual verification of address requirements, and must document that reason.

49. Where alternative methods to verify address are relied on, a Regulated Entity must consider whether enhanced monitoring of activity and transactions is appropriate.

50. A Regulated Entity should not (i) only record a post office box number as an address, or (ii) fail to take steps to verify that a residential address is valid when establishing a customer relation and when subsequently keeping it up to date in accordance with periodic risk based reviews.

GUIDANCE NOTES

51. Where a natural person has a valid reason for being unable to produce more usual documentation to verify residential address, satisfactory verification of address may be established by:

- Verification of a "locator" address – a locator address is an address at which it would normally be possible to physically meet or contact a natural person (with or without prior arrangement), for example, a natural person's place of work.

- A written confirmation received from a natural person satisfying the criteria for a suitable certifier (see Section 3.12.1.1) that confirms residential address and that the certifier has visited the natural person at that address.

3.6.2 IDENTIFICATION AND VERIFICATION: LEGAL PERSONS (EXCEPT FOUNDATIONS)

OVERVIEW

52. The following requirements are relevant to situations where the customer is a legal person (except a foundation).

53. The requirements also apply to situations where a legal person is an UBO of a customer, or is a third party (underlying customer) on whose behalf a customer is acting.

3.6.2.1 Establishing identity

REGULATORY REQUIREMENTS

54. A Regulated Entity must collect relevant identification information on a legal person (and any subsequent changes).

55. A Regulated Entity must collect relevant identification information on the UBOs of the legal person (and any subsequent changes).

GUIDANCE NOTES

56. A Regulated Entity may demonstrate collection of identification information which is reliable, independent and relevant where it requests, receives and keeps up to date the following information and requests and receives from the legal person certain assurances.

All customers (and UBOs where different)
• Name of body. • Any trading names. • Date and country of incorporation/registration. • Official identification number. • Registered office address. • Mailing address (if different). • Principal place of business/operations (if different). • Names of all directors (or equivalent). Identification information of directors (or equivalent) who have authority to operate a relationship or to give the Regulated Entity instructions concerning the use or transfer of funds or assets – in line with guidance for natural persons.

57. The assurances are that the legal person has provided all of the information requested, and that it will update the information provided in the event of subsequent change.

3.6.2.2 Verifying identity

REGULATORY REQUIREMENTS

58. A regulated Entity must verify the identity of the legal person.

59. A Regulated Entity should take reasonable measures to verify the UBOs of the legal person and any subsequent changes (in line with guidance for natural persons and trustees).

GUIDANCE NOTES

60. A Regulated Entity may demonstrate that it has verified the identity of a legal person where it verifies the following components:

All customers:
• Name of body. • Date and country of incorporation/registration. • Official identification number.
Standard and higher risk – additional verification:
• Registered office address. • Principal place of business/operations (where different to registered office).

61. Components of identity may be verified using one or more of the following verification methods:

Lower risk – minimum one verification method:
• Company registry extract. • Notarial deed confirming the aforementioned components.
Standard and higher risk – minimum two verification methods:
• Certificate of incorporation (or other appropriate certificate of registration or licensing). • Memorandum and Articles of Association (or equivalent). • Company registry search. • Latest audited financial statements. • Independent data sources, including electronic sources, e.g. business information services. • Notarial deed confirming the aforementioned components. • Personal visit to principal place of business.

62. In case of a foreign legal person, the aforementioned verification methods are equally applicable. In addition a Regulated Entity may also verify the identity of a foreign legal person by obtaining reliable and internationally accepted documents, data, or information, or documents, data, or information that have been recognized by law in the state of origin of the customer as a valid means of identification.

63. A Regulated Entity may demonstrate that it has taken reasonable measures to verify the UBOs of the legal person where it verifies the identity of the following:

All customers:
• Natural persons holding an interest in the capital of the legal person of 25% or more or 25% or more of the voting rights in the legal person – in line with guidance for natural persons and trustees. • Those directors (or equivalent) who have authority to operate a relationship or to give the Regulated Entity instructions concerning the use or transfer of funds or assets – in line with guidance for natural persons. • Natural persons with ultimate effective control over the legal person's assets, including the natural persons comprising the mind and management of the legal person, e.g. directors – in line with guidance for natural persons. Refer to Section 3.12 for enhanced due diligence requirements for higher risk relationships.

64. Natural persons having ultimate effective control over a legal person will often include directors or equivalent. In the case of partnerships, associations, clubs, societies, charities, church bodies, etc., this will often include members of the governing body or committee plus executives.

65. Where a Regulated Entity is not familiar with the form of the evidence obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

66. Where a Regulated Entity verifies the identity of UBOs on a remote basis, reference should be made to the requirements and guidance set out in Section 4.12.1 for non-face to face identification and verification.

67. Where a director (or equivalent) holds this role by virtue of his employment by (or position in) a Regulated Entity that is a trust service provider, a Regulated Entity may demonstrate that it has taken reasonable measures to identify that person and to verify his identity where it obtains the following:

- the full name of the director; and
- an assurance from the trust service provider that the natural person is an officer or employee.

3.6.3 IDENTIFICATION AND VERIFICATION: FOUNDATIONS

68. The following requirements are relevant to situations where the customer is a foundation.

69. The requirements also apply to situations where a foundation is an UBO of a customer, or is a third party (underlying customer) on whose behalf a customer is acting.

3.6.3.1 Establishing identity

REGULATORY REQUIREMENTS

70. A Regulated Entity must collect relevant identification information on a foundation (and any subsequent changes).

71. A Regulated Entity must collect relevant identification information on the persons who are concerned with the foundation (and any subsequent changes).

GUIDANCE NOTES

72. A Regulated Entity may demonstrate collection of relevant identification information where it requests, receives and keeps up to date the following information and requests and receives form the foundation certain assurances.

All customers:
• Name of foundation. • Date and country of incorporation. • Type of foundation – charitable or otherwise. • Official identification number. • Registered business address. • Mailing address (if different). • Principal place of business/operations (if different). • Type of foundation (e.g. charitable). • Control structure and beneficiaries. • Nature of activities undertaking. • Geographical sphere of the foundation. • Identification information for all council members who have authority to operate a relationship or to give the Regulated Entity instructions concerning the use or transfer of

funds or assets – in line with guidance for natural persons and legal persons. • Identification information for the founder, a person (other than the founder of the foundation) who has endowed the foundation, and, if any rights a founder of the foundation had in respect of the foundation and its assets have been assigned to some other person, that person – in line with guidance for natural persons and legal persons.
Standard and higher risk – additional information:
• Identification information for all council members and, if any decision requires the approval of any other person, that person – in line with guidance for natural persons and legal persons. • Identification information on any beneficiary entitled to a benefit under the foundation in accordance with the charter or the regulations of the foundation – in line with guidance for natural persons and legal persons. • Identification information on any other beneficiary and person in whose favor the council may exercise discretion under the foundation in accordance with its charter or regulations and that have been identified as presenting higher risk – in line with guidance for natural persons and legal persons.

73. The assurances are that the foundation has provided all of the information requested, and that it will update the information provided in the event of subsequent change.

3.6.3.2 Verifying identity

REGULATORY REQUIREMENTS

74. A Regulated Entity must verify the identity of the foundation.

75. A Regulated Entity should take reasonable measures to verify the identity of persons who are concerned with the foundation and any subsequent changes of persons who are concerned with the foundation (in line with guidance for natural persons and legal persons).

GUIDANCE NOTES

76. A Regulated Entity may demonstrate that it has verified the identity of a foundation where it verifies the following components:

All customers:
• Name of foundation. • Date and country of incorporation. • Official identification number.
Standard and higher risk-additional verification:
• Business address. • Principal place of business/operations (if different).

77. Components of identity may be verified using one or more of the following verification methods:

Lower risk – minimum one verification method:
• Extract of Chamber of Commerce. • Notarial deed confirming the aforementioned components.
Standard and higher risk – minimum two verification methods:
• Charter (or equivalent). • Extract of Chamber of Commerce. • Latest (audited) financial statements. • Independent data sources, including electronic sources. • Notarial deed confirming the aforementioned components.

78. In case of a foreign foundation, the aforementioned verification methods are equally applicable. In addition a Regulated Entity may also verify the identity of a foreign foundation by obtaining reliable and internationally accepted documents, data, or information, or documents, data, or information that have been recognized by law in the state of origin of the customer as a valid means of identification.

79. Refer to Section 3.12 for enhanced due diligence requirements for higher risk relationships.

80. Where a Regulated Entity is not familiar with the form of the evidence obtained to verify identity, appropriate measures may be necessary to satisfy itself that the evidence is genuine.

81. Where a Regulated Entity verifies information on a remote basis, reference should be made to the requirements and guidance set out in Section 4.12.1 for non-face to face identification and verification.

82. Where a council member who is a natural person holds this role by virtue of his employment by (or position in) a Regulated Entity that is a trust service provider, a Regulated Entity may demonstrate that it has taken reasonable measures to identify that person and to verify his identity where it obtains the full name of the council member and an assurance from the trust service provider that the natural person is an officer or employee.

3.6.4 IDENTIFICATION AND VERIFICATION: TRUSTEES AND EXPRESS TRUSTS

OVERVIEW

83. Express trusts cannot form business relationships or carry out occasional transactions themselves. It is the trustee of the trust who will enter into a business relationship or carry out the occasional transaction on behalf of the trust and who will be considered to be the customer (i.e. the trustee is acting on behalf of a third party – the trust and the natural persons concerned with the trust).

84. The requirements set out in this section also apply to situations where a trustee is an UBO of a customer, or is a third party (underlying customer) on whose behalf a customer is acting.

3.6.4.1 Establishing identity

REGULATORY REQUIREMENTS

85. A Regulated Entity must collect relevant identification information on the trustee(s) and on the express trust (and any subsequent changes).

86. A Regulated Entity must collect relevant identification information on the natural persons who are concerned with the trust (and any subsequent changes).

GUIDANCE NOTES

87. A Regulated Entity may demonstrate the collection of relevant identification information where it requests, receives and keeps up to date the following information and requests and receives from the trustee(s) certain assurances:

All customers:
• Name. • Date of establishment. • Official identification number (e.g. tax identification number or registered charity or non-profit organization number). • Identification information of trustee(s) and the person(s) who otherwise exercise(s) effective control – in line with guidance for natural persons and legal persons. • Mailing address of trustee(s). • Identification information of settlor(s) – in line with guidance for natural persons and legal persons. • Identification information of UBO(s) with regard to the assets in the trust – in line with guidance for natural persons.
Standard and higher risk – additional information:
• Identification information on beneficiaries with a vested right – in line with guidance for natural persons and legal persons. • Identification information on any other beneficiaries and persons who are the object of a power and that have been identified as presenting higher risk – in line with guidance for natural persons and legal persons. • Refer to Section 3.12 for enhanced due diligence requirements for higher risk relationships.

88. The assurances are that the trustee(s) has/have provided all of the information requested, and that the trustee(s) will update the information provided in the event of subsequent change.

3.6.4.2 Verifying identity

REGULATORY REQUIREMENTS

89. A Regulated Entity must verify the name and date of establishment of the express trust. Whilst there is no requirement to review an existing trust instrument (or similar instrument) as a whole,

satisfactory evidence of the appointment of the trustee(s), and the nature of his duties must be obtained.

90. A Regulated Entity must verify the identity of the trustee(s) of the express trust and any subsequent change in trustee(s) (in line with guidance for natural persons and legal persons).

91. A Regulated Entity must take reasonable measures to verify the identity of the natural persons who are concerned with the express trust (as set out at Section 4.6.4.1) and any subsequent changes (in line with guidance for natural persons and legal persons).

92. In the case of a standard or higher risk relationship, a Regulated Entity must take reasonable measures to verify the identity of a beneficiary with a vested right at the time of or before distribution of trust property or income.

93. In the case of a standard or higher risk relationship, a Regulated Entity must take reasonable measures to verify the identity of any other beneficiaries and persons who are the object of a power and that have been identified as presenting higher risk, at the time that the risk is identified.

GUIDANCE NOTES

94. Where a Regulated Entity seeks to verify the identity of natural persons who are concerned with a trust on a non-face to face basis, for example, through copy documentation provided by the trustee(s), reference should be made to the requirements and guidance set out in Section 3.12.1 for non-face to face identification and verification.

3.7 RELATIONSHIP INFORMATION

OVERVIEW

95. As mentioned above CDD goes beyond the identification of customers and UBOs and the verification of their identity. This section describes the basic requirements regarding obtaining relationship information, in addition to identification information. Refer to Sections 3.11 and 3.12 for situations in which simplified CDD will be allowed or enhanced CDD will be required.

STATUTORY REQUIREMENTS

96. *Pursuant to Article 3, paragraph 1, subsection c, of the AML/CFT State Ordinance, a Regulated Entity must establish the purpose and intended nature of the business relationship*.

97. *Pursuant to Article 3, paragraph 1, subsection c, of the AML/CFT State Ordinance, a Regulated Entity must conduct on-going monitoring of the business relationship and the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Regulated Entity's knowledge of the customer, the UBO, their risk profile, including, where necessary, an assessment of the funds that are involved in the transaction or business relationship*.

