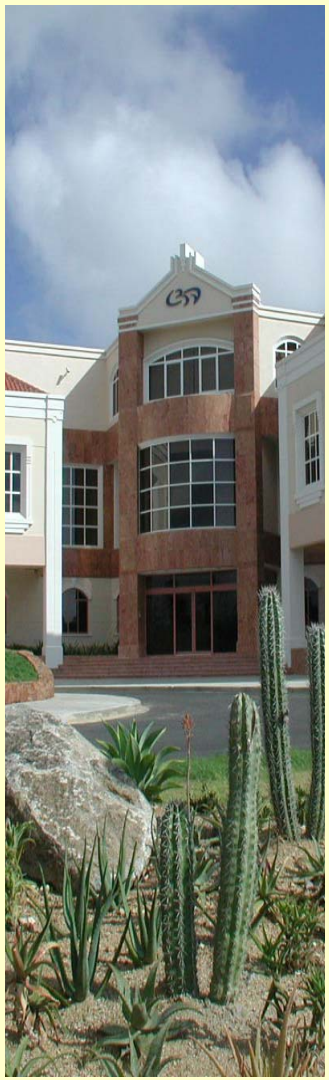
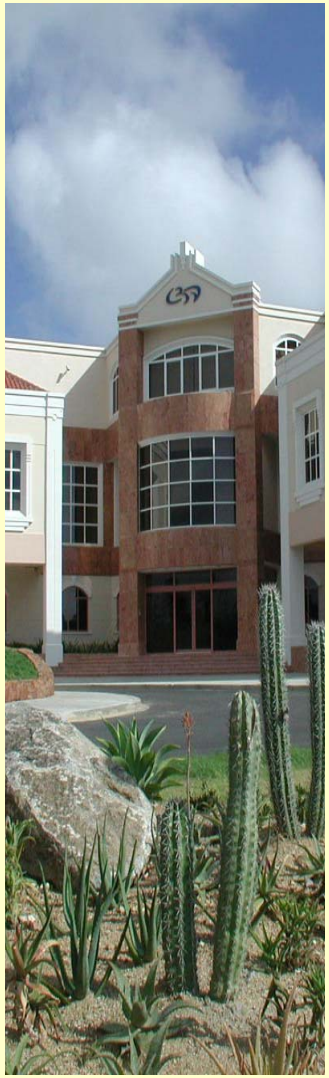


Highlights New AML/CFT Legislation

George Croes

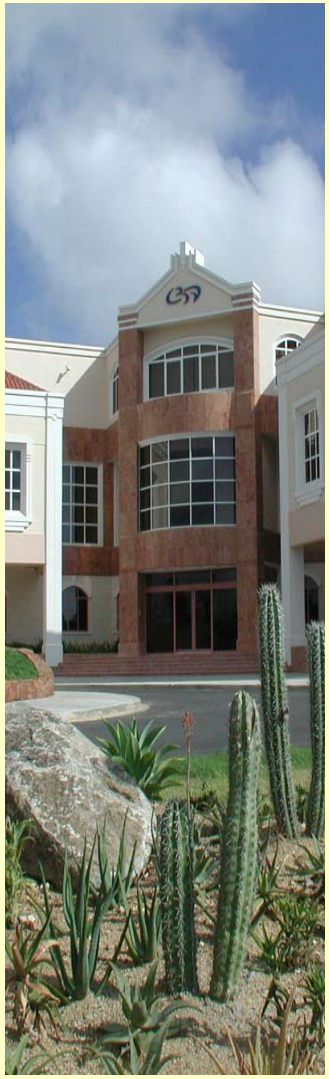
Senior Policy Advisor Integrity and International Affairs

