CENTRALE BANK VAN ARUBA

GUIDANCE NOTES

FOR THE ESTABLISHMENT OF A POLICY DOCUMENT AND ACCOMPANYING CDD PROCEDURES TO RISK RATE THE EXISTING CUSTOMER BASE

FOR THE BENEFIT OF

NON-REGULATED FINANCIAL SERVICE PROVIDERS AND DESIGNATED NON-FINANCIAL SERVICE PROVIDERS

IN ACCORDANCE WITH

ARTICLE 2, PARAGRAPH 7, OF THE ENACTMENT ORDINANCE STATE ORDINANCE FOR THE PREVENTION AND COMBATING OF MONEY LAUNDERING AND TERRORIST FINANCING

June 30, 2011

J.E. Irausquin Boulevard 8 P.O. Box 18 Oranjestad Aruba
www.cbaruba.org

CONTENT

GLOSSARY

In the context of these Guidance Notes 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.
AML/CFT 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.
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).
CBA:	Centrale Bank van Aruba.
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.
Criminal Code:	Criminal Code of Aruba (AB 1991 no GT 50).
customer (or client):	A client as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance.
Designated Non-Financial Service Provider:	A designated non-financial service provider as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance.
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.
Enactment State Ordinance:	Enactment Ordinance State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (In*voeringsverordening 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).
FATF:	Financial Action Task Force on Money Laundering.
FATF Recommendations:	The FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing.
Financial Service Provider:	A financial service provider as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance.
high value dealer:	A natural person, legal person or corporation which on a commercial or professional basis trades on or acts as an intermediary in the purchase and sale of immobile objects, vehicles, ships, aircraft, objects of arts, antiquities, and the rights to which these objects can be subjected.
Non-Regulated Financial Service Provider:	A financial service provider as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance that is not licensed or registered by the CBA pursuant to the SOSCS, SOSIB or SOSMTC.
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 or SOSTSP and falling under the definition of Financial Service Provider or a Designated Non-Financial Service Provider.
Service Provider:	Entity that is a Non-Regulated Financial Service Provider or a Designated Non-Financial Service Provider.
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 Service Provider 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.
UBO:	Ultimate beneficial owner (or beneficiary) as mentioned in Article 1, paragraph 1, of the AML/CFT State Ordinance.

1. INTRODUCTION TO THE GUIDANCE NOTES

1.1 PURPOSE AND SCOPE OF THE GUIDANCE NOTES

1. On June 1, 2011 the AML/CFT State Ordinance entered into force. The CBA is charged with the supervision of compliance with the AML/CFT State Ordinance.

2. Pursuant to Article 2, paragraph 1, of the Enactment State Ordinance, Non-Regulated Financial Service Providers and Designated Non-Financial Service Providers (hereinafter referred to as Service Providers) must formulate and adopt a policy document and accompanying CDD procedures to risk rate its existing customers. In accordance with Article 2, paragraph 1 in conjunction with 6, of the Enactment State Ordinance, Service Providers must do so within 8 months as of June 1, 2011.

3. These Guidance Notes provide further guidance (leidraad), as meant in Article 2, paragraph 7, of the Enactment Ordinance State Ordinance, from the Centrale Bank van Aruba (CBA) to assist Service Providers to design a policy document and accompanying CDD procedures to risk rate their existing customer base. These Guidance Notes do not particularly concern any other aspects of the AML/CFT State Ordinance, such as CDD measures in respect of new customers and the requirements regarding reporting of unusual transactions, record keeping and an adequate administrative organization and internal control system. Reference is made to the AML/CFT State Ordinance and the Enactment State Ordinance for further details on the requirements and the relevant transitional provisions (if any). Note that no transitional periods apply with regard to, *inter alia*, the obligation to perform CDD measures in respect of new customers and to report unusual transactions to the MOT.

4. Although these Guidance Notes are aimed specifically to fulfill the CBA's obligation under Article 2, paragraph 7, of the Enactment State Ordinance, they may also be helpful for Service Providers when formulating CDD and customer acceptance policies, procedures and measures as meant in Article 46 of the AML/CFT State Ordinance.

5. These Guidance Notes are aimed at the following Service Providers:

	Financial service provider: anyone who on a commercial basis conducts one or more of the following activities or operations to or for the benefit of a customer:
1.	To accept deposits and other repayable funds from the public.
2.	To grant loans.
3.	Financial leasing, with the exception of consumer-related leasing.
4.	To transfer or to cause the transfer of money or values.
5.	To issue and manage means of payment other than money, at any rate including credit cards, debit cards, checks, traveler's checks, bank and money orders, and electronic money.
6.	To provide financial guarantees and commitments.
7.	To trade in money market instruments, foreign currency, payment instruments, shares, exchange, interest, and index instruments, transferable securities, and commodities futures trading.
8.	To participate in the issue of securities and to provide financial services related to this issue.
9.	To manage individual and collective investment portfolios.
10.	To receive for safekeeping and manage cash or liquid securities on behalf of third parties.
11.	To otherwise invest, administer, or manage funds or moneys on behalf of third parties.
12.	To underwrite, redeem and pay, as well as to act as an intermediary, in the underwriting, redeeming and payment of a life insurance agreement as meant in Article 1 of the SOSIB, and other investment-related insurance products.
13.	To exchange money and foreign currency.
	Designated non-financial service provider:
1.	A natural person, legal person, corporation or partnership that acts as a lawyer, civil notary, tax advisor or in the exercise of a similar legal profession or company.
2.	A natural person, legal person, corporation or partnership that acts as an external registered accountant, an external accountant-administration consultant or a similar profession.
3.	A natural person, legal person or corporation which on a commercial or professional basis trades on or acts as an intermediary in the purchase and sale of immobile objects, vehicles,

	ships, aircraft, objects of arts, antiquities, and the rights to which these objects can be subjected.
4.	A natural person, legal person, or corporation who/which trades in precious metals, precious stones and jewels on a commercial or professional basis.
5.	A casino as meant in Article 1, paragraph 1, of the State Ordinance Games of Hazard (AB 1990 No. GT 44), as well as an internet casino.
6.	A trust and company service provider as meant in Article 1 of the SOSTSP.