98. *According to Article 5, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity must, if a customer is a legal person or arrangement, take reasonable measures that in any case lead to the Regulated Entity understanding the ownership and control structure of the customer. Moreover, if a customer is acting as a trustee of a trust or if the business relationship is entered into or if the transaction is performed in connection with the management of a trust, these reasonable measures must, according to Article 5, paragraph 3, of the AML/CFT State Ordinance, also lead to the settlor of the trust and the UBO to the assets of the trust being identified and their identity being verified*.

REGULATORY REQUIREMENTS

99. All key documents (or parts thereof) used to verify the identity must be understandable (i.e. in a language understood by the employees of the Regulated Entity), and must be translated into English or Dutch at the request of the CBA or other relevant authorities, including the MOT.

100. The extent of relationship information to be obtained in respect of a particular customer or UBO or type of customer or UBO, must depend on the risk assessment for that (type of) customer or UBO (refer to Section 3.8), including the jurisdiction with which the customer or UBO is connected, the characteristics of the product or service requested, how the product or service will be delivered, as well as other factors specific to the (type of) customer or UBO.

3.7.1 THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

GUIDANCE NOTES

101. A Regulated Entity may demonstrate collection of relevant relationship information where it requests, receives and keeps up to date the following information:

Relationship information:	
All customer types:	• Purpose and intended nature of relationship.[3] • Type, volume and value of activity expected. [4] • Details of any existing relationships with the Regulated Entity. • Reason for using overseas service provider (non-residents only).
Additional relationship information:	
Express trusts:	• Type of trust (e.g. fixed interest, discretionary, testamentary). • Structure of any underlying legal persons (if applicable) and nature of activities undertaken by the trust and any underlying legal persons. • Classes of beneficiaries, including any charitable causes named in the trust instrument. • Name of trustee's regulator, if applicable.

[3] With regard to banking business, refer to Appendix 1 for an example of a Transaction Profile Report.

[4] With regard to banking business, refer to Appendix 1 for an example of a Transaction Profile Report.

Legal persons:	• Entity and group (if applicable) ownership and control structure • Nature of activities undertaken. • Geographical sphere of the legal person's activities and assets. • Name of regulator, if applicable.
Foundations:	• Type of foundation (e.g. charitable) • Control structure. • Nature of activities. • Geographical sphere of the foundation. • Name of regulator, if applicable.

3.7.2 SOURCE OF FUNDS AND WEALTH

102. The ability to follow the audit trail for criminal funds and transactions flowing through the financial sector is a vital law enforcement tool in ML and FT investigations. Understanding the source of funds and, in higher risk relationships, the customer's source of wealth is also an important aspect of CDD.

GUIDANCE NOTES

103. A Regulated Entity may demonstrate that it has collected relevant relationship information by:

All customers:
• Taking reasonable measures to establish source of funds for each customer and, when third party funding is involved, making further enquiries as to the relationship between the person providing the funds and the customer.[5]
Higher risk – additional measures:
• Taking reasonable measures to establish a customer's source of wealth. • Considering whether it is appropriate to take measures to verify source of funds and wealth.

104. The AML/CFT State Ordinance and the Handbook stipulate record keeping requirements for transaction records, which require information concerning the remittance of funds to be recorded (e.g. the name of the bank and the name and account number of the account from which the funds were remitted). This is not to be confused with source of funds.

105. In determining source of wealth it will often not be necessary to establish the monetary value of a person's net worth.

[5] With regard to banking and money transfer business, refer to Appendix 2 and 3, respectively, for an example of a Source Of Funds Declaration Form.

3.8 RISK PROFILE

STATUTORY REQUIREMENTS

106. *Pursuant to Article 6, paragraph 3, of the AML/CFT State Ordinance, a Regulated Entity must establish a risk profile of the customer and the UBO*.

REGULATORY REQUIREMENTS

107. The process of determining an appropriate risk profile must take into account the absence or presence of relevant factors, whether any compensating factors apply and the CDD information held by the Regulated Entity.

108. The sophistication of the risk assessment process must be determined according to factors established by the business risk assessment.

109. A customer or UBO risk profile must, in any event, contain sufficient information to enable a Regulated Entity to:

- identify a pattern of expected business activity and transactions within each business relationship; and

- identify unusual or higher risk activity and transactions that may indicate ML or FT activity.

GUIDANCE NOTES

110. A Regulated Entity may demonstrate an effective process to conduct an initial customer risk assessment and determine a customer risk profile by taking into account:

- the CDD information (identification and relationship information) obtained and the evaluation of this information carried out against relevant “factors to consider” and external data sources; and

- inconsistencies between the CDD information obtained, for example, between specific information concerning source of funds or source of wealth, and the nature of transactions.

111. In determining a risk profile for a customer, the presence of one factor to consider that might indicate higher risk will not automatically establish that a customer is higher risk. Equally, the presence of one lower risk factor should not automatically lead to a determination that a customer is lower risk.

112. Where it is appropriate to do so, risk may be assessed generically for customers falling into similar categories. For example, the business of some Regulated Entities, their products, and customer base, can be relatively simple, involving few products, with most customers falling into similar risk categories. In such circumstances, a simple approach may be appropriate for most customers, with the focus being on those customers who fall outside the norm.

113. A more complex system may be appropriate for diverse customer bases or Regulated Entities with broad ranges of products or services.

3.8.1 FACTORS TO CONSIDER

GUIDANCE NOTES

114. The following factors may be relevant when assessing and evaluating the relationship information, and are not exhaustive. A Regulated Entity should consider whether other variables are appropriate factors to consider in the context of the products and services that it provides and its customer base. Where this evaluation of CDD information highlights a higher risk, then it may prove necessary to request further information.

Country risk:
• Residence in or connection with higher risk jurisdictions. The following jurisdictions may be considered to present a higher risk: o those that are generally considered to be un-cooperative in the fight against ML and FT; o those that have inadequate AML/CFT safeguards in place; o those that have high levels of organized crime; o those that have strong links (such as funding or other support) with terrorist activities; o those that are vulnerable to corruption; and o those that are the subject of UN or EU sanctions measures or prescribed persons or organizations listed by the OFAC. In assessing which jurisdictions may present a higher risk, objective data published by the IMF, FATF (whether or not circulated by the CBA), World Bank, the Egmont Group of Financial Intelligence Units, US Department of State (International Narcotics Control Strategy Report), OFAC, and Transparency International (Corruption Perception Index) will be relevant. • Geographical sphere of business activities, e.g. the location of the markets in which a customer does business. • Familiarity of a Regulated Entity with a country, including knowledge of its local legislation, regulations and rules, as well as the structure and extent of regulatory oversight, for example, as a result of a Regulated Entity's own operations within that country.
Product or service risk:
• Ability to make payments to third parties. • Ability to pay in or withdraw cash. • Ability to migrate from one product to another. • Ability to hold boxes, parcels or sealed envelopes in safe custody. • Ability to use numbered accounts. • Ability to use "hold mail" facilities. • Ability to pool underlying customers. • Ability that the account is used as a trust account (*derdengeldenrekening*). • Mechanism or instrument that could be used to finance activity-based financial prohibitions (i.e. prohibitions on provision of financial services related to the supply, sale, transfer, manufacture or use of prohibited items, materials, equipment, goods and technology). • Ability to redeem a life insurance policy very soon after purchasing it. • Ability to fund insurance policies by third parties/persons different to the policyholder who have not been subjected to the regular identification procedures when the insurance contract was concluded.

- Ability to use large premium deposits to fund annual premiums.
- The provision of a back-to-back loan (the Regulated Entity makes available funds or financial instruments to a customer and receives collateral, whether direct or indirect, from the customer's own liquid assets).

Delivery risk:

- Indirect relationship with the customer – use of third parties.
- Non-face to face relationships – product or service delivered exclusively by post, telephone, internet etc.
- Availability of “straight-through processing” of customer transactions.

Customer risk:

- Type of customer. For example, a PEP will present a higher risk.
- Nature and scope of business activities generating the funds/assets. For example, a customer conducting activities which are prohibited if carried on with certain countries; a customer engaged in higher risk trading activities; or a customer engaged in a business which involves significant amounts of cash, may indicate higher risk.
- Transparency of customer. For example, persons that are subject to public disclosure rules, e.g. on exchanges or regulated markets (or consolidated subsidiaries of such persons), or subject to licensing by a statutory regulator, may indicate lower risk. Customers where the structure or nature of the entity or relationship makes it difficult to identify the true UBOs may indicate higher risk.
- Reputation of a customer. For example, a well known, reputable person, with a long history in its industry, and with abundant independent information about it and its UBOs may indicate lower risk.
- Behavior of a customer. For example, where there is no commercial rationale for a customer buying the products that he seeks, requests undue levels of secrecy, or where it appears that an “audit trail” has been deliberately broken or unnecessarily layered, a customer may indicate higher risk.
- The regularity or duration of the relationship. For example, longstanding relationships involving frequent customer contact that result in a high level of understanding of the customer relationship may indicate lower risk.
- Type and complexity of relationship. For example, unexplained use of corporate structures and express trusts or foundations, and use of nominee and bearer shares may indicate higher risk.
- Value of assets handled.
- Value and frequency of cash or other “bearer” transactions.
- Delegation of authority by the customer. For example, the use of powers of attorney, representative offices may indicate higher risk.
- Nature of the relationship between a customer’s UBOs and account signatories.
- In the case of an express trust or foundations, the relationship of the settlor(s) or founder(s) to beneficiaries with a vested right, to other beneficiaries and persons who are the object of a power. (See also Section 3.6.4.)
- In the case of an express trust or foundation, the nature of classes of beneficiaries and classes within an expression of wishes. (See also Section 3.6.4)

3.8.2 EXTERNAL DATA SOURCES

GUIDANCE NOTES

115. Appropriate external data sources will include sources such as domestic legislation applying UN and EU sanctions and measures, and guidance issued by the CBA, and may include information published by governments and law enforcement authorities on terrorists (e.g. government agencies such as the Federal Bureau of Investigation and OFAC), electronic subscription databases, the internet and other media.

116. In particular, the CBA maintains a consolidated list of targets listed by the UN. Moreover, DNB maintains a consolidated list of targets listed by the EU.

3.9 UPDATING CDD AND CUSTOMER RISK PROFILES

STATUTORY REQUIREMENTS

117. *According to Article 7 of the AML/CFT State Ordinance, a Regulated Entity must ensure that the data, documents and information obtained through the a CDD process are kept up to date and relevant, in particular if it concerns customers, UBOs or business relationships that pose a higher risk of ML or FT*.

GUIDANCE NOTES

118. In the case of a business relationship assessed as presenting higher risk, a Regulated Entity may demonstrate that its CDD information remains up to date where it is reviewed and updated on at least an annual basis.

119. In the case of other relationships, a Regulated Entity may demonstrate that its CDD information remains up to date where it is reviewed and updated on a risk sensitive basis, including where additional "factors to consider" become apparent.

120. Trigger events, e.g. the opening of a new account, the purchase of a further product, or meeting with a customer may also present a convenient opportunity to update CDD information.

121. A comprehensive understanding of the risk presented by a business relationship may only become evident at a later stage following the establishment of relationship. A Regulated Entity may demonstrate that its customer risk assessments remain up to date where its review procedures (as outlined above), and its monitoring procedures (Section 4) involve consideration as to the on-going appropriateness of the customer's risk assessment.

3.10 AUTHORISED REPRESENTATIVES

STATUTORY REQUIREMENTS

122. *According to Article 5, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must, if a customer is a legal person or arrangement, (i) verify that a natural person purporting to act on behalf of the customer is authorized to do so; (ii) identify that natural person and verify that natural person's identify; and (iii) record information on the legal status and provisions regulating the power to bind the legal person or arrangement*.

REGULATORY REQUIREMENTS

123. A Regulated Entity must obtain a copy of the power of attorney (or other authority or mandate) that provides the natural persons representing the customer with the right to act on its behalf.

3.11 SIMPLIFIED CDD MEASURES

STATUTORY REQUIREMENTS

124. *Article 10 of the AML/CFT State Ordinance provides for simplified CDD measures as opposed to the basic CDD requirements described above*.

125. *Pursuant to Article 10, paragraph 1, subsection a, of the AML/CFT State Ordinance simplified CDD measures may be applied when it concerns the following clients*:

- *a Regulated Entity;*
- *a foreign financial service provider, provided it is subject to the internationally accepted AML/CFT requirements and it is supervised with regard to the compliance with these requirements;*
- *public limited companies and comparable entities, which are subject to statutory requirements with regard to the disclosure of their financial reporting and the shares of which are traded on recognized stock exchanges as designated by regulation of the Minister of Finance.*
- *public limited companies of which all shares are held by the State of Aruba (Land Aruba);*
- *the State of Aruba (Land Aruba) and other public legal persons established in Aruba;*
- *public legal persons established and active in other parts of the Kingdom of the Netherlands.*

126. Pursuant to Article 10, paragraph 1, subsection b, of the AML/CFT State Ordinance simplified CDD measures may be applied when it concerns the following transactions or business relationships:

- *a life insurance agreement of which the annual premium does not exceed Afl. 1,500.-, or of which the amount of the single premium does not exceed Afl. 4,000.-;*
- *a pension or a similar arrangement intended to provide an employee with a retirement benefit, in which the contributions for the benefit of the pension schemes are made through deductions from the salary of the employee, and the employee is not allowed to assign, pledge, or transfer as security his rights arising from the pension scheme to third parties;*
- *ultimate beneficiaries to accounts kept with a designated non-financial service provider intended solely for the keeping of money for third parties, provided these service providers are subject to AML/CFT regulations that comply with the internationally accepted AML/CFT requirements and that they are effectively supervised with regard to the compliance with these requirements.*

127. Pursuant to Article 10, paragraph 2 of the AML/CFT State Ordinance, a Regulated Entity must collect sufficient data to be able to establish whether simplified CDD measures may be applied.