Contents presentation



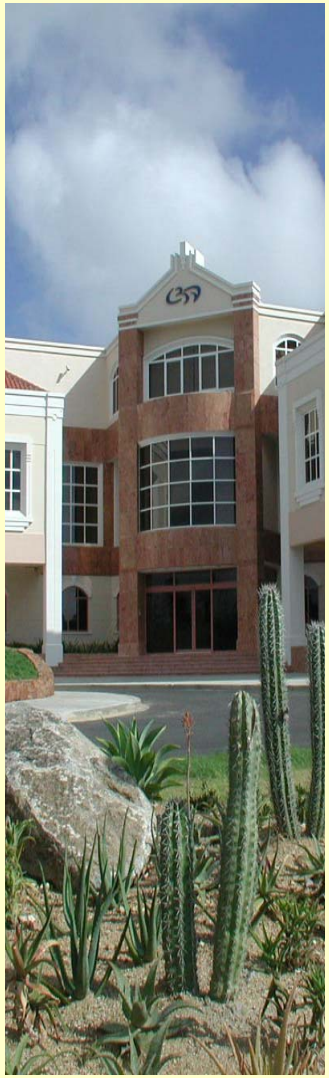
I. Introduction
II. Current AML/CFT Legal Framework of Aruba
III. Main Characteristics SOIPS (LID) and SORUT (LMOT)
IV. Evaluation of SOIPS and SORUT
V. Introduction Highlights New AML/CFT Legislation
VI. Highlights New AML/CFT State Ordinance
VII. Customer Due Diligence
VIII. Reporting of unusual transactions to the MOT
IX. Record Keeping
X. Supervision and Enforcement
XI. Procedures and Measures
XII. Implementation

I. INTRODUCTION



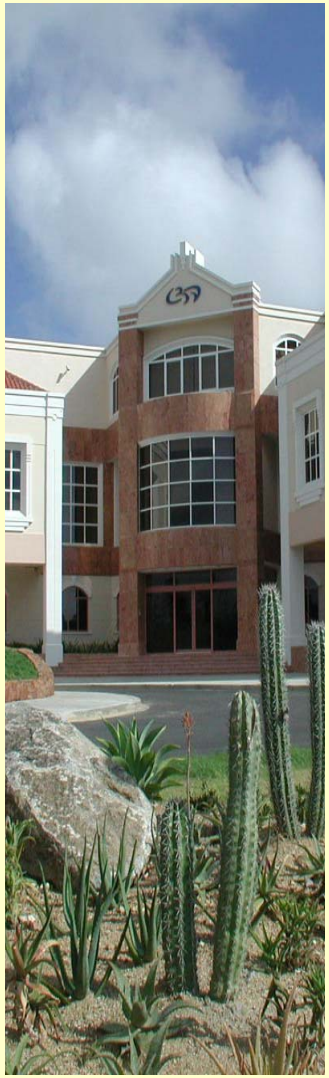
- Since the 1990's countries and jurisdictions are required to have systems in place for the prevention and combat of money laundering and terrorist financing. Such systems are usually referred to as AML/CFT systems (anti-money laundering and combating the financing of terrorism).
- The global standard for effective AML/CFT systems is set by the Financial Action Task Force (FATF) through its 40 + 9 Recommendations.
- The 40 + 9 FATF Recommendations have regard to:
  - (i) Legal systems
  - (ii) Preventive measures to be taken by financial institutions and non-financial businesses and professions
  - (iii) Institutional and other measures
  - (iv) International cooperation
  - (v) Special Recommendations (9) on Terrorist Financing
- For an exhaustive overview please refer to www.fatf-gafi.org.

II. Current AML/CFT Legal Framework



- State Ordinance on Identification when Providing Services (*Landsverordening identificatie bij dienstverlening*), henceforth referred to as SOIPS.
- The State Ordinance on the Reporting Obligation Unusual Transactions (*Landsverordening meldplicht ongebruikelijke transacties*), henceforth referred to as SORUT.
- Both state ordinances are implemented further in secondary legislation such as the ministerial indicator regulations
- Articles 430b, 430c and 430d of the Penal Code (*Wetboek van Strafrecht van Aruba*) which criminalize money laundering.
- Article 140a of the Penal Code which criminalizes terrorist financing.
- The Sanctions State Ordinance 2006 (*Sanctieverordening 2006*) and the Sanctions State Decree Combat Terrorism and Terrorist Financing (*Sanctiebesluit bestrijding terrorisme en terrorismefinanciering*).
- The various AML/CFT-oriented directives issued by the CBA to the supervised entities pursuant to the regulatory state ordinances.