6. Please note that it only concerns institutions that are **not** already licensed or registered by the CBA pursuant to the SOSCS, SOSIB, SOSMTC or SOSTSP. If a Service Provider will in the future become licensed or registered by the CBA pursuant to the SOSCS, the SOSIB, the SOSMTC, the SOSTSP or other sectoral supervisory law, these Guidance Notes will no longer apply. In such case, the CBA's AML/CFT Handbook is applicable. The AML/CFT Handbook contains mandatory requirements as well as guidance notes.

1.2 LEGAL STATUS OF THE GUIDANCE NOTES

7. The Guidance Notes are not legally binding. They present ways of complying with the AML/CFT State Ordinance and must always be read in conjunction with these statutory requirements. This allows a Service Provider 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 Service Provider is in compliance with the statutory requirements.

1.3 OBJECTIVES OF THE GUIDANCE NOTES

8. The objectives of these Guidance Notes are as follows:
   - to explain the background of the AML/CFT State Ordinance and the importance of preventing and combating money laundering and terrorist financing.
   - to outline the requirements of the AML/CFT State Ordinance and the Enactment State Ordinance related legislation in respect of the existing customer base.
   - to assist a Service Provider to comply with the requirements of the AML/CFT State Ordinance described above through practical interpretation;
   - to provide a base from which Service Providers can design, tailor and implement their own risk assessment policies and accompanying CDD procedures;
   - to promote the use of a proportionate risk based approach to CDD measures which directs resources towards higher risk customers.

2. BACKGROUND OF THE GUIDANCE NOTES

2.1 FIGHTING MONEY LAUNDERING AND TERRORIST FINANCING

9. Money laundering and terrorist financing are a serious threat to a country's economy and can affect economic growth. Moreover, the failure to have in place an effective AML/CFT regime that meets international standards could have adverse cost implications both for domestic institutions and for international trade. Furthermore, the soundness, integrity and stability of the financial sector and the confidence in the financial system as a whole could be seriously jeopardized by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. Both money laundering and terrorist financing affect the integrity and reputation of a country's financial sector as a whole and of individual financial and other service providers.[1]

10. A key imperative for Aruba is to ensure that the financial system cannot be used for the purposes of money laundering and terrorist financing. Aruba has a strong commitment at political, government and industry level to play an active part in the international fight against money laundering and terrorist financing. Accordingly, the authorities of Aruba will take a strong line toward any business or profession that assists in money laundering and terrorist financing, 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.

2.2 FATF

11. The Aruban AML/CFT legislation is based on the recommendations of the FATF. The FATF is an inter-governmental body, established in 1989, whose purpose is the development and promotion of policies to combat money laundering and terrorist financing, both at national and international levels. The Kingdom of the Netherlands, and thus Aruba, is a FATF member.

12. The FATF has drawn up 40 Recommendations to combat money laundering and 9 Special Recommendations to combat terrorist financing. The 40 + 9 Recommendations, together with their interpretative notes, are recognized to provide the international AML/CFT standards. The FATF monitors progress made by member governments in implementing the FATF Recommendations, primarily through its mutual evaluation programme.

13. Furthermore, the FATF undertakes regular exercises which identify and describe trends in the means used by money launderers and terrorist financers. The result of the typology work conducted by the FATF can be found on the FATF website (http://fatf-gafi.org/typologies).

2.3 AML/CFT STATE ORDINANCE

14. In 2008, the FATF, together with the CFATF, conducted an evaluation of the Aruban AML/CFT system. The mutual evaluation report assessed Aruba's level of compliance with the FATF Recommendations. It identified many areas of good practice, but also made recommendations on how to strengthen certain aspects of the system. In order to implement strong AML/CFT defences, the State Ordinance on the Identification when Providing Services (AB 1995, no. 86) and the State Ordinance on the Reporting obligation of Unusual Transactions (AB 1996, no. 85) have been merged in the AML/CFT State Ordinance. Furthermore, it contains strengthened requirements in the area of CDD, and takes care of the inconsistencies between the previous State Ordinance on the Identification when Providing Services and the State Ordinance on the Reporting obligation of Unusual Transactions. On 1 June 2011, the AML/CFT State Ordinance entered into force.

[1] Refer to the FATF Report "Global Money Laundering & Terrorist Financing Threat Assessment", July 2010 (available on the FATF website: http://www.fatf-gafi.org/dataoecd/48/10/45724350.pdf).

15. The provisions of the AML/CFT State Ordinance can be summarized as follows:
- in certain prescribed situations, a Service Provider must undertake CDD measures (which go beyond the identification of the customer and the verification of his identity);
- the extent of CDD measures is to be determined on a risk sensitive basis;
- the AML/CFT State Ordinance determines certain high risk situations, which require enhanced CDD measures;
- unusual transactions must be reported to the MOT;
- the AML/CFT State Ordinance provides for record keeping requirements;
- a Service Provider must set adequate policies and have written procedures and measures aimed at the prevention of money laundering and terrorist financing;
- as part of those measures, a Service Provider must appoint a MLCO and a MLRO.