128. Pursuant to Article 10, paragraph 3 of the AML/CFT State Ordinance, a Regulated Entity must not apply simplified CDD measures if the customer, business relationship or transaction carries a higher risk for ML or FT of if there are indications that the customer is involved with ML or FT.

GUIDANCE NOTES

129. A Regulated Entity may demonstrate that it has adequately determined that a jurisdiction's requirements comply with internationally accepted AML/CFT requirements (i.e. the FATF Recommendations), if the Regulated Entity has considered the following:

- whether or not the jurisdiction is a member of the FATF, a member state of the EU, a member of the EEA, or a part of the Kingdom of the Netherlands;
- the legislation and other requirements in place in the jurisdiction;
- recent independent assessments of that jurisdiction's AML/CFT framework, such as those conducted by the FATF, the World Bank and the IMF; and
- other publicly available information concerning the effectiveness of a jurisdiction's AML/CFT framework.

130. The following may be considered to be public legal persons established in Aruba:

- The Government of Aruba (Land Aruba);
- Government-owned public limited company, but not public limited companies or entities owned wholly or partially by these public limited companies;
- An entity established by law of Aruba (e.g. CBA, AZV, SVB).

131. The following may be considered to be public entities within the Kingdom of the Netherlands:

- The Government of the Netherlands (*Staat der Nederlanden*);
- The Government of Curaçao (*Land Curaçao*);
- The Government of St. Maarten (*Land St. Maarten*);
- An entity established by law of the Netherlands, Curaçao or St. Maarten (e.g. DNB, CBCS).

3.12 ENHANCED CUSTOMER DUE DILIGENCE

STATUTORY REQUIREMENTS

132. *Pursuant to Article 11 of the AML/CFT State Ordinance, a Regulated Entity must perform enhanced CDD if and when a business relationship or a transaction by its nature entails a higher risk of ML or FT. Enhanced CDD must be performed prior to the business relationship or the transaction as well as throughout the course of the business relationship, in any case in the following situations:*

- *when a client is not a resident of Aruba, respectively not established in Aruba;*
- *if a client is not physically present for identification;*
- *if it concerns private banking;*
- *with legal persons, trusts and comparable entities that are intended as private assets holding vehicles;*

- *with bodies corporate and comparable entities with shares in bearer form or nominee shareholders;*

- *with natural persons, legal persons, trusts and comparable entities that originate from countries or jurisdictions which do not or insufficiently apply the internationally accepted AML/CFT standards;*

- *with PEPs;*

- *when entering into correspondent banking relations;*

- *other situations to be determined by regulation of the Minister of Finance.*

133. *Pursuant to Article 13, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must pay special attention to:*

    - *business relationships and transactions with natural persons, legal persons, trusts and comparable entities originating from countries or jurisdictions that do not, or insufficiently comply with the internationally accepted AML/CFT standards;*

    - *all complex and unusual large transactions and to all unusual patterns of transactions, which have no apparent economic or lawful purpose.*

134. *If a Regulated Entity can reasonably suspect that a transaction with a natural person, legal person, trust or a comparable entity originating from a country or jurisdiction as meant in paragraph 134 does not have an apparent economic or lawful purpose, or if a transaction as meant in paragraph 134 should arise, it must, pursuant to Article 13, paragraph 2, of the AML/CFT State Ordinance, examine the background and the purpose of such transactions and record its findings in writing. In accordance with Article 13, paragraph 3, of the AML/CFT State Ordinance, these findings must be kept for at least ten years*.

135. *Pursuant to Article 14 AML/CFT State Ordinance, a Regulated Entity must pursue an adequate policy and have adequate procedures in place aimed at the prevention of the misuse of new technological developments and instruments for ML and FT. These procedures must particularly address any risks associated with non-face to face business relationships and transactions*.

3.12.1 NON-FACE TO FACE IDENTIFICATION AND VERIFICATION

OVERVIEW

136. Frequently, relationships will be established where there is no face to face contact with the natural persons to be identified, for example:

    - relationships established by natural persons through the post, by telephone or via the internet; and

    - where identification information is provided through a trustee on persons who are concerned with a trust, or by a company on the persons who are its UBOs.

137. There may also be circumstances where there is face to face contact with a natural person, but where documentary evidence is to be provided at a time when the natural person is not present.

138. This section contains requirements that are relevant where there has been no face to face contact with a natural person, and where documentary evidence is to be provided at a time when the natural person is not present.

REGULATORY REQUIREMENTS

139. Where a business relationship is established or occasional transaction conducted remotely, or where the identity of a natural person is to be verified using documentary evidence when the natural person is not physically present, a Regulated Entity must perform an additional check to reduce the risk of identity fraud.

GUIDANCE NOTES

140. A Regulated Entity may demonstrate that the specific additional check undertaken is appropriate where it takes into account the customer risk assessment, matching the level of assurance given by the check to the risk presented by the customer.

141. Additional checks to reduce the risk of identity fraud may include:

- Verification of identity using a further verification method listed in Section 3.6.1.
- Obtaining copies of identification documents certified by a suitable certifier (see below).
- Requiring the first payment for the financial services product or service to be drawn on an account in the customer's name at a bank that is a Regulated Person or a foreign financial service provider, provided it is subject to the internationally accepted AML/CFT requirements and it is supervised with regard to the compliance with these requirements.
- Telephone contact with the customer prior to establishing a business relationship on a home or business number which has been verified, or a "welcome call" to the customer before transactions are permitted, using the call to verify additional aspects of CDD information that have been previously provided.
- Internet sign-on following verification measures where the customer uses security codes, tokens, and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address.
- Specific card or account activation measures.

3.12.1.1 Suitable certifiers

OVERVIEW

142. Use of a certifier guards against the risk that copy documentation provided is not a true copy of the original document and that the documentation does not correspond to the customer or UBO whose identity is to be verified.

REGULATORY REQUIREMENTS

143. A suitable certifier must be subject to professional rules of conduct, which provide comfort as to the integrity of the certifier.

144. A suitable certifier must certify that:

- he has seen original documentation verifying identity and/ or residential address;
- the copy of the document (which he certifies) is a complete and accurate copy of that original; and
- where the documentation is to be used to verify identity of a natural person and contains a photograph, the photograph contained in the document certified bears a true likeness to the natural person requesting certification,
- or use wording to the same effect.

145. The certifier must also sign and date the copy document, and provide adequate information so that he may be contacted in the event of a query.

146. In circumstances where the suitable certifier is located in a higher risk jurisdiction, or where a Regulated Entity has some doubts as to the veracity of the information or documentation provided by the customer, the Regulated Entity must take steps to check that the suitable certifier is real.

GUIDANCE NOTES

147. Acceptable persons to certify evidence of identity (suitable certifiers) may include:

- a member of the judiciary;
- an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;
- a civil notary.

3.12.2 HIGHER RISK COUNTRIES AND JURISDICTIONS

REGULATORY REQUIREMENTS

148. Regulated Entities must treat countries and jurisdictions listed in the FATF statements (circulated by the CBA), highlighting jurisdictions which do not or insufficiently apply the FATF Recommendations or which are the subject of international countermeasures, as countries and jurisdictions that do not or insufficiently apply the internationally accepted AML/CFT standards. These letters circulated by the CBA will be numbered sequentially and placed in the designated area “Financial Sanctions” on the CBA’s website.

3.12.3 PEPS

OVERVIEW

149. Corruption inevitably involves serious crime, such as theft or fraud, and is of global concern. The proceeds of such corruption are often transferred to other jurisdictions and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates.

150. By their very nature, ML investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both businesses and jurisdictions concerned. This is in addition to the possibility of criminal charges.

151. Indications that a customer may be connected with corruption include excessive revenue from "commissions" or "consultancy fees" or involvement in contracts at inflated prices, where unexplained "commissions" or other charges are paid to third parties.

152. The risk of handling the proceeds of corruption, or becoming engaged in an arrangement that is designed to facilitate corruption, is greatly increased where the arrangement involves a PEP. Where the PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

153. PEP status itself does not, of course, incriminate natural persons or entities. It will, however put an customer into a higher risk category.

STATUTORY REQUIREMENTS

154. *Pursuant to Article 12, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must pursue an adequate policy and have risk-oriented procedures in place to determine whether a customer, a potential customer or a UBO is a PEP. A Regulated Entity must have procedures in place to determine the source of wealth of customers and UBOs who are considered PEPs*.

155. *Pursuant to Article 12, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity that enters into a business relationship or carries out a transaction for a PEP must ensure that: (a) the decision to enter into the business relationship or the performance of the occasional transaction is made or approved by senior management; (b) on-going monitoring on the business relationship is conducted*.

156. *Where, after the commencement of the business relationship, a customer or UBO is subsequently considered a PEP, a Regulated Entity must, pursuant to Article 12, paragraph 3, of the AML/CFT State Ordinance, have the continuation of the business relationship approved by senior management*.

157. *Pursuant to Article 12, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity must consider a customer, a potential client or an UBO a PEP up to five years after he has ceased to occupy the prominent public position. This equally applies to this person's close associates*.

GUIDANCE NOTES

158. For the purposes of determining whether a person is a close associate of a PEP, a Regulated Entity need only consider information that it holds or is publicly known.

159. A Regulated Entity may demonstrate that it has appropriate policies, procedures and measures for determining whether it is servicing a PEP where it:

- Considers in any case the persons who are or have been charged with the following positions as PEPs:
    - heads of state, heads of government, ministers and state secretaries;
    - members of parliament;
    - members of supreme courts, constitutional courts and other high tribunals that render judgments that generally are not open to appeal;
    - members of courts of auditors and boards of directors of central banks;

- members of directors of central banks;
- ambassadors and chargés d'affaires;
- high-ranked army officers;
- members of executive, management or supervisory bodies of state companies;
- positions held at an international level, such as representative with the United Nations;

- Considers direct family members and close associates as PEPs.
- Assesses whether the customer or a UBO holds a prominent public function in Aruba.
- Assesses those jurisdictions with which customers or UBOs are connected, which pose the highest risk of corruption. One source of information is the Transparency International Corruption Perception Index.
- Establishes who are the current and former holders of prominent public functions within those higher risk countries and determines, as far as is reasonably practicable, whether or not customers have any connections with such natural persons (including through immediate family or close associates). In determining who are the current and former holders of prominent public functions, it may have regard to information already held by the Regulated Entity and to external information sources such as the UN, the European Parliament, the Group of States Against Corruption (Greco), and commercially available databases.
- Exercises vigilance where customers or UBOs are involved in business sectors that are vulnerable to corruption such as, but not limited to, oil or arms sales. One source of information is the Transparency International Corruption Perception Index.

3.12.4 CORRESPONDENT BANKING

OVERVIEW

160. Correspondent banking is a term given to the provision of services by one bank (the "correspondent") to another bank (the "respondent") for the benefit of the customers of the respondent. As a result, the correspondent bank indirectly makes its services available to the customers of the respondent business; in doing so, the correspondent potentially exposes itself to additional risk. This section sets out the additional CDD measures required where a bank enters into a correspondent banking relationship to appropriately manage the risk presented by that relationship.

STATUTORY REQUIREMENTS

161. *Pursuant to Article 17, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity, being a bank as meant in the SOSCS, that intends to enter into a correspondent banking relationship must ensure that:*

- *it gathers sufficient information about the respondent bank to understand fully the nature of the respondent's business and the reputation of the respondent bank and the quality of supervision exercised over this bank, including information about any investigations regarding ML and FT or supervisory measures taken;*

- *it assesses the respondent bank's AML/CFT procedures and measures and ascertains that these procedures and measures are adequate and effective;*

- *the respective AML/CFT responsibilities of each bank are recorded in writing.*

162. *Pursuant to Article 17, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity, being a bank as meant in the SOSCS, must only enter into a new correspondent banking relationship after a decision made to this effect by senior management*.

163. *If a correspondent banking relationship involves the maintenance of "payable-through accounts", a Regulated Entity, being a bank as meant in the SOSCS, must, pursuant to Article 17, paragraph 3, of the AML/CFT State Ordinance, ascertain that the respondent bank has identified its customers that have direct access to these payable-through accounts, and that it has verified their identity in accordance with the internationally accepted standards for identification and identity verification. The Regulated Entity must also ascertain that the respondent bank is able to provide all relevant customer identification information upon request*.