III. Main Characteristics SOIPS and SORUT



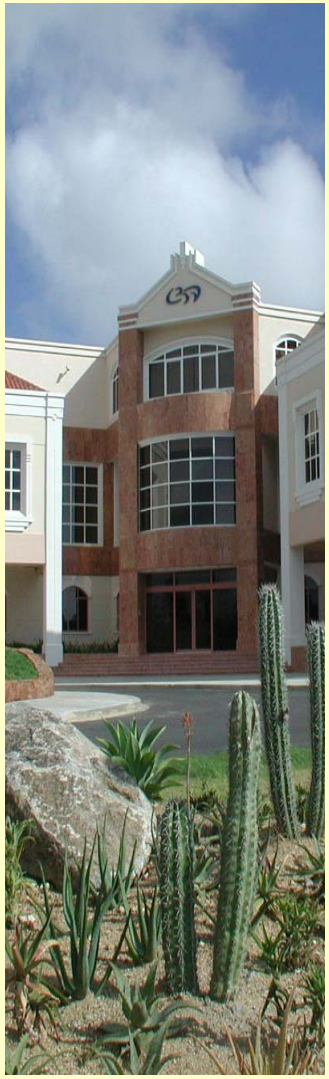
The main characteristics of the SOIPS are:

(i) CDD/KYC provisions based on the identification of customers prior to the provision of a requested financial service as defined in article 1 of the SOIPS;

(ii) Applicable to the financial institutions and non-financial businesses and professions as described in article 1 of the SOIPS (e.g. credit institutions, life insurers, MTCs, lawyers, notaries, high value goods dealers and jewelers);

(iii) Since February 5, 2009, also possible to impose administrative fines and penalty charge orders to a maximum of Afl. 250.000,- per infraction.

III. Main Characteristics SOIPS and SORUT (cont'd)



The main characteristics of the SORUT are:

(i) Contains a reporting system for financial institutions and non-financial businesses and professions based on unusual transactions;

(ii) Institutes the MOT (Meldpunt Ongebruikelijke Transacties) as the Aruban center for the receipt, analysis and dissemination of unusual transactions;

(iii) Special powers granted to the MOT such as power to request additional information (*bevraging*);

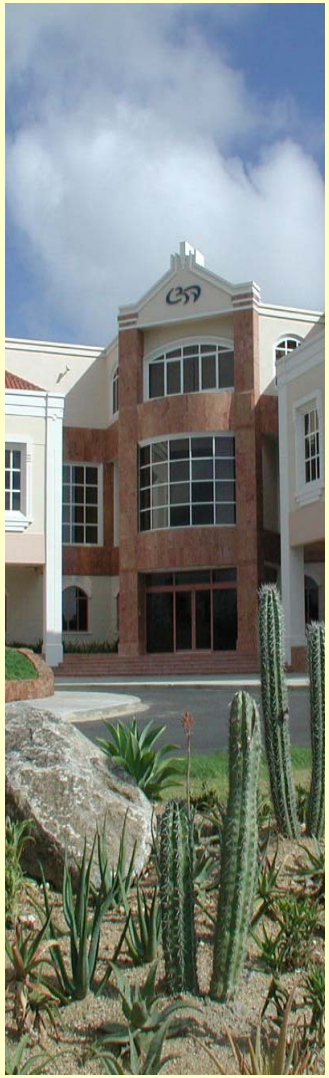
(iv) Civil and criminal indemnity provisions for reporters and their personnel;

(v) Since July 1, 2010 compliance supervision with respect to financial institutions conducted by the CBA and with respect to other service providers by the MOT;

(vi) Since February 5, 2009 same administrative sanctioning possibilities as with SOIPS;

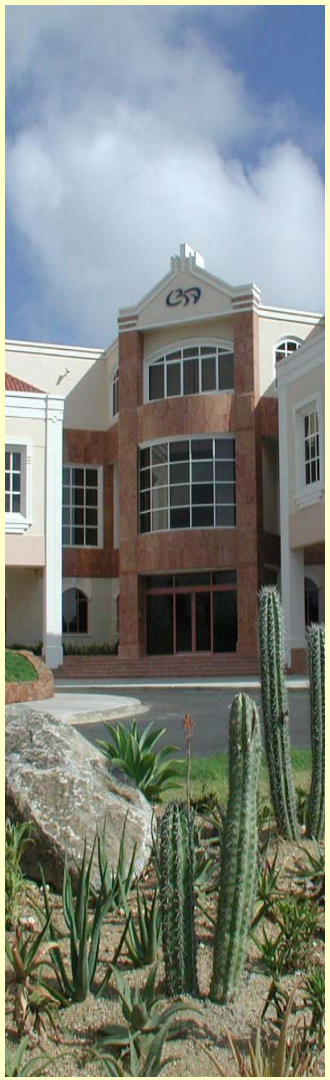
(vii) Indicators for the reporting of unusual transactions to the MOT set out in the ministerial indicator regulations (currently 5).