Please note that the above list only provides a high level outline of the obligations set out in the AML/CFT State Ordinance, and is therefore not exhaustive. For a complete overview, refer to the text of the AML/CFT State Ordinance itself.

16. The AML/CFT State Ordinance introduces a risk-oriented approach and creates flexibility for the Service Provider. At the same time it implies greater responsibility. Service Providers have to assess the risk exposure entailed by certain customers, products and services and have to align their efforts accordingly. Mandatory rules are not imposed on institutions on how to comply, but rather what has to be complied with. A Service Provider, however, must ensure that it maintains adequate AML/CFT policies, procedures and measures to ensure that the AML/CFT State Ordinance is complied with. Moreover, a Service Provider must ensure that its employees are familiar with the provisions of the AML/CFT State Ordinance and that they receive regular training in order to enable them to recognize unusual transactions.

17. Each Service Provider must recognize the role that it must play in protecting itself, and its employees, from involvement in money laundering and terrorist financing, and also in protecting Aruba's reputation of probity.

18. Businesses or professions not acting in compliance with the AML/CFT State Ordinance will risk administrative sanctions, including a direction (*aanwijzing*), a penalty charge order (*last onder dwangsom*) or an administrative fine (*bestuurlijke boete*), and criminal prosecution. Moreover, they will face the loss of their reputation.

2.4 UNDERSTANDING MONEY LAUNDERING AND TERRORIST FINANCING

2.4.1 MONEY LAUNDERING

19. The Criminal Code contains various money laundering provisions included in Articles 430b, 430c and 430d. Money laundering occurs whenever there is any form of relationship or arrangement involving monies or other assets that are proceeds of a crime, including, but not limited to, the receiving, holding, transfer or disguising the origin of such assets. Proceeds of crime may be generated in various ways, for example trafficking of drugs, aggravated theft, illegal arms trafficking, corruption and people smuggling, but also tax fraud.

20. Traditionally, money laundering has been described by reference to the following three distinct phases:
- Placement: The funds generated from crime are placed into the financial system either directly or indirectly. This is the point at which the proceeds of crime are most apparent. For example, deposit takers, money transfer companies and cash based businesses are vulnerable to being used at this stage.
- Layering: The illicit proceeds are separated from their criminal source by creating complex layers of financial transactions and corporate structures designed to disguise the audit trail and provide anonymity. This stage can involve a range of different businesses, products and entities.
- Integration: Once the criminal origin of the funds has been obscured, they are integrated back into the economy as legitimate funds or assets. All financial and non–financial businesses and professions are vulnerable to being used at this stage.

21. The aforementioned traditional model is useful, but it does not adequately explain all situations in which money laundering occurs where the facts do not fit the model. In some cases, money laundering may be more about disguising ownership of property rather than any of the three stages described above.

22. A Service provider itself may also be held liable under the Criminal Code for negligent money laundering (*schuldwitwassen*) or aiding and abetting (*medeplichtigheid*), for example where a Service Provider receives, holds or transfers assets that are proceeds of crimes or is in involved in or advises on (financial) transactions concerning such assets.

2.4.2 TERRORIST FINANCING

23. Terrorist financing is punishable under Article 140a of the Criminal Code. Terrorist financing can be summarized as the financing of terrorist acts, terrorists or terrorist organizations. This includes the directly or indirectly collecting of, or making available, monies or other assets that are used for the commission of a terrorist offense or for the support of persons or organizations that commit or intend to commit terrorist offenses, or an offense to prepare or facilitate a terrorist offense or to support persons or organizations that commit or intend to commit terrorist offenses.[2]

[2] Refer to the FATF Report "Terrorist Financing", 29 February 2008 (available on the FATF website: http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf).

3. CUSTOMER RISK ASSESSMENT AND RISK RATING

3.1 RISK BASED APPROACH

24. Pursuant to Article 6, paragraph 3, of the AML/CFT State Ordinance, a Service Provider must tailor the CDD measures to the risk-sensitiveness for money laundering or terrorist financing in relation to the type of customer, business relationship, product, or transaction. The Service Provider is therefore required to develop a risk based approach to determining the type and extent of CDD measures to apply to different types of customers, products and services. For example, the type and extent of customer identification information and relationship information, the nature of verification of the information obtained, and the level of business relationship monitoring activity.

25. A risk based approach will serve to balance the cost burden placed on a Service Provider and on their customers with the risk that the Service Provider may be used in money laundering and terrorist financing by focusing resources on higher risk areas.

26. 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 money laundering or terrorist financing does not mean that the customer is not a money launderer or financing terrorism. Note also that over time, based upon the ongoing monitoring and review of the business relationship and customer risk profile, a customer risk may change, i.e. a lower risk customer may migrate into a medium or higher risk customer or vice versa.

3.2 RISK RATING OF THE EXISTING CUSTOMER BASE

3.2.1 INTRODUCTION

27. As mentioned above, a Service provider must formulate and adopt a policy document and accompanying CDD procedures to risk rate its existing customer base. An existing customer means any customer that the Service Provider maintains a continuing business relationship with as at the date that the AML/CFT State Ordinance came into force (i.e. June 1, 2011). In accordance with Article 1, paragraph 1, of the AML/CFT State Ordinance a business relationship in this context means any business, professional, or commercial relationship between a Service Provider on the one hand, and a customer on the other hand, which is connected to the commercial or professional activities of the Service Provider, and which is assumed to last some time.