164. *Pursuant to Article 18 of the AML/CFT State Ordinance, a Regulated Entity, being a bank as meant in the SOSCS, must not enter into or maintain a correspondent banking relationship with a shell bank. Regulated Entities, being banks as meant in the SOSCS, must ascertain that foreign financial service providers, with which they enter into or maintain a correspondent banking relationship, do not have their accounts used by shell banks. If such a situation nevertheless occurs, the Regulated Entity must promptly end the correspondent banking relationship*.

REGULATORY REQUIREMENTS

165. A Regulated Entity, being a bank as meant in the SOSCS, must inform the CBA immediately after senior management has decided to enter into a correspondent banking relationship.

GUIDANCE NOTES

166. A Regulated Entity that is a correspondent bank may demonstrate that it has gathered sufficient information about the respondent to understand fully the nature of its business where it obtains information concerning the following:

- the geographic location of the customer base;

- the general nature of the customer base;

- the nature of the services which the respondent provides to its customers;

- whether relationships are conducted by the respondent on a non-face to face basis; and

- the extent to which the respondent relies on third parties to identify and hold evidence of identity or to conduct other CDD measures on customers.

167. A Regulated Entity that is a correspondent bank may also determine the reputation of a respondent by assessing its stature, using, inter alia, public sources such as the Bankersalmanac.com Due Diligence Repository.

168. A Regulated Entity that is a correspondent bank may also determine quality of supervision exercised over a respondent by considering the independent assessments of that respondent's jurisdiction's AML/CFT framework, such as those conducted by the FATF, the World Bank and the IMF.

169. Where customers of the respondent have direct access to the services of the correspondent bank, a Regulated Entity that is a correspondent bank may satisfy itself as to the adequacy of a respondent's CDD measures, and its ability to provide relevant CDD information and documents on request where it obtains a written assurance from the respondent to this effect. The correspondent bank may also satisfy itself as to the adequacy of the CDD measures of the respondent and its ability to produce information and documentation on request by periodically requesting relevant CDD information and documents.

170. If other measures do not suffice, a Regulated Entity that is a correspondent bank may visit the respondent at their premises prior to or within a reasonable period of time after establishing a correspondent banking relationship, amongst other things to confirm that the respondent is not a shell bank.

3.12.5 ENHANCED CDD FOR OTHER HIGH RISK CUSTOMERS

GUIDANCE NOTES

171. A Regulated Entity may demonstrate that it has applied enhanced CDD measures to higher risk customers where it undertakes one of more of the measures set out below. The nature of the measures to be applied will depend on the circumstances of the business relationship or transaction and the factors leading to the customer being considered to be higher risk.

172. Enhanced CDD measures include:

- obtaining further CDD information (identification information and relationship information, including further information on the source of funds and source of wealth), from either the customer or independent sources (such as the internet, public or commercially available databases);
- taking additional steps to verify the CDD information obtained;
- commissioning CDD reports from independent experts to confirm the veracity of CDD information held;
- requiring higher levels of management approval for higher risk new customers;
- requiring more frequent review of business relationships;
- requiring the review of business relationships to be undertaken by the compliance function, or other employees not directly involved in managing the customer; and
- setting lower monitoring thresholds for transactions connected with the business relationship.

3.13 INTRODUCING BUSINESS

OVERVIEW

173. An introduced relationship is where the introducer (an intermediary or other third party) has an established relationship with a customer and wishes to introduce that customer to a Regulated Entity. The customer seeks to form a direct relationship with a Regulated Entity. The customer will therefore have two direct relationships, one with the introducer and one with the Regulated Entity to which he has been introduced.

174. A Regulated Entity may rely on introducers that meet certain conditions to perform elements a, b, and c of Article 3, paragraph 3, of the AML/CFT State Ordinance, provided that the requirements set out in this section are complied with. This means that a Regulated Entity does not need to duplicate CDD measures that will have already been conducted by the introducer.

175. Examples of introducers include:

- Insurance intermediaries who arrange for their customers an insurance policy with an insurance company.

- Trust service providers who arrange for a bank or investment account, for example, to be established in the name of a client company, and not in the name of the trust service provider.

176. Outsourcing arrangements are not included within the scope of this section, as these are distinct from introduced relationships. In an outsourcing arrangement, the customer will have a direct relationship with a Regulated Entity and not with the third party carrying on the outsourced activity. Although the third party may have substantial contact with the customer, the customer is a customer of the Regulated Entity and not of the third party. The third party will be carrying on the outsourced activity for the Regulated Entity according to the terms of a contract with the Regulated Entity. (Refer to Section 2.8.)

STATUTORY REQUIREMENTS

177. *In accordance with Article 15 and 16 of the AML/CFT State Ordinance, a Regulated Entity should only rely on introducers being (i) Regulated Entities, (ii) Aruba-based designated non-financial service providers as meant in subsection 1° or 2° of the definition of "designated non-financial service provider" in Article 1, paragraph 1, of the AML/CFT State Ordinance; or (iii) service providers based in a country or jurisdiction designated by the Minister of Finance, notwithstanding that the ultimate responsibility for CDD remains with the Regulated Entity relying on the introducer*

178. *Pursuant to Article 15 and 16 of the AML/CFT State Ordinance, a Regulated Entity that relies on an introducer, must:*

- *satisfy itself that all relevant data, documents and information relating to the CDD conducted by the introducer will be made available to the Regulated Entity upon request without delay; and*

- *satisfy itself that the introducer has procedures and measures in place to comply with the CDD requirements and to record the relevant CDD information in line with Article 3 and 33 of the AML/CFT State Ordinance, respectively*.

REGULATORY REQUIREMENTS

179. A Regulated Entity must be able to demonstrate that the conditions required by the AML/CFT State Ordinance are met.

180. In order to rely on measures that have been conducted by an introducer under Articles 15 or 16, a Regulated Entity must first assess the risk in avoiding applying such measures or placing reliance. Where appropriate, it must take additional measures to manage its risk.

181. In order to demonstrate that a Regulated Entity has obtained sufficient information about the introduced customer, a Regulated Entity must:

- Obtain customer information profiles from the introducer on each of the introduced customers – in line with guidance for natural persons, legal persons (including foundations) and trustees –

set out in Sections 3.6 and 3.7. The information provided in the customer information profile will depend upon the Regulated Entity's assessment of the risk presented by a particular customer or UBO.

- Be satisfied that the introducer will notify the Regulated Entity of any material changes to the customer information profile provided.

182. All relevant data, documents and information relating to the CDD conducted by the introducer passed by the introducer to a Regulated Entity (on request) must be confirmed by the introducer as being a true copy of either an original or copy document held on its file.

183. In the event that an introducer terminates its relationship with a customer introduced to a Regulated Entity, the Regulated Entity must require the introducer to provide the Regulated Entity with:

- copies of the relevant data, documents and information relating to the CDD conducted by the introducer; or

- an assurance that the introducer will continue to hold the necessary data, documents and information on behalf of the Regulated Entity until such time as is agreed.

GUIDANCE NOTES

Risk assessment – factors to consider

184. One or more of the following factors will be relevant when conducting a risk assessment for an introducer:

- The stature and regulatory track record of the introducer.

- The adequacy of the AML/CFT framework in place in the jurisdiction in which the introducer is based and the period of time that the framework has been in place.

- The adequacy of the supervisory AML/CFT regime to which the introducer is subject.

- The adequacy of the AML/CFT measures in place at the introducer.

- Previous experience gained from existing relationships connected with the introducer.

- The nature of the business conducted by the introducer. Relevant factors include:

  - the geographic location of the customer base;

  - the general nature of the customer base, e.g. whether institutional or private client;

  - the risk appetite of the introducer; and

  - the nature of the services which the introducer provides to its customers.

- Whether relationships are conducted by the introducer on a face to face basis.

- Whether specific relationships are fully managed by an introducer.

- The extent to which the introducer itself relies on third parties to identify its customers and to hold evidence of identity or to conduct other CDD measures, and whether such third parties are regulated.

- Whether or not specific introduced relationships involve PEPs or other higher risk relationships.

Additional measures

185. Where, having assessed risk, a Regulated Entity determines that additional measures are required, these may include all, or some, of those listed below:

- Making specific enquiries of the introducer to determine the adequacy of AML/CFT measures in place.

- Reviewing the AML/CFT policies and procedures in place at the introducer.

- Where the introducer is a member of a financial services group, making enquiries concerning the extent to which group standards are applied to and assessed by the introducer's compliance function or internal audit function.

- Conducting (or commissioning from an external expert) periodic sample testing of the adequacy of the introducer's AML/CFT policies and procedures, whether through on-site visits, or through requesting specific CDD information and/or copy documentation to be provided.

- Requesting specific CDD information and/or copy documentation to be provided, to confirm that the introducer is able to satisfy any requirement for such information and documentation to be available without delay at the request of the Regulated Entity.

- Where an introduced relationship presents higher ML or FT risk, considering whether it is appropriate to rely solely upon the information provided by the introducer, and whether additional CDD information and/or documentation is required.

Access to CDD data, documents and information

186. A Regulated Entity may demonstrate that an introducer will provide CDD data, documents and information in relation to introduced customers, without delay where it requires relevant CDD data, documents and information to be made available within 5 working days of a request.

Group introducers

187. In the case that an introducer as meant in Article 15 or 16 of the AML/CFT State Ordinance is a company (branch or subsidiary) in the same group as the Regulated Entity, the Regulated Entity may demonstrate that it has satisfied itself that the Statutory Requirements are met where:

- The introducer is subject to group AML/CFT requirements;

- If it concerns a foreign introducer, the introducer is registered or otherwise authorized in another country and the conduct of the introducer's business is subject to supervision for compliance with group AML/CFT requirements.

3.14 CDD REQUIREMENTS WHEN ACQUIRING A BUSINESS OR BLOCK OF CUSTOMERS

OVERVIEW

188. This section establishes the requirements when established business relationships are taken on when acquiring a business or block of customers.

REGULATORY REQUIREMENTS

189. Before acquiring a business with established business relationships or a block of business relationships, a Regulated Entity must undertake sufficient due diligence on the vendor to establish the level of CDD information and evidence of identity held in relation to the business to be acquired.

190. A Regulated Entity should only rely on the information and evidence of identity previously obtained by the vendor where the following criteria are met:

- the vendor is a Regulated Person; and
- the Regulated Entity has assessed that the vendor's CDD procedures are satisfactory. This assessment must either involve sample testing, or alternatively an assessment of all relevant CDD for the relationships to be acquired.

191. When relying on this concession, a Regulated Entity must obtain from the vendor the CDD information and evidence of identity held for each customer acquired.

192. Otherwise, where the vendor is not a Regulated Person or where deficiencies in the vendor's CDD measures are identified (either at the time of transfer or subsequently), an acquiring business must determine and implement a program to apply CDD procedures on each customer and to remedy deficiencies.

193. The Regulated Entity must agree its program with the CBA.

194. CDD must be undertaken as soon as possible in line with a risk based approach and requirements set out in the Handbook.

4. WIRE TRANSFERS

4.1 OVERVIEW

1. The purpose of this section of the Handbook is to ensure that transfers of funds are accompanied by certain information on the payer. The Statutory Requirements set out in this section follow from the State Decree Regulation Wire Transfers, which is based on Article 6, paragraph 4, of the AML/CFT State Ordinance. The Statutory Requirements apply to Regulated Entities that are financial service providers as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance whose business includes carrying out wire transfers (payment service providers as meant in Article 1 of the State Decree Regulation Wire Transfers). The Statutory Requirements aim at preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs. The requirements differ depending on the role of the Regulated Entity (ordering, intermediary or beneficiary institutions).

2. Wire transfer means any transaction carried out on behalf of a payer (originator) through a Regulated Entity, being a payment service provider, by electronic means with a view to making funds available to a payee (beneficiary) at another payment service provider, irrespective of whether the payer and the payee are the same person.

3. A payer means a person who is an account holder who allows a wire transfer from that account or where there is no account, a person who places an order for a wire transfer. A payee means a person who is the intended final recipient of transferred funds.

4. This section also sets out exemptions to the general requirements which apply in certain scenarios.

4.2 EXEMPTIONS

STATUTORY REQUIREMENTS

5. *Pursuant to Article 2 of the State Decree Regulation Wire Transfers, the Statutory Requirements do not apply to the following wire transfers:*

- *wire transfers carried out using a credit or debit card, if*
    - *the payee has an agreement with the Regulated Entity permitting payment for the provision of goods and services; and*
    - *an unique identifier, allowing the transaction to be traced back to the payer, accompanies the wire transfer.*
- *wire transfers carried out by means of a mobile telephone or any other digital or information technology device, if:*
    - *the wire transfer is pre-paid; and*
    - *the transferred funds do not exceed Afl. 300.*
- *wire transfer where the payer withdraws cash from the payer's own account;*
- *Wire transfers where there is a debit transfer authorization between two parties permitting payments between them through accounts, provided an unique identifier accompanies the wire transfer to enable the transaction to be traced back;*

- *It is a wire transfer to Aruban public authorities for taxes, fines or levies;*

- *Both the payer and the payee are payment service providers acting on their own behalf.*

4.3 OBLIGATIONS OF THE ORDENING PAYMENT SERVICE PROVIDER

STATUTORY REQUIREMENTS

6. *Pursuant to Article 3, paragraph 1, of the State Decree Regulation Wire Transfers, the ordering Regulated Entity (the payment service provider of the payer) must ensure that qualifying wire transfers are accompanied by the complete information on the payer*.