IV. Evaluation of the SOIPS and SORUT



- The SOIPS and SORUT and their subsequent secondary legislation have been in force since February 1996 and have undergone many changes, mainly as a consequence of the changes in the international standards, such as the FATF 40 + 9 Recommendations.
- In 2008-2009 the SOIPS and SORUT underwent an in-depth review by the FATF as part of the third mutual evaluation of Aruba's AML/CFT system.
- As for the SOIPS and SORUT, the following deficiencies were noted:
  (i) The scope of the SOIPS and SORUT is not harmonized as each state ordinance has its own, divergent definition of financial and non-financial services;
  (ii) Certain categories of financial services providers, such as investment businesses (including stock exchanges) and life insurance brokers are not covered by the SOIPS and SORUT;

IV. Evaluation of the SOIPS and SORUT (cont'd)



(iii) CDD requirements for supervised financial institutions are spread over the SOIPS and the various AML/CFT Directives of the CBA, which carries the risk of contradiction;

(iv) Absent or inadequate provisions in SOIPS regarding ultimate beneficial ownership, enhanced due diligence for high risk customers (such as PEPs), and ongoing monitoring of businesses and relations;

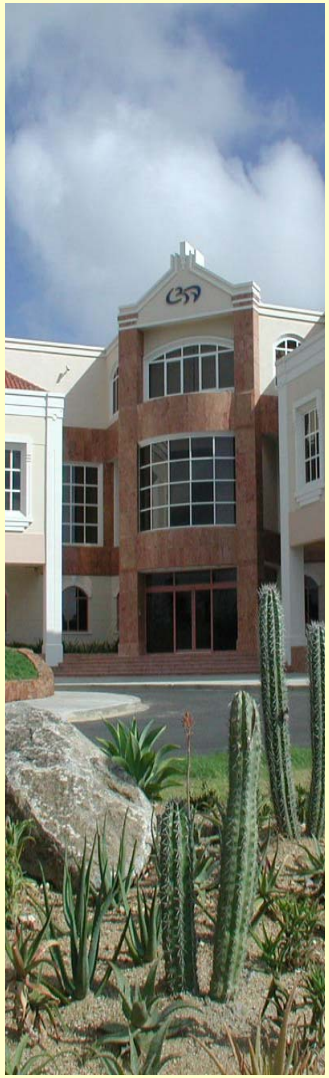
(v) As for SORUT, not all predicate offences covered by the reporting obligation;

(vi) Lack of indicators for certain financial services, *de facto* excluding these from the reporting obligation;

(vii) The role and composition of the Advisory Committee (*Begeleidingscommissie*) appears to compromise the autonomy of the MOT;

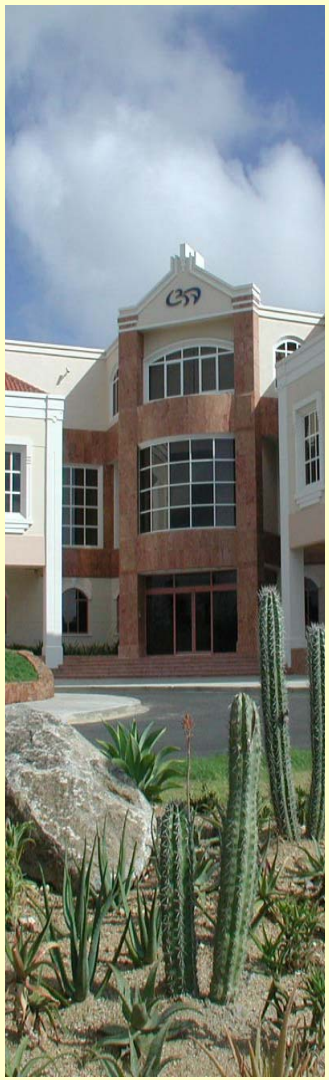
(viii) Both SOIPS and SORUT: sanctions not proportionate, effective and dissuasive according to standards.