28. 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 to catch up with the requirements of the AML/CFT State Ordinance, the Enactment State Ordinance contains transitional arrangements to allow Service Providers a maximum time frame within which to upgrade the information required. It is explicitly required that a Service Provider 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 following timetables set out in the transitional provisions of Article 2 of the Enactment State Ordinance:
    - Within 8 months as of June 1, 2011: formulate and adopt a policy document and accompanying CDD procedures to risk rate existing customers.
    - Within 10 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 12 months as of June 1, 2011: carry out and complete full CDD measures on high risk customers, including in any case higher risk situations as indicated in Articles 11 to 13, paragraphs 1 and 2, of the AML/CFT State Ordinance (refer to Section 4.1.2 on enhanced CDD measures).
    - Within 18 months as of June 1, 2011: carry out and complete full CDD measures on medium risk customers.
    - Within 30 months as of June 1, 2011: carry out and complete CDD measures on low risk customers, including in any case lower risk situations as indicated in Article 10, paragraphs 1, of the AML/CFT State Ordinance (refer to Section 4.1.3 on simplified CDD measures).

29. The first two stages of the catching up exercise are further explained in the remainder of this section. Sections 4.2 and 4.3 elaborate on the latter three stages.

30. For the benefit of Service Providers, and in accordance with Article 2, paragraph 7, of the Enactment State Ordinance, the CBA has drafted these Guidance Notes as an aid to design, tailor and implement their own risk assessment policies and accompanying CDD procedures to risk rate their existing customer base.

31. Note that irrespective of the risk rating allocated to existing customers, or the Service Provider's progress through the transitional arrangements, in accordance with Article 6, paragraph 1, subsections d and e, and Article 6, paragraph 2, subsection g in conjunction with Article 6, paragraph 1, subsections d and e, of the AML/CFT State Ordinance, CDD measures must always be applied immediately:
    - where a Service Provider suspects money laundering or terrorist financing; or
    - where a Service provider has doubts about the veracity or adequacy of documents, data or information that is held.

3.2.2 RISK ASSESSMENT

32. A Service Provider must determine its initial approach to performing the CDD process with regard to its existing customers, depending on the type of customer, business relationship, product or transaction involved.

33. As a starting point, to adequately carry out such an exercise, a Service Provider may conduct and document a business risk assessment at a macro level (step 1). In particular, the Service Provider may consider the extent of its overall 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.

34. As part of its business risk assessment, a Service Provider may consider the following questions:
    - What are we, who are we and what do we do?
    - How and where do we carry on our business activities?
    - Who do we do business with?
    - Where do our customers reside?
    - Are we a complex or simple business?
    - Do we have multiple or single premises?
    - Do we rely on any third party to process our business or act on our behalf?
    - Is our head office in another jurisdiction?
    - Do we have any branches or subsidiaries in other jurisdictions?

35. The next step – following the business risk assessment – will then be to determine a risk assessment and risk classification of existing customer relationships, based on the type of customer, business relationship, product or transaction involved (step 2). The sophistication of the risk customer assessment process can be determined according to factors established by the business risk assessment. Below examples of risk factors (regarding type of customer, business relationship and product or transaction) that can be used are further explained. Please note that the AML/CFT Ordinance has designated certain customers, products and services as high risk in which situations enhanced CDD is mandatory. Furthermore, the AML/CFT State Ordinance prescribes certain situations in which simplified CDD is allowed. Refer to Sections 4.1.2 and 4.1.3, respectively.

3.2.3 CUSTOMER RELATING RISK FACTORS

36. Determining the potential money laundering or terrorist financing risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. Based on its own criteria, a Service Provider should seek to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. In particular, some countries pose an inherently higher risk than others. Customers that are associated with higher risk countries, as a result of their citizenship, country of business, country of residence, etc. require enhanced CDD measures, depending upon their overall risk profile taking into account all other relevant factors.

37. The factors below relating to a customer may be relevant when assessing and evaluating the risk profile of a customer. These factors are not exhaustive. A Service Provider 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.

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.
- Customers who have no address, or multiple addresses, without legitimate reasons.
- Transparency of customer. For example, customers where the structure or nature of the entity or relationship makes it difficult to identify the true UBOs may indicate higher risk.
- Unwillingness or reluctance to provide information.
- Lack of contact, when this would normally be expected.
- 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, where a customer requests undue levels of secrecy, where a customer appears to be structuring a transaction in various smaller transactions below the designated thresholds in an attempt to avoid the filing of an unusual transaction report (also known as smurfing), 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.
- Inexplicable changes in ownership or subsequent altering of the legal structure of a customer (change of name or corporate seat).
- 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.
- Position of intermediaries is unclear.
- In the case of an express trust or foundation, 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.
- In the case of an express trust or foundation, the nature of classes of beneficiaries and classes within an expression of wishes.
- Customers with multi-jurisdictional operations that do not have adequate centralized corporate oversight.

Country risk:

- Residence in or connection with higher risk jurisdictions. The following jurisdictions present a higher risk:
  - those that are generally considered to be un-cooperative in the fight against money laundering or terrorist financing;
  - those that have inadequate AML/CFT safeguards in place;
  - those that have high levels of organized crime;
  - those that have strong links (such as funding or other support) with terrorist activities;
  - those that are vulnerable to corruption; and
  - 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) are relevant.
- Geographical sphere of business activities, e.g. the location of the markets in which a customer does business.
- Familiarity of a Service Provider 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 Service Provider's own operations within that country.