7. *In accordance with Article 1 and Article 3, paragraph 2, of the State Decree Regulation Wire Transfers, the complete information on the payer must include the payer's full names, address and account number, except that:*

    - *the payer's address may be substituted with the payer's date and place of birth, customer identification number or national identity number as meant in Article 3, paragraph 1, subsection c, of the Identity Cards Ordinance (Landsverordening identiteitskaarten, AB 2001, no. 8);*

    - *In the absence of an account number, an unique identifier must be included, which allows the wire transfer to be traced back to the payer*.

8. *According to Article 3, paragraph 3, of the State Decree Regulation Wire Transfers, there are two exceptions to the above mentioned rule:*

    - *If the ordering and the beneficiary payment service provider are both situated in Aruba, the wire transfer should only be required to be accompanied by:*

        - *the payer's account number; or*

        - *an unique identifier allowing the transaction to be traced back to the payer.*

    However, if the beneficiary payment service provider so requests, the ordering payment service provider must, within three working days after the day on which the ordering payment service receives the request, make the complete information on the payer available to the beneficiary payment service provider.

9. *Pursuant to Article 4 of the State Decree Regulation Wire Transfers, the ordering payment service provider is not obliged to accompany the wire transfer with complete information on the payer in the case of a batch file transfer from a single payer, where some or all of the beneficiary payment service providers are situated outside Aruba, if:*

    - *the batch file contains the complete information on the payer; and*

    - *the individual wire transfers bundled together in the batch file carry the payer's account number or an unique identifier.*

10. *Pursuant to Article 8 of the State Decree Regulation Wire Transfers, the ordering payment service provider must keep for ten years the records of complete information on the payer that accompanies a wire transfer*.

4.4 OBLIGATIONS OF THE BENEFICIARY PAYMENT SERVICE PROVIDER

STATUTORY REQUIREMENTS

11. *Pursuant to Article 5 of the State Decree Regulation Wire Transfers, the beneficiary payment service provider must ascertain that fields within the messaging or payment and settlement system used to effect the wire transfer in respect of the information on the payer have been completed in accordance with the characters or inputs admissible within the conventions of that messaging or payment and settlement system. The beneficiary payment service provider must have effective procedures in place to identify wire transfers lacking complete information on the payer. Refer to Article 3 and 4 of the Statutory Requirements set out in paragraphs 6 to 9, for the respective requirements for wire transfers where the ordering payment service provider is situated in Aruba or abroad, or if it concerns a batch file transfer*.

12. *Pursuant to Article 6 of the State Decree Regulation Wire Transfers, the beneficiary payment service provider that becomes aware that required information on the payer is incomplete, must reject the wire transfer until it has received said information*.

13. *Pursuant to Article 8 of the State Decree Regulation Wire Transfers, the beneficiary payment service provider must keep for 10 years the records of any received information on the payer*.

REGULATORY REQUIREMENTS

14. If the ordering payment service provider regularly fails to supply complete information on the payer required by the State Decree Regulation Wire Transfers, the beneficiary payment services provider must report that fact to the CBA.

15. If the ordering payment service provider regularly fails to supply complete information on the payer required by the State Decree Regulation Wire Transfers, the beneficiary payment service provider must take steps to attempt to ensure that the ordering payment service provider complies with the requirements set out in this section.

16. If, after the beneficiary payment service provider has taken steps as set out above in relation to a ordering payment service provider, the requirements as to supply complete information on the payer are still not regularly complied with by the ordering payment service provider of the payer, the beneficiary payment service provider must either:

    - reject any future wire transfers from that payment services provider, or

    - decide whether or not to restrict or terminate its business relationship with that payment services provider, either with respect to wire transfer services or with respect to any supply of services.

17. Missing or incomplete information on the payer must be a factor in assessing whether a wire transfer, or any related transaction is to be regarded as unusual transactions for the purposes of the AML/CFT State Ordinance and subsequently reported to the MOT.

GUIDANCE NOTES

18. The beneficiary payment service provider may demonstrate that is has taken steps to attempt to ensure that the ordering payment service provider complies with the requirements set out in this section where it:

    - uses warnings to the ordering payment service provider; and

    - sets deadlines for the ordering payment service provider to comply with the requirements as to supply complete information on the payer.

4.5 OBLIGATIONS OF THE INTERMEDIARY PAYMENT SERVICE PROVIDER

STATUTORY REQUIREMENTS

19. *Pursuant to Article 7 of the State Decree Regulation Wire Transfers, an intermediary payment services provider must ensure that all received information on the payer that accompanies a wire transfer is retained with the transfer*.

20. *Pursuant to Article 8 of the State Decree Regulation Wire Transfers, an intermediary payment service provider must keep for ten years the records of any received information on the payer*.

4.6 PROCEDURES AND MEASURES

STATUTORY REQUIREMENTS

21. *Pursuant to Article 9 of the State Decree Regulation Wire Transfers, a payment services provider must have procedures and measures in place regarding:*

    - *The furnishing of information on the payer accompanying wire transfers and related documentary evidence to the CBA, upon request without delay;*

    - *the decision making regarding payment service providers that regularly fail to supply complete information on the payer.*

5. MONITORING ACTIVITY AND TRANSACTIONS

5.1 OVERVIEW

1. Section 3 addresses the capturing of sufficient information about a customer, a UBO and the business relationship that will allow a Regulated Entity to: develop a profile of expected activity to provide a basis for identifying unusual and higher risk activity and transactions.

2. This section requires a Regulated Entity to monitor business relationships and to:

   - identify and apply additional scrutiny to unusual and higher risk activity or transactions,

   - identify all transactions that meet specific objective tests

   so that ML or FT may be identified and, where possible, prevented. An effective monitoring system requires a Regulated Entity to identify unusual and higher risk activity, to maintain up to date CDD information and to ask pertinent questions to determine whether there is a rational explanation for the activity or transactions identified. The scrutiny of activity and transactions may involve requesting additional CDD information.

3. For some customers, a complete customer profile and appropriate risk assessment may only become evident once the relationship has been established, making monitoring of customer activity and transactions key to obtaining a complete understanding of business relationships.

4. Unusual activity or transactions may be identified as activity that is inconsistent with the expected pattern of activity within a particular relationship, or with the normal business activities for the type of product or service that is being delivered. Where a Regulated Entity's customer base is homogeneous, and where the products and services provided to customers result in uniform patterns of activity or transactions, it will be more straightforward to establish parameters to identify usual and unusual activity. However, where each customer is unique, and where the product or service provided is customized, a Regulated Entity will need to tailor monitoring systems to the nature of its business and facilitate the application of additional judgment and experience to the identification of unusual activity. For such businesses, appropriate staff training in the recognition of unusual activity is vital.

5. Monitoring procedures may involve both real time and post event monitoring. Real time monitoring will focus on activity and transactions when information or instructions are received from customers, before or as the instruction is processed. Post event monitoring may involve end of day, weekly, monthly or annual reviews of customer activity and transactions. Real time monitoring of activity will be more effective at reducing a Regulated Entity's exposure to ML and FT risk. Post event monitoring may be more effective at identifying patterns of unusual customer activity or transactions.

6. Monitoring may involve manual and automated procedures. Automated monitoring procedures may add value to manual procedures (particularly for Regulated Entities with large volumes of customer transactions) by producing exception reports identifying transactions or activity for further examination that fall outside of parameters for usual activity. The appropriateness of automated monitoring procedures will depend on the relevance of the parameters to the nature of business undertaken by a Regulated Entity.

7. Unusual or higher risk activity or transactions may indicate ML or FT activity where there is no apparent economic or visible lawful purpose.

8. Where monitoring indicates possible ML or FT activity, and the process of undertaking identification procedures is managed without due care, contact between a Regulated Entity and a customer (or his advisors) could unintentionally lead to the customer being tipped off. Section 6.4 considers this situation.

9. Sufficient guidance and training of staff is essential to enable them to recognize ML and FT activity. Requirements for training in the recognition and handling of unusual activity are covered in Section 7.

5.2 OBLIGATION TO MONITOR

STATUTORY REQUIREMENTS

10. *Pursuant to Article 3, paragraph 1, subsection d, of the AML/CFT State Ordinance, a Regulated Entity must conduct on-going monitoring of the business relationship and the transactions undertaken throughout the course of the business relationship to ensure that these transactions are consistent with the Regulated Entity's knowledge of the customer and the UBO, their risk profile, including where necessary, an assessment of the funds that are involved in the transaction or business relationship*.

11. *Pursuant to Article 11 of the AML/CFT State Ordinance, a Regulated Entity must perform enhanced CDD throughout the course business relationship if and when a business relationship or a transaction by its nature entails a higher risk of ML or FT, in any case in the following situations:*

- *when a client is not a resident of Aruba, respectively not established in Aruba;*
- *if a client is not physically present for identification;*
- *if it concerns private banking;*
- *with legal persons, trusts and comparable entities that are intended as private assets holding vehicles;*
- *with bodies corporate and comparable entities with shares in bearer form or nominee shareholders;*
- *with natural persons, legal persons, trusts and comparable entities that originate from countries or jurisdictions which do not or insufficiently apply the internationally accepted AML/CFT standards;*
- *with PEPs;*
- *when entering into correspondent banking relations;*
- *other situations to be determined by regulation of the Minister of Finance.*

12. *Pursuant to Article 12, paragraph 2, subsection b, of the AML/CFT State Ordinance, a Regulated Entity that enters into a business relationship or carries out a transaction for a PEP must ensure that on-going monitoring on the business relationship is conducted*.

REGULATORY REQUIREMENTS

13. A Regulated Entity must, as a part of its on-going CDD procedures, establish appropriate customer activity and transaction monitoring procedures that scrutinize the activity and transactions of its customers.

14. The monitoring procedures must require more intensive scrutiny of higher risk customers (including PEPs) and higher risk products/services.

15. The monitoring procedures must include those:

- which provide for the identification and scrutiny of:
  - transactions that are deemed unusual transactions based on the objective indicators;
  - complex or unusually large transactions;
  - unusual patterns of transactions or transactions which have no apparent economic or lawful purpose;
  - business relationships and transactions connected with jurisdictions which do not, or insufficiently, comply with the international AML/CFT standards, including but not limited to the FATF Recommendations;
  - business relationships and transactions connected with jurisdictions which are the subject of Aruban, UN, US or EU countermeasures;
  - Business relationships or transactions that are designated by Article 11 of the AML/CFT State Ordinance to by its nature entail a higher risk of ML or FT;
  - any other activity, the nature of which, causes the Regulated Entity to regard it as particularly likely to be related to ML or FT.
- which specify additional procedures where products and transactions are susceptible to anonymity.

16. The monitoring procedures must:

- involve a Regulated Entity applying its understanding of its business (i.e. the outcome of its business risk assessment – Section 2.3) to determine the nature of usual activity and its expectations for unusual and higher risk activity and transactions;
- be designed to result in the identification of unusual and higher risk activity or transactions;
- require that, in particular, special attention is paid to specific higher risk activity and transactions;
- require the examination of any unusual or higher risk activity or transaction to determine the background and purpose of the activity or transaction;
- in connection with the above examination, involve the collection of additional information (where appropriate);
- establish whether there is a rational explanation (an apparent economic or visible lawful purpose) for the unusual or higher risk activity or transaction, and document these findings in writing; and
- result in appropriate action being taken as a result of the findings of the above procedures.

GUIDANCE NOTES

17. **Appropriate monitoring systems**. In determining the nature of the monitoring procedures appropriate for a business, a Regulated Entity may have regard to the following factors:

- its business risk assessment;
- the size and complexity of its business;
- its ability to monitor transactions or activity in real time (i.e. before customer instructions are put into effect);
- whether it is possible to establish appropriate standardized parameters for unusual transactions; and
- the monitoring procedures that already exist to satisfy other business needs.

18. **Identifying unusual activity/transactions**. Appropriate factors to consider in determining whether activity or transactions are unusual include:

- the expected frequency, size, volume and origin/destination of customer funds whether specific to an individual customer, or for a generic customer type or product type; and
- the presence of risk factors specific to the nature of the activity and customer base of the Regulated Entity based on its knowledge of its customer base (refer to Section 2.3) and having regard to typologies (whether external or developed from its own experiences) relevant to the nature of business activities.

19. **Examining unusual and higher risk activity**. A Regulated Entity may demonstrate that it is appropriately examining unusual and higher risk activity and transactions where it:

- reviews the identified activity/transaction in light of the customer risk assessment and the CDD information that it holds;
- makes unusual transaction reports;
- makes further enquiries to obtain any further information required to enable a determination as to whether the activity/transaction has a rational explanation; and
- considers the activity or transaction in the context of any other relationships connected with the customer.

20. The examination of unusual and higher risk activity or transactions may be conducted either by customer facing staff, or by an independent reviewer. In any case, the reviewer must have access to relevant CDD information, and the enquiries made and the conclusions reached by the reviewer must be appropriate. Refer to Section 8 for record keeping requirements.