V. Introduction Highlights New AML/CFT Legislation



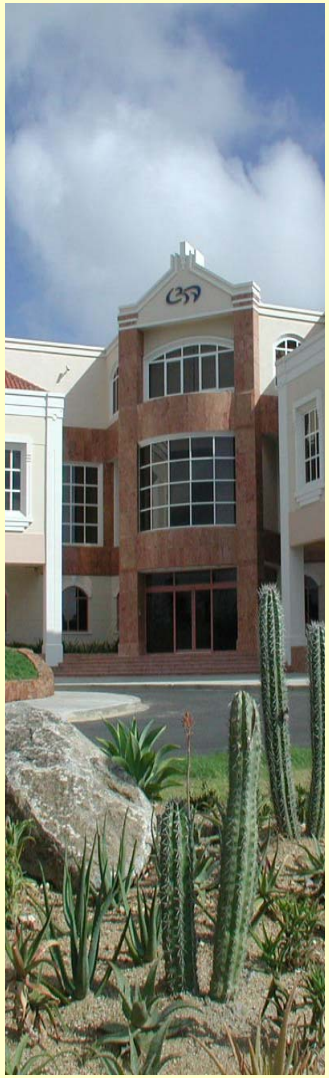
- After the adoption of the MER, the Government of Aruba began working swiftly on improving the AML/CFT system of Aruba in accordance with the FATF 40 + 9 Recommendations.
- As for the legal framework for Customer Due Diligence (CDD) and the reporting of unusual transactions by financial institutions and non-financial businesses and professions, a new and comprehensive state ordinance will replace the SOIPS and SORUT.
- The new state ordinance will be named *Landsverordening voorkoming en bestrijding witwassen en terrorismefinanciering* (State Ordinance Prevention and Combat of Money Laundering and Terrorist Financing), henceforth referred to as the AML/CFT State Ordinance
- The AML/CFT State Ordinance is scheduled to enter into force on January 1, 2011.

VI. Highlights New AML/CFT State Ordinance



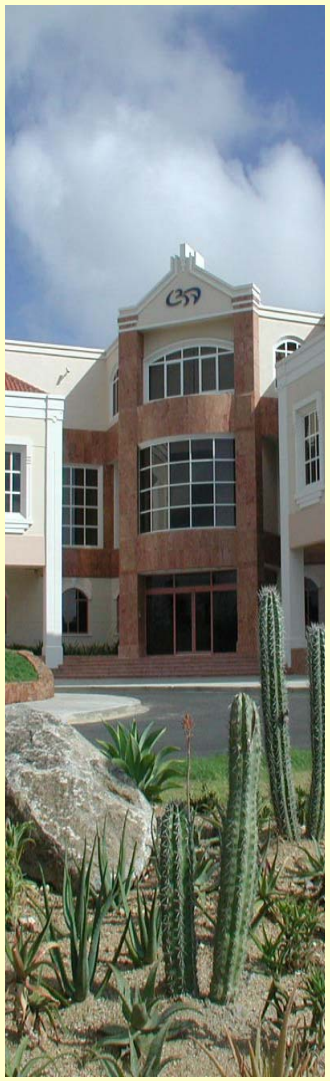
- The AML/CFT State Ordinance will address the following main issues:
  (i) Customer Due Diligence (CDD)
  (ii) The reporting of unusual transactions to the MOT
  (iii) Record Keeping
  (iv) Supervision and Enforcement
  (v) Procedures and Measures
- The basic obligations regarding CDD, the reporting obligation and record keeping will be set out in the AML/CFT State Ordinance using the relevant FATF Recommendations as a benchmark, while additional requirements will be set out in the handbooks to be issued by the CBA pursuant to the AML/CFT State Ordinance
- The scope of the AML/CFT State Ordinance will cover the financial institutions as defined in the FATF standards (regulated and non-regulated by the CBA), as well as the Designated Non-Financial Businesses and Professions (DNFBPs).

VII. Customer Due Diligence: Scope



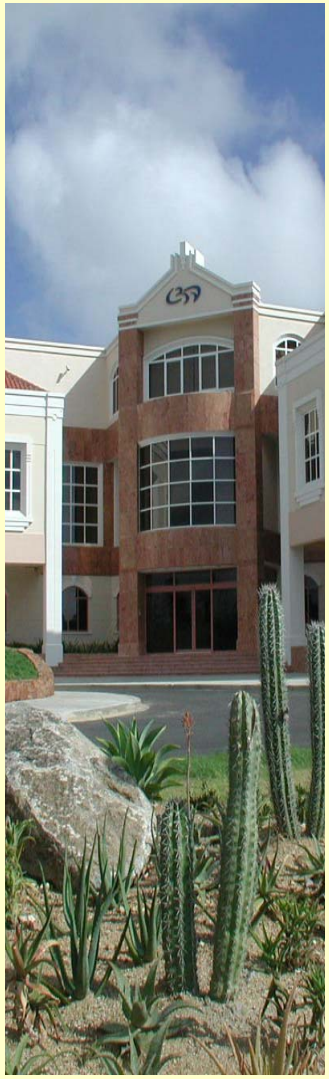
- All service providers (financial institutions and DNFBPs) will be required to carry out CDD that will include the following:
  - (i) Identification of the customer and verification of the identity of that customer;
  - (ii) Identification of the ultimate beneficial owner and carrying out reasonable measures to verify the identity of the ultimate beneficial owner in such a way that the service provider is satisfied with the identity of the ultimate beneficial owner;
  - (iii) Determining the purpose and intended nature of the business relationship;
  - (iv) Ongoing monitoring of the business relationship and of the transactions carried out during the course of the business relationship in order to ensure that these correspond with the knowledge on the customer and the ultimate beneficial owner, their risk profile and, if applicable, an investigation on the source of wealth.