38. Further to the abovementioned general risk factors, the following appendices will provide some examples of sector-specific customer risk factors:
    - Appendix 1: Examples of risk factors for legal professionals and accountants.
    - Appendix 2: Examples of risk factors for real estate agents.
    - Appendix 3: Examples of risk factors for dealers in precious metal and stones.
    - Appendix 4: Examples of risk factors for casinos.
    - Appendix 5: Examples of risk factors for Non-Regulated Financial Service Providers.

3.2.4 PRODUCT OR SERVICE RELATED RISK FACTORS

39. The relevant risk factors relating to the business relationship, product or transaction involved will depend on the type of Service provider concerned. Refer to the appendices listed in paragraph 38 above.

3.2.5 RELEVANT OTHER INFORMATION SOURCES

40. Also refer to the following FATF guidance documents, that provide, *inter alia*, sector-specific risk factors:
    - "RBA Guidance for legal professionals", 23 October 2008, in particular Section 3 containing guidance for legal professionals on implementing the risk-based approach.
    - "RBA Guidance for accountants", 17 June 2008, in particular Section 3 containing guidance for accountants on implementing the risk-based approach.
    - "RBA Guidance for real estate agents", 17 June 2008, in particular Section 3 containing guidance for real estate agents on implementing the risk-based approach.
    - "RBA Guidance for dealers in precious metal and stones", 17 June 2008, in particular Section 3 containing guidance for dealers on implementing the risk-based approach.
    - "RBA Guidance for Casinos", 23 October 2008, in particular Section 3 containing guidance for casinos on implementing the risk-based approach.
    - "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing", June 2007.
    - "Risk-Based Approach Guidance for the Life Insurance Sector", October 2009, also containing guidance for life insurance intermediaries on implementing a risk-based approach.

    These (and other) FATF guidance documents can be found on the FATF website: http://www.fatf-gafi.org/document/21/0,3746,en_32250379_32235720_44123221_1_1_1_1,00.html.

41. Furthermore the following FATF Typology Reports may, in any case, be relevant:
    - "Vulnerabilities of Casinos and Gaming Sector", March 2009.
    - "Money Laundering and Terrorist Financing in the Securities Sector", October 2009.
    - "Money Laundering and Terrorist Financing Through the Real Estate Sector", 29 June 2007

    These (and other) FATF Typologies Reports can be found on the FATF website: http://www.fatf-gafi.org/typologies.

42. For Service providers involved in real estate, the Dutch Financial Expertise Centre (*Financieel Expertise Centrum* or FEC) identified red flags in relation to the misuse of real estate, relevant for, *inter alia*, real estate agents, notaries, lawyers, accountants and financial institutions (*Red flags Misbruik Vastgoed – actualisering 2010*, available on the FEC website: http://www.fec-partners.nl).

4. CDD REQUIREMENTS

4.1 GENERAL FRAMEWORK

43. CDD plays a crucial role in achieving the objective of the AML/CFT state ordinance, i.e. to prevent and combat money laundering and terrorist financing. The CDD obligations on Service Providers are designed to make it more difficult for the (financial) service industry to be used for money laundering or terrorist financing.

44. Sound CDD measures are vital because they:
- help to protect the Service Provider and the integrity of the sector in which it operates by reducing the likelihood of the Service provider becoming a vehicle for, or a victim of, financial crime; and
- assist law enforcement, by providing available information on customers or activities and transactions being investigated – following an unusual transaction report to the MOT.

45. The statutory CDD requirements involve the application of basic CDD measures. Furthermore, the AML/CFT State Ordinance requires Service Providers to apply enhanced CDD measures in higher risk situations. On the other hand, the AML/CFT State Ordinance allows Service providers to apply simplified CDD measures in certain designated lower risk situations.

4.1.1 BASIC CDD MEASURES

46. The basic CDD measures required by Articles 3 to 5 of the AML/CFT State Ordinance 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 Service provider's knowledge of the customer and the UBO.

4.1.2 ENHANCED CDD MEASURES

47. Pursuant to Article 11 of the AML/CFT State Ordinance, a Service Provider must perform enhanced CDD if and when a business relationship or a transaction by its nature entails a higher risk of money laundering or terrorist financing. 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 customer is not a resident of Aruba, respectively not established in Aruba;
- if a customer 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.

48. Pursuant to Article 13, paragraph 1, of the AML/CFT State Ordinance, a Service Provider must pay special attention to:
a. 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;

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

49. If a Service Provider 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 48 does not have an apparent economic or lawful purpose, or if a transaction as meant in paragraph 48, under a, 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. Moreover, the filing of an unusual transaction report to the MOT may be required. In accordance with Article 13, paragraph 3, of the AML/CFT State Ordinance, the findings must be kept for at least ten years.

4.1.3 SIMPLIFIED CDD MEASURES

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

51. 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 that is subject to internationally accepted AML/CFT requirements and that it is adequately supervised;
- companies of which the shares are traded on stock exchanges as designated by the Minister of Finance and that are subject to statutory financial reporting disclosure requirements.
- public limited companies of which all shares are held by the State of Aruba (*Land Aruba*);
- the country of Aruba (Land Aruba) and other public legal persons established in Aruba (see paragraph 56 below);
- public legal persons established and active in other parts of the Kingdom of the Netherlands.

52. 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;
- UBOs to accounts kept with a Designated Non-Financial Service Provider intended solely for the keeping of money for third parties, provided that the service provider is subject to internationally accepted AML/CFT requirements and that it is adequately supervised.