21. **Appropriate follow up action may include**:

- Updating CDD information to record the results of the enquiries made;
- Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and/or additional CDD information obtained;

- Considering whether adjusting the monitoring system is required, e.g. to result in further staff training in the identification of unusual or higher risk activity and transactions, refinement of the monitoring system's parameters, enhancement of controls for more vulnerable products/services/business units;

- Applying increased levels of monitoring to particular relationships;

- Where the activity or transaction does not have a rational explanation, considering whether the circumstances require a unusual activity report to be submitted to the Regulated Entity's MLRO (Section 6);

- Considering whether the customer's risk profile, after reassessment, is still acceptable and the business relationship with the customer can be continued or must be terminated.

22. In line with enhanced CDD requirements for higher risk customers (Section 3.12), more intensive scrutiny of customer activity and transactions may involve, for example:

    - More frequent review and updating of CDD information;

    - More regular review of customer activity and transactions against the customer's expected activity profile;

    - The application of lower thresholds for the monitoring of customer activity and transactions;

    - Customer reviews being conducted by persons not directly involved in managing customer relationships.

5.3 AUTOMATED MONITORING METHODS

REGULATORY REQUIREMENTS

23. A Regulated Entity must assess the appropriateness of an automated monitoring method.

24. Use of automated monitoring systems does not remove the requirement for a Regulated Entity to otherwise remain vigilant. Factors such as staff intuition, direct contact with a customer, and the ability, through experience, to recognize activity and transactions that do not seem to make sense, cannot be automated and must not be under estimated.

GUIDANCE NOTES

25. Automated monitoring methods may be effective in recognizing unusual and higher risk activity or transactions.

26. Exception procedures and reports can provide a simple but effective means of monitoring all transactions to or from particular geographical locations or accounts, and any activity that falls outside of pre-determined parameters – based on thresholds that reflect the nature and level of activity and the risk profiles or the relationships that are being monitored.

27. Large or more complex Regulated Entities may be required to use automated monitoring systems to facilitate the monitoring of significant volumes of transactions, or – in an e-commerce environment – where the opportunity for human scrutiny of individual transactions is limited.

28. In the case of monitoring activity and transactions that may be conducted with natural persons who are the subject of countermeasures, applied under Aruban UN, US and EU sanctions and measures, the use of electronic external data sources may be particularly effective.

6. REPORTING UNUSUAL TRANSACTIONS

6.1 OVERVIEW OF SECTION

1. This section outlines the requirements concerning disclosure of information where a Regulated Entity has identified unusual transactions set out in the AML/CFT State Ordinance. This may be based on objective or subjective indicators.

6.2 EVALUATION OF UNUSUAL TRANSACTIONS BY THE MLRO

REGULATORY REQUIREMENTS

2. A Regulated Entity must provide that:

   - All relevant information is promptly made available to the MLRO (or deputy MLRO) on request so that internal unusual transactions reports are properly assessed.

   - Each unusual transaction report is considered by the MLRO (or deputy MLRO) in light of all relevant information.

   - With regard to the unusual transactions reports made according to the subjective criteria the MLRO (or deputy MLRO) must document the evaluation process followed and reasons for the decision to report or not to report to the MOT.

GUIDANCE NOTES

3. In order to demonstrate that a report is considered in light of all relevant information when evaluating an unusual transaction report, the MLRO (or deputy MLRO) may, among others:

   - Review and consider transaction patterns and volumes, previous patterns of instructions, the length of the business relationship and CDD information.

   - Examine other connected accounts or relationships. Connectivity can arise through commercial connections, such as transactions to or from other customers or common introducers, or through connected natural persons, such as third parties, common ownership of entities or common signatories. However, the need to search for information concerning connected accounts or relationships should not delay the filing of a report to the MOT.

6.3 DISCLOSURE OF UNUSUAL TRANSACTIONS REPORTS TO THE MOT

STATUTORY REQUIREMENTS

4. *Pursuant to Article 26, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must report a conducted or intended unusual transaction to the MOT, without delay after it has become aware of the unusual nature of the transaction. Whether a transaction is considered an unusual transaction must be assessed on the based on the objective and subjective indicators adopted by the Minister in accordance with Article 25 of the AML/CFT State Ordinance*.

5. *Pursuant to Article 26, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity must include, in any case, the following information in an unusual transaction report:*

   - *the identity of the customer;*

- *the nature and number of the identity document of the customer;*

- *the nature, time, and place of the transaction;*

- *the amount and destination and source of the monies, securities, precious metals, or other values involved in a transaction;*

- *the circumstances based on which the transaction is considered unusual.*

- *if it concerns a transaction regarding a high value object, a description of the object in question.*

- *the indicator or indicators pursuant to which the transaction has been designated as unusual.*

6. *Pursuant to Article 27, paragraph 2, of the AML/CFT State Ordinance, a Regulated Entity that has submitted an unusual transaction report to the MOT, must, if so requested by the MOT, provide further data or information. The requested data or information must be provided to the MOT in writing, and, in case of urgency determined as such by the MOT, orally, within the period set by the MOT*.

7. *Pursuant to Article 28 of the AML/CFT State Ordinance, a Regulated Entity must make unusual transactions reports to the MOT in accordance with the directions of the MOT*.

8. *Article 29 of the AML/CFT State Ordinance states that data or information provided in accordance with Articles 26 or 27, paragraph 2, of the AML/CFT State Ordinance may not be used as a basis for, or for the benefit of a criminal investigation or prosecution on suspicion of, or as evidence regarding a charge of ML or FT by the Regulated Entity, or its employees, that provided the data or information. Data or information provided on the reasonable supposition that Articles 26 or 27, paragraph 2, of the AML/CFT State Ordinance are implemented, may not be used as a basis for or for the benefit of a criminal investigation or prosecution on suspicion of, or as evidence regarding a charge of violation of the articles 285 or 286 of the Criminal Code of Aruba*.

9. *Pursuant to article 30 of the AML/CFT State Ordinance, a Regulated Entity, or its employees, that has made an unusual transactions report in good faith pursuant to Article 26 of the AML/CFT State Ordinance or that has provided data or information to the MOT pursuant to Article 27, paragraph 2, of the AML/CFT State Ordinance shall not be liable for any damage suffered by a third party in consequence thereof*.

REGULATORY REQUIREMENTS

10. A Regulated Entity must establish and maintain reporting procedures which:

- communicate the identity of the MLRO (and any deputy MLROs) to the Regulated Entity's employees;

- encompass the reporting of attempted transactions and business that has been turned away.

- require that as soon as it is reasonably practicable an internal unusual transactions report is made to the MLRO (or to a deputy MLRO) of any information or other matter coming to the attention of any member of staff handling financial or trust services business which, in the opinion of that person, (possibly) meets the objective indicators or the subjective indicators;

- require that a report is considered promptly ("without delay" in the meaning of Article 26, paragraph 2, subsection e, of the AML/CFT State Ordinance) by the MLRO (or a deputy MLRO)

in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report constitutes an unusual transaction;

- allow the MLRO (or a deputy MLRO) to have access to all other information which may be of assistance in considering the report; and

- provide for the information or other matter contained in a report to be disclosed as soon as is reasonably practicable by the MLRO (or deputy MLRO) to the MOT in writing, where the MLRO (or deputy MLRO) has determined that the information or other matter contained in the report constitutes an unusual transaction.

11. A Regulated Entity must provide that:

- Where a customer fails to supply adequate CDD information (including information on UBOs), consideration is given to making an unusual transaction report.

- Unusual transactions reports include a statement of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of ML or FT activity and full details of the customer.

- Internal unusual transactions reports are not filtered out by supervisory staff or managers such that they do not reach the MLRO (or deputy MLRO).

12. A Regulated Entity must establish and maintain arrangements for disciplining any member of staff who fails, without reasonable excuse, to make an internal unusual transaction report where he or she is aware of any information or other matter that (possibly) meets the objective indicators or the subjective indicators for the reporting of unusual transactions.

GUIDANCE NOTES

13. A Regulated Entity may demonstrate that unusual transactions reports are made to the MOT as soon as is reasonably practicable by having in place reporting lines that are as short as possible with the minimum number of people between the employee initiating the internal unusual transaction report and the MLRO (or deputy MLRO). While a Regulated Entity may allow its staff to discuss relationships and transactions with line managers before making an unusual transaction report, it will be the decision of the staff member whether to make the internal report to the MLRO.

14. A Regulated Entity may demonstrate that it has established and maintained appropriate arrangements for disciplining staff, where employment contracts or employment handbooks provide for the imposition of disciplinary sanctions for failing to make an internal unusual transaction report without a reasonable excuse.

6.4 TIPPING OFF

STATUTORY REQUIREMENTS

15. *Pursuant to Article 31 of the AML/CFT State Ordinance, any person must treat any information where that person knows or suspects that an unusual transaction report has been made, or that an investigation is under way or proposed, as strictly confidential*.

REGULATORY REQUIREMENTS

16. The Regulated Entity must ensure that its employees are regularly reminded of the tipping off prohibition via training sessions or otherwise.

7. VETTING, AWARENESS AND TRAINING OF EMPLOYEES

7.1 OVERVIEW OF SECTION

1. One of the most important controls over the prevention and detection of ML and FT is to have appropriately vetted staff who are:

   - alert to ML and FT risks; and

   - well trained in the identification of unusual or higher risk activities or transactions, which may indicate ML or FT.

2. The effective application of even the best designed policies, procedures and measures can be quickly compromised if staff lacks competence or probity, are unaware of or fail to apply policies, procedures and measures, and are not adequately trained.

3. It is essential that a Regulated Entity has a clear and well articulated policy for ensuring that staff are:

   - competent and have probity;

   - aware of their obligations under the AML/CFT Laws and Regulations (and by extension, also the Handbook) and the relevant AML/CFT provisions of the Criminal Code of Aruba (AB 1991 no GT 50) (Articles 140a, 430b, 430c and 430d); and

   - trained in the identification of unusual or higher risk activities or transactions, which may indicate ML or FT activity, and in the Regulated Entity's CDD, reporting and record keeping procedures.

4. In particular, customer facing employees and those who handle or are responsible for the handling of customers and transactions will provide the business with its strongest defense, or its weakest link.

5. A Regulated Entity should also encourage its staff to "think risk" as they carry out their duties within the legal and regulatory framework governing ML and FT.

7.2 OBLIGATION TO PROMOTE AWARENESS AND TO TRAIN

STATUTORY REQUIREMENTS

6. *Pursuant to Article 46 of the AML/CFT State Ordinance, a Regulated Entity must pursue adequate policies and have procedures and measures in place regarding, inter alia, the recruitment, background, education, guidance and on-going training of employees*.

REGULATORY REQUIREMENTS

7. A Regulated Entity must, in relation to Relevant Employees:

   - take regular and appropriate measures to ensure they are aware of:

     - the CDD, record keeping and internal reporting procedures, and such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing ML and FT; and

- the enactments in Aruba relating to ML and FT;

- regularly provide those employees with training in the recognition and handling of transactions carried out by or on behalf of any person who is or appears to be engaged in ML or FT; and

- establish and maintain procedures that monitor and test the effectiveness of the employees' awareness of AML/CFT issues and the training provided to employees.

- The term "employee" must not be limited to natural persons working under a contract of employment, but must also include temporary and contract staff, and the staff of any third parties fulfilling a function in relation to a Regulated Entity under an outsourcing agreement.

GUIDANCE NOTES

8. When determining whether an employee is a Relevant Employee, a Regulated Entity may take into account the following:

   - whether the employee is undertaking any customer facing functions, or handles or is responsible for the handling of business relationships or transactions in a front office, middle office or back office environment;

   - whether the employee is directly supporting a colleague who carries out the above activity; and

   - whether an employee's role has changed to involve the above activities.

9. Customer facing Relevant Employees will include, for example, relationship managers, trust and company administrators, stockbrokers, investment advisors, money transfer companies' front and back office staff, insurance company sales people, insurance brokers, etc. Non-customer facing Relevant Employees will include, for example, the (deputy-)MLRO, the (deputy-)MLCO, the internal auditor and natural persons processing and book-keeping customer transactions. Relevant Employees will also include the Board and senior managers.

7.3 VETTING OF RELEVANT EMPLOYEES

REGULATORY REQUIREMENTS

10. A Regulated Entity must vet and monitor the competence and probity of Relevant Employees.

GUIDANCE NOTES

11. A Regulated Entity may demonstrate that vetting procedures are appropriate where (at the time of recruitment or subsequent change in role) it carries out one or more of the following activities, as appropriate for the nature of the employee's role and responsibilities:

    - Obtaining and confirming references.

    - Obtaining and confirming employment history and qualifications disclosed.

    - Obtaining a Declaration of Good Conduct or an equivalent declaration.

    - Obtaining details of any regulatory action taken against the individual (or absence of such action).

    - Obtaining and confirming details of any criminal convictions (or absence of such convictions).

12. In order to obtain details of any regulatory action taken against the individual, a Regulated Entity would first need to obtain the consent from the applicant for a job to carry out such verification of the information contained in his application form as considered necessary. The Regulated Entity can then send that authorization to any employer or regulatory authority as evidence that the employer/regulatory authority is alleviated of duties of confidentiality regarding that person, and as such can confirm the accuracy of information provided by the applicant.