VII. Customer Due Diligence: Scope (cont'd)



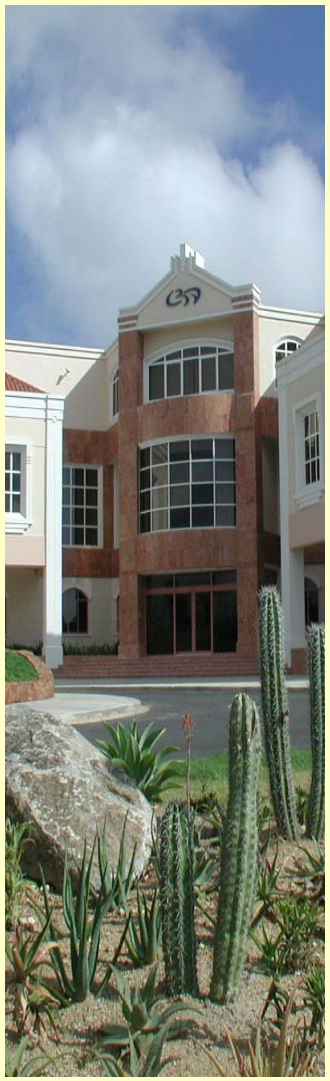
- A service provider shall investigate if a natural person appearing before him is acting for himself or for a third party;
- If a service provider knows or should reasonably suspects that a natural person appearing before him is acting for a third party, he must take reasonable measures to determine the identity of that third party and verify that identity;
- If the client is a legal person, the reasonable measures meant above must enable the service provider to understand the ownership and actual control structure of the client and to establish the natural person or persons who have ultimate ownership and control of the legal person;
- If a natural person appears on behalf of a client, the service provider shall identify that person and verify that identity prior to the provision of the service;
- If a client is a legal person, the service provider shall establish if the natural person acting on its behalf is so authorized and shall record the data on the client's legal structure and proxy.

VII. Customer Due Diligence: when required



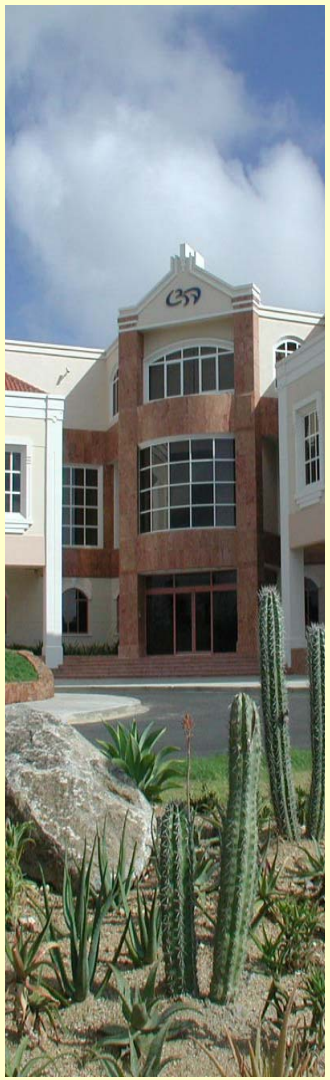
- Financial institutions will be required to perform CDD in the following cases:
  - (i) when establishing a business relationship;
  - (ii) when carrying out occasional transactions for a client above Afl. 25,000.00;
  - (iii) when carrying out money transfers as meant in the SOSMTC;
  - (iv) when there are indications that the client is involved in money laundering or terrorist financing;
  - (v) if there are doubts about the veracity or reliability of previously acquired data on the client;
  - (vi) if the risk of an existing client's involvement with money laundering or terrorist financing gives rise to such.