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

54. Pursuant to Article 10, paragraph 3, of the AML/CFT State Ordinance, a Service Provider must not apply simplified CDD measures if the customer, business relationship or transaction carries a higher risk for money laundering or terrorist financing of if there are indications that the customer is involved with money laundering or terrorist financing.

55. A Service Provider 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 Service Provider has considered the following (cumulative):
- 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.

56. 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).

57. 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. De Nederlandsche Bank, Centrale Bank van Curaçao en Sint Maarten).

4.1.4 WHEN TO APPLY CDD MEASURES

58. Article 6, paragraph 1 and 2, of the AML/CFT State Ordinance prescribes the various situations per category of Service Providers in which CDD measures must be applied.

59. Pursuant to Article 8, paragraph 1, of the AML/CFT State Ordinance, a Service Provider 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 to this basic rule:
- a Service Provider may verify the identity of the customer and the UBO during the establishment of the business relationship, if this is necessary in order not to disrupt the service provision, and there is little risk of money laundering or terrorist financing; in this case, the Service Provider shall verify the identity as soon as practicable after the first contact with the customer;
- a Service Provider being a civil notary can establish the identity of the customer and verify the UBO when identification is required pursuant to Article 20, first paragraph, of the State Ordinance on Civil Notaries (*Landsverordening op het notarisambt*, AB 1990, no. GT 69).

60. According to Article 9, paragraph 1, of the AML/CFT State Ordinance, a Service Provider must not enter into a business relationship or carry out an occasional 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. Pursuant to Article 9, paragraph 2, of the AML/CFT State Ordinance, a Service Provider 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.

4.2 CDD PROCESS IN 7 STEPS

61. Below, the basic CDD process is summarized in 7 steps:

Step 1:	**Applicability of CDD requirements** Assess whether or not the business relationship or transaction falls within the scope of the AML/CFT State Ordinance: • All Service Providers: i) the establishment in or from Aruba of a business relationship. ii) if there are indications that the customer is involved in money laundering or terrorist financing. iii) if the Service Provider doubts the soundness or reliability of data obtained from the customer previously. iv) if the risk of involvement of an existing customer in money laundering or terrorist financing gives reason to do so. • Non-Regulated Financial Service Provider: the performance in or from Aruba of a transaction, or two or more related transactions, for the benefit of the customer with a value of Afl. 25,000.- or more. • Lawyers, (candidate) notaries, tax advisors, accountants, or similar profession: the services designated in Article 6, paragraph 2, subsection b of the AML/CFT State Ordinance. • Real estate agent and other high value dealers: i) the purchase and sale in or from Aruba of register objects, as well as the rights to which these objects can be subjected (no threshold applicable).

	ii) the performance of cash transactions with a value of Afl. 25,000.- or more. • Casino: the performance of cash transactions with a value of Afl. 5,000.- or more.
Step 2:	**Identification** Collect relevant identification information on a customer: • Natural person: the surname, given names, date and place of birth, and address. • Legal person: the legal form, name under the Articles of Association, trade name, address, and, if the legal person is listed with the Chamber of Commerce, the registration number, and of the persons acting on behalf of the legal person the surname, given names, and date of birth; Record and retain the information collected.
Step 3:	**Verification** Verify the customer's identity using reliable documents, data or information from a reliable and independent source, for example: • Resident natural person: passport, driver's license or identity card. • Non-resident natural person: passport. • Domestic legal person: company registry extract. • Foreign legal person: documents, data, or information that is reliable and internationally accepted or recognized by law in the state of origin of the customer as a valid means of identification. Record and retain the identification verification methods and documents used.
Step 4:	**UBO** If the customer is a legal person or arrangement (such as a trust), then also the UBO must be identified and his identity must be verified (see steps 2 and 3 above).
Step 5:	**PEP** Determine whether a customer or a UBO is a PEP. Also involve immediate family members and close associates. Check internet, reliable (inter)national PEP-lists or other reliable information sources. If a customer or a UBO is a PEP, senior management approval is required to enter into the business relationship or perform the transaction.
Step 6:	**Relationship information and risk assessment** Higher risk customers or services trigger more sophisticated CDD measures, including more far-reaching verification methods. To establish an adequate customer risk profile, the Service Provider assesses: • The purpose and intended nature of the business relationship. • The nature of the transaction. • The source and destination of the funds or other assets involved in the business relationship or transaction. The Service Provider thus collects information from the customer: What does the customer want, and why, and does this make sense? The customer risk profile will enable a Service Provider 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 money laundering or terrorist financing activity. Record and retain the information collected and the customer risk profile.
Step 7:	**Monitoring and review** Ongoing attention to the risk profile of a customer and monitoring whether the transactions are consistent with the expected business activity and transactions. If this is not the case, updating of the customer risk profile may be required. Self-evidently, the Service Provider will consider whether the filing of an unusual transaction report to the MOT is required.

62. The above overview provides a high level summary of the CDD process and requirements. Although this overview will probably suffice for most customers, business relationships or transactions, it may not for all. For more complex and higher risk customers, business relationships or transactions, a more sophisticated approach may be appropriate in line with the prescribed risk based approach. The AML/CFT Handbook (available on the CBA website) may in these situations also serve as useful guidance.

4.3 APPLYING CDD MEASURES TO EXISTING CUSTOMERS

63. Pursuant to of the Enactment State Ordinance, a Service Provider must apply the aforementioned CDD measures in line with the provisions in the AML/CFT State Ordinance applicable to that relationship.