7.4 AWARENESS OF EMPLOYEES

REGULATORY REQUIREMENTS

13. A Regulated Entity must have appropriate measures in place to make Relevant Employees aware of:

- The Regulated Entity's policies, procedures and measures designed to prevent and detect ML and FT.
- The statutory and regulatory obligations under which the business operates and under which the Regulated Entity and/or its employees may be held personally liable.
- The implications of failing to report information in accordance with procedures may result in criminal, regulatory and/or disciplinary sanctions.

7.4.1 ALL RELEVANT EMPLOYEES

GUIDANCE NOTES

14. A Regulated Entity may demonstrate that it has appropriate measures in place where it:

- Informs Relevant Employees of the identity of the MLRO and the procedures to make internal unusual transactions reports.
- Provides Relevant Employees with a copy of its AML/CFT procedures manual.
- Makes its AML/CFT procedures manual available on its intranet site.
- Provides Relevant Employees with a document outlining the Regulated Entity's and their own obligations and potential criminal liability under Articles 430b, 430c, 430d and 140a of the Criminal Code of Aruba (AB 1991, no. GT 50).
- Requires employees to acknowledge that they have received and understood its AML/CFT procedures manual.
- Periodically tests employees' awareness of policies, procedures and measures and statutory and regulatory obligations.

15. It is not sufficient to provide employees with a copy of the Handbook, as the Handbook is designed to provide a base from which a Regulated Entity can design and implement and tailor its own policies, procedures and measures appropriate to its business.

7.4.2 THE BOARD

REGULATORY REQUIREMENTS

16. The Board must understand the strategic and practical aspects of ML and FT such that it can make informed decisions as to whether the proposals being put forward with regard to the business risk assessment and the policies, procedures and measures, are relevant and sufficient. The Board must also be sufficiently aware of their legal obligations to properly prioritize the budgetary and resource requirements of implementing an effective range of defenses against ML and TF.

7.4.3 NON-RELEVANT EMPLOYEES

GUIDANCE NOTES

17. A Regulated Entity may demonstrate that it has appropriate measures in place with regard to non-Relevant Employees (e.g. staff who do not fall within the definition of Relevant Employees outlined above, but who nonetheless could either be used by or facilitate the work of money launderers or terrorist financiers – for example, clerical staff, secretaries, security staff and cleaning staff have access to entry passwords, computer systems, files, letterheads, etc.) where it:

- Informs staff of the identity of the MLRO and the procedures to make internal unusual transactions reports.

- Provides staff with a document outlining the Regulated Entity's and their own obligations and potential criminal liability under articles 430b, 430c, 430d and 140a of the Criminal Code of Aruba (AB 1991, no. GT 50).

7.4.4 ONGOING AWARENESS (ALL EMPLOYEES)

OVERVIEW

18. With the passage of time between training initiatives, the level of employee awareness of the risk of ML and FT decreases. The utilization of techniques to maintain a high level of awareness can greatly enhance the effectiveness of a Regulated Entity's defenses against ML and FT.

GUIDANCE NOTES

19. A Regulated Entity may demonstrate that it has appropriate measures to maintain awareness where it:

- keeps employees aware of AML/CFT (such as updates issued by the CBA, or developments in international standards) as they occur;

- provides employees with case studies illustrating how products or services provided by the Regulated Entity may be abused;

- provides employees with refresher training such as that available on line;

- advises employees of current news stories involving ML and FT activity; and

- sends e-mail reminders of employee obligations and the need to remain vigilant.

7.5 TRAINING OF EMPLOYEES

OVERVIEW

20. The guiding principle of all training should be to encourage employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the Regulated Entity against the threat of ML and FT.

21. There is a tendency, in particular on the part of more junior employees, non-customer facing staff, and support staff to mistakenly believe that the role that they play is less pivotal than, or secondary to, that of more senior colleagues or customer facing colleagues. Such an attitude can lead to failures to report important information because of mistaken assumptions that the information will have already been identified and dealt with by other colleagues.

REGULATORY REQUIREMENTS

22. A Regulated Entity must provide employees with adequate training at appropriate frequencies so that employees are kept informed of new developments and risk factors connected with ML and FT. Such training must:

- be tailored to the Regulated Entity and relevant to the employees to whom it is delivered;
- highlight to employees the importance of the contribution that they can individually make to the prevention and detection of ML and FT; and
- cover key aspects of AML/CFT Laws and Regulations and the relevant AML/CFT provisions of the Criminal Code of Aruba (AB 1991 no GT 50) (Articles 140a, 430b, 430c and 430d).

7.6 ADEQUACY OF TRAINING

7.6.1 ALL RELEVANT EMPLOYEES

GUIDANCE NOTES

23. A Regulated Entity may demonstrate the provision of adequate training to relevant staff where it addresses:

- AML/CFT Laws and Regulations (and by extension, also the Handbook) and the relevant AML/CFT provisions of the Criminal Code of Aruba (AB 1991 no GT 50) (Articles 140a, 430b, 430c and 430d);
- Vulnerabilities of services and products offered by the Regulated Entity, and subsequent ML and FT risk, on the basis of its business risk assessment.
- Policies, procedures and measures, and employees' responsibilities.
- Application of risk based CDD policies, procedures and measures.
- Recognition of and dealing with unusual or higher risk activity and transactions, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships.
- ML and FT developments, including techniques, methods, trends and typologies.

- Management of business relationships or transactions which have been the subject of a unusual transactions report, e.g. risk of committing the offence of tipping off, and dealing with questions from such customers, and/or their advisers.

7.6.2 NON-RELEVANT EMPLOYEES

GUIDANCE NOTES

24. A Regulated Entity may demonstrate the provision of adequate training where the training promotes an awareness of the threat of ML and FT and the reporting procedures that should be followed in the event that unexplained unusual, or higher risk activity or transactions are spotted.

7.7 TIMING AND FREQUENCY OF TRAINING

GUIDANCE NOTES

25. A Regulated Entity may demonstrate the provision of training at appropriate frequencies by:

- Providing all employees with induction training within 15 working days of the commencement of employment and, when necessary, where there is a subsequent change in an employee's role.

- Delivering refresher training to all employees at least once every 2 to 3 years, and otherwise determining the frequency of training for Relevant Employees on the basis of risk, with more frequent training where appropriate due to the nature of the role being undertaken; for example, customer facing staff and relationship managers are particularly well placed to identify unusual transactions or structures, settlements staff are particularly well placed to identify circular transactions with no lawful or commercial basis, etc.

7.8 MONITORING THE EFFECTIVENESS OF TRAINING

GUIDANCE NOTES

26. A Regulated Entity may demonstrate that it has assessed the effectiveness of training provided by:

- Testing employees' understanding of the Regulated Entity's AML/CFT policies, procedures and measures, and also their ability to recognize ML and FT activity.

- Monitoring the compliance of employees with AML/CFT policies, procedures and measures, and taking any action that may be necessary.

- Monitoring internal reporting patterns and taking any action that may be necessary.

- The routine supervision of employees.

8. RECORD KEEPING

8.1 OVERVIEW OF SECTION

1. The record keeping obligations are essential to facilitate effective investigation, prosecution and confiscation of criminal property. If law enforcement agencies, either in Aruba or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for ML and confiscation of criminal property may not be possible. Likewise, if the funds used for FT activity cannot be traced back through the financial system, then the sources and the destination of terrorist funding will not be identified.

GUIDANCE NOTES

2. Records may be kept:

   - by way of original documents;
   - by way of photocopies of original documents (certified where appropriate);
   - in scanned form; or
   - in computerized or electronic form.

8.2 RECORDING CDD AND TRANSACTION INFORMATION

STATUTORY REQUIREMENTS

3. *Pursuant to Article 33, paragraph 1, of the AML/CFT State Ordinance, a Regulated Entity must retain all CDD information in an accessible way for a period of at least ten years after the date of termination of the business relationship, or until at least ten years after carrying out the transaction in question. The keeping of records must take place in such manner that separate transactions can be reconstructed at all times and be submitted to the competent authorities on first demand*.

4. *Pursuant to Article 33, paragraph 1, subsection a, of the AML/CFT State Ordinance, the data to be retained with regard to natural persons must include, in any case, the following:*

   - *the surname, given names, date of birth, address, and domicile and/or place of business of the customer and the UBO and of the person acting on behalf of this natural person, or a copy of the document containing a number identifying a person, and based on which identification took place;*
   - *the nature, number, and date and place of issue of the document used to verify the identity;*
   - *the nature and date of the transaction;*
   - *the type and amount of the money involved in the transaction;*
   - *the type and number of the account used during the transaction;*
   - *all account files and business correspondence.*

5. *Pursuant to Article 33, paragraph 1, subsection b, of the AML/CFT State Ordinance, the data to be retained with regard to legal persons incorporated under Aruban law must include, in any case, the following:*

   - *the legal form, name under the Articles of Association, the trade name, address, and, if the legal person is listed with the Chamber of Commerce, the registration number of the Chamber of Commerce, and the manner in which the identity has been verified;*
   - *of the persons acting on behalf of the legal person and of the UBO, the surname, given names, and date of birth;*
   - *the nature and date of the transaction;*
   - *the type and amount of the money involved in the transaction;*
   - *the type and number of the account used during the transaction;*
   - *all account files and business correspondence.*

6. *Pursuant to Article 33, paragraph 1, subsection c, of the AML/CFT State Ordinance, the data to be retained with regard to foreign legal persons and comparable entities must include, in any case, the following:*

   - *the documents used to verify the identity;*
   - *of the persons acting on behalf of the legal person and of the UBO, the family name, given names, and date of birth;*
   - *the nature and date of the transaction;*
   - *the type and amount of the money involved in the transaction;*
   - *the type and number of the account used during the transaction;*
   - *all account files and business correspondence.*

7. *Pursuant to Article 33, paragraph 1, subsection d, of the AML/CFT State Ordinance, the data to be retained with regard to trusts must include, in any case, the following:*

   - *the documents used to verify the identity of the trustee or the person exercising control over the trust, the settlor and of the UBO's of the assets of the trust;*
   - *the nature and date of the transaction;*
   - *the type and amount of the money involved in the transaction;*
   - *the type and number of the account used during the transaction;*
   - *all account files and business correspondence.*

8.2.1 CDD INFORMATION

REGULATORY REQUIREMENTS

8. A Regulated Entity must record and store CDD information in a way that facilitates periodic updating of the information.

GUIDANCE NOTES

9. A Regulated Entity may demonstrate adequate recording and storage of CDD information by ensuring that updated information relating to a customer that is obtained through meetings, discussions, or other methods of communication with the customer is recorded and retained.

8.2.2 TRANSACTION INFORMATION

REGULATORY REQUIREMENTS

10. The records prepared and retained by a Regulated Entity in relation to customer transactions must be orderly and such that the audit trail for incoming and outgoing funds or asset movement is clear and complete.

11. When original documents (such as transaction related vouchers used to input data onto computer systems) that would ordinarily have been destroyed are requested for investigation purposes, a Regulated Entity must ascertain whether the documents have in fact been destroyed.

GUIDANCE NOTES

12. Adequate recording of details of transactions may be demonstrated by including (where appropriate):

    - valuation(s) and price(s);
    - the form (e.g. cash, check, electronic transfer) in which funds are transferred;
    - memoranda of instruction(s) and authority(ies);
    - memoranda of purchase and sale;
    - custody of title documentation; and
    - other records in support of transaction records where these are necessary to enable a clear and complete audit trail of fund or asset movements to be established.

13. Adequate recording of details of transactions may be demonstrated by recording all transactions undertaken on behalf of a customer within that customer's records, enabling a complete transaction history for each customer to be easily constructed. For example, a customer's records may include all requests for wire transfer transactions where settlement is provided other than from funds drawn from a customer's account with the Regulated Entity.

14. When original vouchers or documents are used for account entry, for example, and are not returned to the customer, it is of assistance to the law enforcement agencies if these original documents are kept for at least one year to assist forensic analysis.

8.3 RECORDING COMPLIANCE MONITORING

REGULATORY REQUIREMENTS

15. A Regulated Entity must keep for at least ten years adequate and orderly records to enable the CBA, internal and external auditors and other competent authorities to assess the effectiveness of the AML/CFT policies, procedures and measures that are maintained by a Regulated Entity.

16. A Regulated Entity must keep adequate and orderly records documenting its AML/CFT policies, procedures and measures for at least ten years from the date those policies and procedures are superseded.

GUIDANCE NOTES

17. A Regulated Entity may demonstrate that it has retained adequate records to permit an assessment of effectiveness of policies, procedures and measures where it keeps:

- its business risk assessment;
- compliance reports to the Board; and
- details of testing programs conducted by the MLCO.

8.4 RECORDING UNUSUAL TRANSACTION REPORTS

STATUTORY REQUIREMENTS

18. Pursuant to Article 34 of the AML/CFT State Ordinance, a Regulated Entity must retain all information contained in an unusual transactions report in an accessible way for a period of at least ten years after the filing of the unusual transaction report to the MOT.

REGULATORY REQUIREMENTS

19. A Regulated Entity must keep, for a period of at least ten years from the date that a business relationship ends, or, if in relation to an occasional transaction, for at least ten years from the date that a transaction was completed, orderly records containing:

- internal unusual transactions reports and supporting documentation;
- the decision of the MLRO (or deputy MLRO) concerning whether to make an external unusual transaction report and the basis of that decision; and
- any external unusual transactions reports,

in relation to that business relationship or occasional transaction.