VII. Customer Due Diligence: when required (cont'd)



- DNFBPs will be required to perform CDD in the following cases:
  - (i) lawyers, notaries, accountants and tax advisors, when performing the following activities (*inter alia*):
    - buying and selling of real estate;
    - managing client money, securities or other assets;
    - organizing contributions for the creation, operation and management of companies
    - creation, operation and management of entities and buying and selling of business entities;
  - (ii) real estate agents, when mediating in the buying and selling or real estate (including rights on such real estate);
  - (iii) Casinos, when their customers engage in cash transactions equal to or above Afl. 5000.00

VII. Customer Due Diligence: when required (cont'd)



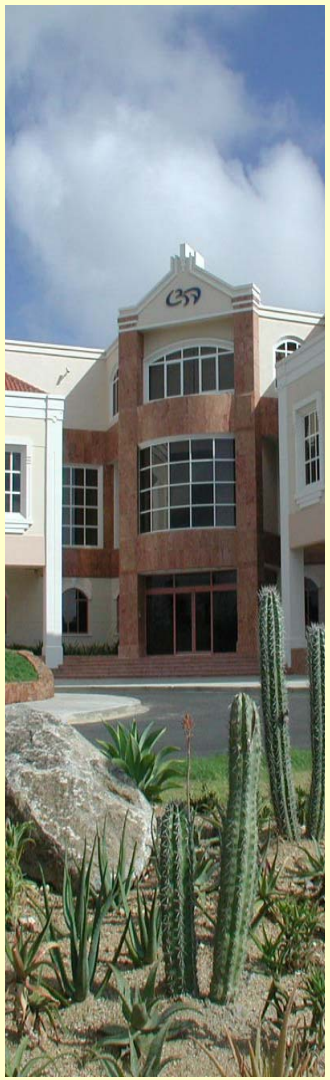
(iv) TCSPs (*trustkantoren*), for almost all of their activities;

(v) Dealers in precious metals, dealers in precious stones and jewelers, when they engage in any cash transaction with a customer equal to or above Afl. 25,000.00;

(vi) when any of the circumstances, set out in (iv) through (vi) for the financial institutions occur.

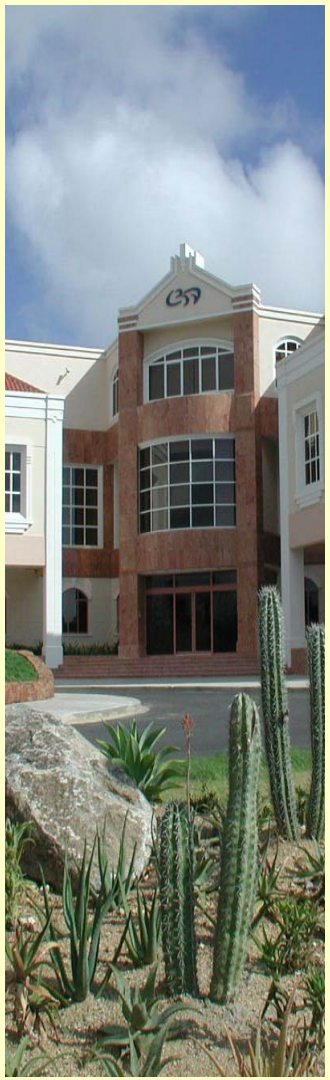
- All service providers will be required to adjust the CDD to the risk sensitivity for money laundering and terrorist financing to the type of client, business relationship, product or transaction and to draw up a risk profile of the customer and the ultimate beneficiary owner.
- Specific rules will be made for CDD when conducting wire transfers with emphasis on gathering and passing on of originator information.
- Data and other information collected during the CDD process must be kept up to date and relevant.