64. After the Service Provider has conducted a risk assessment of its customer base, and subsequently has reviewed the existing customer files and applied and recorded a risk rating (high, medium or low) for each customer, the next stage is the actual updating and upgrading of the quality of information held on existing customers. Starting with high risk customers, the Service Provider will for each customer progress through steps 2 to 6 as mentioned in paragraph 61 above.

APPENDIX 1: Examples of risk factors for legal professionals and accountants

Client risk:
• Reason for a client choosing the firm is unclear, given the firm's size, location or specialization. • Unexplained urgency of assistance required. • Frequent or unexplained change of professional adviser(s), accountants or members of management. • Use of many different firms of accountants and advisers for connected companies and businesses; • Client instructions or funds outside of their personal or business sector profile. • Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear. • Employee numbers or structure out of keeping with size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used). • Sudden activity from a previously dormant client. • Client starts or develops an enterprise with unexpected profile or early results. • Indicators that a client does not wish to obtain necessary governmental approvals/filings, etc. • A client that offers to pay extraordinary fees for services which would not ordinarily warrant such a premium. • Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment. • Clients who offer to pay extraordinary fees for services which would not ordinarily warrant such a premium.
Product or service risk:
• Misuse of pooled client accounts or safe custody of client money or assets. • Advice on the setting up of legal arrangements, which may be used to obscure ownership or real economic purpose (including setting up of trusts, companies or change of name/corporate seat or other complex group structures). • Complex or unusually large transactions, particularly where underlying beneficial ownership is difficult to ascertain and/or where the underlying transactions have been conducted in cash. • Unusual patterns of transactions which have no apparent economic purpose particularly those where a number of jurisdictions and different entities are involved for no logical business reason. • Transactions outside of the normal course of business or where the method or payment/receipt is not usual business practice, such as wire transfers or payments in foreign currency. • Transactions with companies whose identity or beneficial ownership is difficult to establish; • Unusual numbers of cash transactions for substantial amounts or a large number of small transactions that add up to a substantial amount. • Private loan agreements or acknowledgements of debt where the source of funds is unclear. • Loan-back schemes where the client de facto – whether directly or indirectly – lends money to himself. • Back-to-back loan schemes where the client receives funds or financial instruments and provides collateral, whether direct or indirect, from his own liquid assets. • Use of shell companies, trusts or other structures that are merely being used as a front for other activities. • Securities transactions where it is difficult to asses the value of the securities. • Changing instructions, such as: o a client deposits funds into a firm's client account, but then ends the transaction for no apparent reason; o a client advises that funds are coming from one source and at the last minute the source changes; and o a client unexpectedly requests that money received into a firm's client account be sent back to its source, to the client or to a third party. • Misuse of introductory services, e.g. to financial institution.
Product or service risk for accountants:
• Over and under invoicing of goods/services. • Multiple invoicing of the same goods/services.

- Falsely described goods/services – over and under shipments (e.g. false entries on bills of lading).
- Multiple trading of goods/services.
- Loss-making transactions where the loss is avoidable.
- Company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues to operate without reasonable explanation of the continued loss.
- Dealing with money or property when there are suspicions that it is being transferred to avoid the attention of either a trust in a bankruptcy case, a revenue authority, or a law enforcement agency.
- Abnormally extensive or unusual related party transactions;
- Excessive use of off-balance sheet transactions or activity.
- Payments for unspecified services or for general consultancy services.

Product or service risk for legal professionals:

- Services where legal professionals, acting as financial intermediaries, actually handle the receipt and transmission of funds through accounts they actually control in the act of closing a business transaction.
- Services to conceal improperly beneficial ownership from competent authorities.
- Services requested by the client for which the legal professional does not have expertise.
- Transfer of real estate between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
- Administrative arrangements concerning estates where the deceased was known to the legal professional as being a person who had been convicted of proceeds generating crimes.
- Client using financing structures outside the regular financial sector (e.g. financing raised from family members abroad).

APPENDIX 2: Examples of risk factors for real estate agents

Customer risk:
• Significant and unexplained geographic distance between the agent and the location of the customer. • Location of customer's source of funds. • The use of intermediaries who are not subject to adequate AML/CFT requirements and who are not adequately supervised. • Brand new customer carrying out large occasional transactions.
Product or service risk:
• Speed of the transaction (transactions that are unduly expedited without a reasonable explanation may be higher risk). • Type of properties (residential or commercial, vacant land, investment, high-turnover properties, multi-unit properties for lettings/leases). • Successive transactions, especially of same property in short period of time with unexplained changes in value. • Conversion of properties into smaller units. • Introduction of unknown parties at a late stage of transactions, e.g. arrangements made between purchasers. • Third-party vehicles (i.e. trusts) used to obscure true ownership of buyer. • Under- or over-valued transactions. • Sale of properties immediately before restraint or insolvency. • Property value does not match with the profile of the customer. • Unusual sources, e.g. funds obtained from unknown individuals or unusual organizations. • Purchase with large amounts of cash. • Cash deposits or money orders from unusual sources or countries as identified under country/geographic risks. • Use of complex loans, or other obscure means of finance, versus loans from regulated financial institutions. • Unexplained changes in financing arrangements.