8.5 RECORDS RELATING TO HIGHER RISK ACTIVITY AND TRANSACTIONS

REGULATORY REQUIREMENTS

20. A Regulated Entity must keep adequate and orderly records containing the findings of reviews of:

- complex transactions;

- unusual large transactions; and
- unusual patterns of transactions, which have no apparent economic or visible lawful purpose,

for a period of at least ten years from the date the business relationship ends, or, if in relation to an occasional transaction, for ten years from the date that the transaction was completed.

21. A Regulated Entity must keep adequate and orderly records containing the findings of reviews of activity and transactions: (i) connected with jurisdictions which do not, or insufficiently, apply the FATF Recommendations; or (ii) which are the subject of UN, US or EU countermeasures - for a period of at least ten years from the date the business relationship ends, or, if in relation to an occasional transaction, for at least ten years from the date that the transaction was completed.

8.6 TRAINING AND AWARENESS

REGULATORY REQUIREMENTS

22. A Regulated Entity must keep adequate and orderly records for five years detailing the dates on which AML/CFT training was provided, the nature of the training and the names of employees who received the training.

8.7 ACCESS TO AND RETRIEVAL OF RECORDS

REGULATORY REQUIREMENTS

23. A Regulated Entity must record CDD and transaction information in a way that facilitates on-going monitoring of each relationship - in order to meet obligations that are set out in Section 5.

24. For all other purposes, the records retained by a Regulated Entity must be readily accessible by the person. Unless otherwise specified, records relating to CDD and transaction information must be accessible within 5 working days (whether held in Aruba or outside Aruba), or such longer period as agreed with the CBA. Other records must be accessible within 10 working days (whether held in Aruba or outside Aruba), or such longer period as agreed with the CBA.

25. A Regulated Entity must periodically review the accessibility of, and condition of, paper and electronically retrievable records and consider the adequacy of the safekeeping of records.

26. A Regulated Entity must periodically review the procedures relating to retrieval of records.

27. A Regulated Entity that undergoes mergers, take-overs, or internal reorganizations, must ensure that records remain readily retrievable for the required period when rationalizing computer systems and storage arrangements.

28. Records must be maintained in a format that can be made readily available. Where records are kept other than in legible form, they must be maintained so as to be readable at a computer terminal in Aruba - so that they may be produced in legible form.

8.8 EXTERNAL RECORD KEEPING

OVERVIEW

29. Where documentation is held overseas or by third parties, such as under outsourcing arrangements, or where reliance is placed on introducers, this will present additional factors for a Regulated Entity to consider.

30. Where record keeping is outsourced, a regulated entity remains responsible for compliance with all requirements.

REGULATORY REQUIREMENTS

31. A Regulated Entity must not enter into outsourcing arrangements or place reliance on third parties to retain records where access to records is likely to be impeded by confidentiality or data protection restrictions.

8.9 REQUIREMENTS ON CLOSURE OR TRANSFER OF BUSINESS

OVERVIEW

32. Where a Regulated Entity terminates activities, or disposes of business or a block of customers to other service providers, record keeping requirements are unaffected by the termination or disposal.

REGULATORY REQUIREMENTS

33. Record keeping arrangements must be agreed with the CBA where a Regulated Entity terminates activities, or disposes of business or a block of customers to another service provider.

9. ENTERING INTO FORCE AND TRANSITIONAL PROVISIONS

9.1 OVERVIEW OF SECTION

1. The CDD requirements of the AML/CFT State Ordinance and this Handbook apply to all new and existing customers. With regard to existing customers the transitional provisions regarding the AML/CFT State Ordinance are included in Article 2 of the Enactment State Ordinance. Article 3 of the Enactment State Ordinance contains transitional provisions with regard to the controlled business operations (*beheerste bedrijfsvoering*).

2. The CBA expects to see Regulated Entities evidence a robust approach in developing and applying AML/CFT policies, procedures and measures to comply with the transitional provisions provided in the Enactment State Ordinance.

3. Regulated Entities are strongly advised to draw Board's attention to the transitional provisions during which full compliance must be achieved. In line with the applicable laws, failure to comply with the transitional provisions will be treated seriously.

9.2 ENACTMENT DATE

4. The Handbook enters into force on June 1, 2011.

9.3 TRANSITIONAL PROVISIONS REGARDING THE REGULATORY REQUIREMENTS

9.3.1 EXISTING CUSTOMERS

OVERVIEW

5. In order to apply a risk based approach to existing customers, and to effectively update and upgrade the quality of information held on existing customers, the Enactment State Ordinance contains transitional arrangements to allow Regulated Entities a maximum time frame within which to upgrade the information required. It is explicitly required that a Regulated Entity conducts a risk assessment of its existing customer base - based on the information that it holds at the time that it conducts the review and then progresses through the transitional arrangements in line with the timetables set out in the Enactment State Ordinance.

6. Monitoring of existing customers will be based on information that is held by a Regulated Entity, and the requirement to keep documents, data, or information up to date will be understood within the context of what is actually held.

STATUTORY REQUIREMENTS

7. *Pursuant to Article 2 of the Enactment State Ordinance, a Regulated Entity must apply CDD measures that are in line with the provisions in the AML/CFT State Ordinance applicable to that relationship. The CDD work must be completed no later than within the timescales set out in the transitional provisions in the Enactment State Ordinance*.

8. *Pursuant to Article 2 of the Enactment State Ordinance, a Regulated Entity must adhere to the following transitional periods during which Regulated Entities can achieve full compliance:*

- *Within 2 months as of June 1, 2011: formulate and adopt a policy document and accompanying CDD procedures to risk rate customers.*

- *Within 4 months as of June 1, 2011: review all existing customer files and apply and record a risk rating according to the aforementioned policy document.*

- *Within 6 months as of June 1, 2011: carry out and complete full CDD on high risk customers.*

- *Within 12 months as of June 1, 2011: carry out and complete full CDD on medium risk customers.*

- *Within 24 months as of June 1, 2011: carry out and complete CDD on low risk customers.*

9. *Pursuant to Article 2, paragraph 6, of the Enactment State Ordinance, with regard to trust service providers, the above mentioned transitional periods are extended with an additional 6 months*.

10. *Irrespective of the risk rating allocated to existing customers, or the Regulated Entity's progress through the transitional arrangements, in accordance with Article 6, paragraph 1, subsections d and e[6], and Article 6, paragraph 2, subsection g in conjunction with Article 6, paragraph 1, subsections d and e[7], of the AML/CFT State Ordinance, CDD measures must always be applied immediately to existing customers*:

    - *where a Regulated Entity suspects ML or FT; or*

    - *where a Regulated Entity has doubts about the veracity or adequacy of documents, data or information that is held.*

REGULATORY REQUIREMENTS

11. A Regulated Entity must review its existing customer base in order to determine a risk assessment for each customer, including those who have been introduced through a third party.

12. When considering the risk presented by an existing introduced customer its review must consider the status of the review of existing customers by that introducer.

9.3.2 CONTROLLED BUSINESS OPERATIONS

STATUTORY REQUIREMENTS

13. *Pursuant to Article 3 of the Enactment State Ordinance, a Regulated Entity must comply with the following requirements within 3 months as of June 1, 2011:*

    - *Ensuring that the Regulated Entity's foreign branches or subsidiaries apply as much as possible the provisions set by or by virtue of the AML/CFT State Ordinance and the internationally accepted AML/CFT standards (Article 45 of the AML/CFT State Ordinance).*

[6] With regard to Regulated Entities except for Trust Service Providers.

[7] With regard to Trust Service Providers.

- *pursuing an adequate AML/CFT policy and have in place AML/CFT procedures and measures and carry out periodical evaluations of the Regulated Entity's exposure to ML and FT risks (Article 46 of the AML/CFT State Ordinance).*

- *Appointing a MLCO and MLRO and informing the MOT and the CBA of such appointments Article 47 of the AML/CFT State Ordinance).*

14. *Pursuant to Article 3, paragraph 2, of the Enactment State Ordinance, with regard to trust service providers, the above mentioned transitional periods are extended with an additional 6 months*.

9.4 TRANSITIONAL PROVISIONS REGARDING THE REGULATORY REQUIREMENTS

REGULATORY REQUIREMENTS

15. The abovementioned statutory transitional provisions apply mutatis mutandis to the relevant Regulatory Requirements set out in this Handbook. This means that the following transitional periods apply:

    - Section 2: 3 months as of the entering into force of this Handbook.

    - Section 3 (only insofar as it concerns existing customers): the transitional periods as described in paragraph 7 above with the proviso that the transitional periods take effect as of the entering into force of this Handbook.

16. With regard to trust service providers, the above mentioned transitional periods are extended with an additional 6 months.

17. In all other respects, no transitional periods apply.

APPENDIX 1 – EXAMPLE TRANSACTION PROFILE REPORT

TRANSACTION PROFILE REPORT

Company:_____

Date:_____

Description of the major business activities/nature of the banking transactions:

Estimated banking transaction volume (and state if per day, week, month):

Estimated largest banking transaction (amount and currency):

Brief description of anticipated cash activity:

The above information is correct and accurately described. I/We agree to inform the bank timely and accurately of any change that would cause the information as described above to be incorrect and agree to satisfy any information requests the bank may have concerning circumstances leading to any change in the above mentioned declaration.

Name:_____

Position within Company:_____

Additional comments (if any):_____

Signature:_____

Approved by:_____ Date:_____/_____/_____

APPENDIX 2 – EXAMPLE SOURCE OF FUNDS DECLARATION FORM (BANKING)

SOURCE OF FUNDS DECLARATION FORM (BANKING)

Name: _____Nationality:_____

[ ] Passport [ ] ID [ ] Driver's license *(Copy identification document attached)*

Employer:_____ Occupation:_____

Residency: [ ] Resident [ ] Non Resident

Account number:_____ Bank:_____

Permanent/Legal address:_____

_____Tel:_____

State/City: _____Country:_____

Temporary address in Aruba:_____Tel:_____

This section must be filled out when performing a financial transaction on behalf of a company.

Company Name:_____

Company address:_____Tel:_____

I declare that the amount of **AFL/USD/EUR/NAFL/Other** _____represents funds obtained by the undersigned from the following **source(s)*****:

_____

_____

*Provide information such as the person/entity from which funds have been received, date of receipt and the **reason** for receiving funds. If deemed necessary by the bank supporting documents should be submitted.

Specify currency type(s) and denomination(s) _____

This transaction includes: (check all applicable transactions)

[ ] cash out of check
[ ] wire transfer
[ ] cash / check deposit on account no: _____i.n.o.:_____
[ ] payment on credit card no.: _____
[ ] exchange foreign currency
[ ] payment on loan

State purpose of the transaction**:

_____

Provide relevant information on the **destination of the funds if not credited on an account.

Did you exchange foreign currency in the last three months?: No [ ] Yes [ ] Amount_____

I certify that the information in this Source of Funds declaration form is complete and correct to the best of my knowledge and belief.

Signature: _____ **Date:** ____/____/_____

Name bank employee : _____ Initials: _____

Name supervisor : _____ Initials: _____

Remark(s) : _____

Date : _____/_____/_____

APPENDIX 3 – EXAMPLE SOURCE OF FUNDS DECLARATION FORM (MONEY TRANSFER)

SOURCE OF FUNDS DECLARATION FORM (MONEY TRANSFER)

Transaction number:

Name (private person):_____ Nationality:_____

Country of birth:_____ Date of birth:_____

Identification number*:_____ [ ] Passport [ ] Aruban ID document [ ] Driver's license
*Check the identification document type box that pertains to the identification number.

Expiration date:_____

Employer:_____ Occupation:_____

Residency**: [ ] Resident [ ] Non-Resident

Permanent address (abroad):_____

_____

Country:_____ State:_____

(Temporary) address in Aruba:_____Tel:_____

**Non residents must fill out their permanent address abroad and temporary address in Aruba. Residents must fill out their local address in the appropriate space above.

This section must be filled out when performing a financial transaction on behalf of another person.

Name*:_____
*Name of person on whose behalf the money is sent.

Address*:_____Tel:_____
*Address of person on whose behalf the money is sent.

Identification number*:_____ [ ] Passport [ ] Aruban identification [ ] Driver's license
*Check the identification document type box that pertains to the identification number of the person on whose behalf the money is sent.

Expiration date:_____

Relationship to the sender:_____

This section must be filled out when performing a financial transaction on behalf of a company.

Company name:_____

Company address:_____Tel:_____

I declare that the amount of Afl./US$ _____ represents funds obtained by the undersigned from the following source(s)***:

_____

_____

_____

_____

***In case deemed necessary supporting documents should be submitted.

State the relationship to the beneficiary:_____

Specify currency type(s) and denomination(s):_____

State nature of the transaction:_____

Customer signature:_____ Date:_____/_____/_____
day month year

For internal use only:

Name of employee:_____Initials:_____

Remark(s):_____ _____

_____

_____

_____

Reviewed by the Compliance Officer on:_____/ _____/ _____
Day Month Year