APPENDIX 3: Examples of risk factors for dealers in precious metal and stones

Retail customer risk:
• Use of cash. It should be recognized, however, that many persons desire anonymity in , especially jewelry, purchases for purely personal reasons, or at least the absence of paper records, with no connection to money laundering or terrorist financing. • Payment by or delivery to third parties. However, not all third party payments are indicative of AML/CFT. It may be common in jewelry purchases that a woman will select an article of jewelry, and a man will later make payment and direct delivery to the woman. • Brand new customer carrying out large occasional transactions.
Business counterparty risk:
• A counterparty that does not understand the industry in which he proposes to deal, or does not have a place of business or equipment or finances necessary and appropriate for such engagement, or does not seem to know usual financial terms and conditions. • Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit. • Has significant and unexplained geographic distance from the dealer. • Uses banks that are not specialized in or do not regularly provide services in such areas, and are not associated in any way with the location of the counterparty and the products. • Makes frequent and unexplained changes in bank accounts, especially among banks in other countries. • Involves third parties in transactions, either as payers or recipients of payment or product, without apparent legitimate business purpose. • Will not identify beneficial owners or controlling interests, where this would be commercially expected. • Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries. • Uses cash in its transactions with the dealer, or with his own counterparties in a nonstandard manner. • Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose.
Product risk:
• All diamonds, jewels, and precious metals can potentially be used for money laundering and terrorist financing, but the utility and consequent level of risk are likely to vary depending on the value of the product. Unless transactions involve very large quantities, lower value products are likely to carry less risk than higher value products. However, dealers must be aware that values can be volatile dependent upon supply and demand. Relative values of some materials can vary dramatically between different countries, and over time. • Dependent upon the nature of the transaction, counterparties, and quantities, gold can be higher risk. Pure gold, or relatively pure gold, is the same substance worldwide, with a worldwide price standard published daily, and it can also be used as currency itself, e.g. by hawalas. Gold is available in a variety of forms, e.g. bars, coins, jewelry, or scrap, and trades internationally in all of these forms. • The physical characteristics of the products offered are also a factor to consider. Products that are easily portable and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border money laundering. For example, diamonds are small, light in weight, not detected by metal detectors, and a very large value can be easily concealed. • The risk of dealing in stolen or fraudulent products must be taken into account. As with all valuable objects, diamonds, jewels and precious metals are attractive to thieves, and dealers must be aware of the risks of trading in stolen products. For example, jewelry dealers, pawn shops and buyers of used gold jewelry should remain alert to the possibility of being offered stolen jewelry. In addition to stolen goods, dealers should be aware of the risks associated with fraudulent goods, such as synthetic diamonds represented as natural diamonds, or 14 karat gold represented as 18 karat.

APPENDIX 4: Examples of risk factors for casinos

Customer risk:
• High spenders. Given the variations among casinos, the level of spending considered to be relatively high for an individual customer will vary among operators, and even among casinos owned and managed by the same operator. Customers may become high spenders because of their cumulative spending over a period of time (e.g. customers with relatively high level of spending with casino accountholder relationships). Similarly, casual customers who gamble a relatively large amount of money on a limited number of occasions, perhaps even during a single visit, could equally be considered as high spenders. • Most casinos will have formal or informal policies which centre upon customers whom they consider to be high spenders. These policies may relate to commercial risk, or to marketing information to identify high spending customers provided with complementary goods and services (e.g. refreshments, food, entertainment, merchandise, lodging, show tickets and tickets to special events, or transportation). Some casinos offer special facilities to high spending customers, e.g. the use of VIP rooms to gamble away from the general public areas of casinos. Casinos need to ensure that AML/CFT policies, procedures and measures are applied consistently to all customers. • Disproportionate spenders. Casinos should devise policies relative to obtaining information about customers' financial resources, when feasible and available, to determine if customers fall into this category. • Casual customers. While casual customers can pose a higher money laundering risk in some situations, it may be difficult to identify their associated spending patterns. This category would include tourists, although not all passing tourist trade will fall within this definition. Casinos may host tourists on organized gambling tours, which are discussed below. However, even regular customers may pose a risk, particularly if their spending pattern changes, e.g. it dramatically increases or their rated play does not fit their playing profile e.g. minimal play. • Use of third parties. Criminals may use third parties, or anonymous or identified agents to avoid CDD undertaken at a threshold. They may also be used to gamble, e.g. to break up large amount of cash. Third parties may be used to buy chips, or to gamble on behalf of others with minimal play (which may include early or high cash outs), or cash out/redeem chips for larger denomination currency, casino checks, etc. • Junkets. Over-reliance on tour operators can pose a higher money laundering risk. Casinos need to ensure that AML/CFT policies, procedures and measures are applied consistently to all customers.
Product or service risk:
• Proceeds of crime. However money is transferred to a casino, there is a risk that this money will have arisen from illegal activities such as check fraud, credit/debit card fraud, trafficking of drugs. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk. • Cash. Customers may use a casino to exchange large amounts of illicit proceeds denominated in small bills for larger ones that are easier to hide or transport. Also, certain cash deposits by a customer, especially cash deposits which are considered relatively large either in relation to i) a particular casino's average receipts, or ii) what is known about a customer's financial status. The same applies to the redemption of chips, tickets or tokens for currency. • Casinos may also be aware of customers borrowing money from non-conventional sources, including other customers. Informal money lending can be illegal, and it can also offer criminals an opportunity to introduce proceeds of crime, usually cash, into the legitimate financial system through the casino. • Use of casino deposit accounts. Casinos will wish to encourage their customers to only use their deposit accounts for gambling purposes. Casinos need to consider what constitutes an abuse of such an account and should have policies, procedures and measures to prevent customers from using such accounts to deposit and withdraw without gambling or minimal play.

APPENDIX 5: Examples of risk factors for Non-Regulated Financial Service Providers

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 where the Service Provider 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 (i.e. the entire process for capital markets and payment transactions to be conducted electronically without the need for manual intervention).