VII. Customer Due Diligence: when required (cont'd)



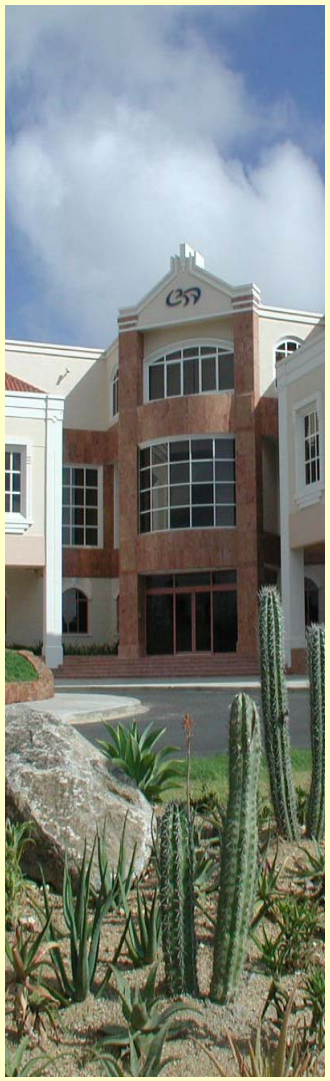
- CDD must be applied before entering into the business relationship or carrying out the transaction (special exceptions apply).
- A service provider shall be prohibited to enter into a business relationship or carry out a transaction, if he has not performed CDD, if he is unable to perform CDD or if the CDD has not led to the intended result.
- If after entering into a business relationship, a service provider is not able to identify the customer and verify the identity, the service provider must terminate the business relationship promptly.

VII. Customer Due Diligence: Enhanced CDD



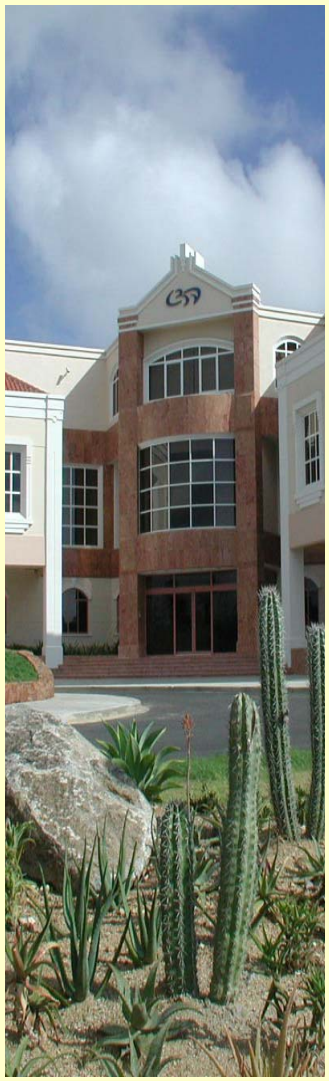
- Enhanced due diligence will be required for categories of customers, business relationships or transactions that pose a higher risk of money laundering or terrorist financing. Examples of these are:
  - (i) Non-resident customers;
  - (ii) Private banking;
  - (iii) Legal persons and arrangments such as trusts that are personal assets holding vehicles
  - (iv) Companies that have nominee shareholders or shares in bearer form;
  - (v) Politically Exposed Persons (foreign and domestic);
  - (vi) Persons and entities from jurisdictions with questionable reputations.
  - (vii) correspondent banking
- Service providers will be required to have risk-based procedures with regard to business relationships and transactions with Politically Exposed Persons (PEPs).

VII. Customer Due Diligence: Enhanced CDD (cont'd)



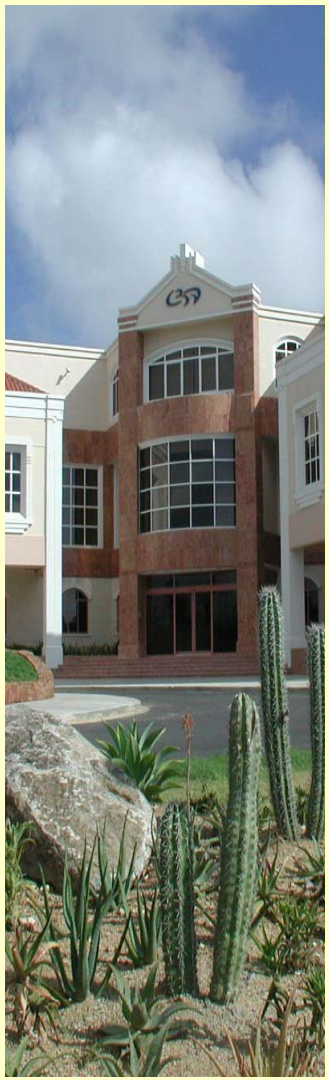
- Service providers will be required to pay special attention to:
  - (i) business relationships and transactions with persons from countries that do not or insufficiently apply the international standards on AML/CFT;
  - (ii) all complex and unusually large transactions and all unusual features of transactions which have no apparent economic or legal purpose.
- In case of a transaction with a person as meant in (i) or a transaction meant in (ii) the service provider shall investigate the background and purpose of that transaction and record his findings in writing.

VII. Customer Due Diligence: Reduced CDD



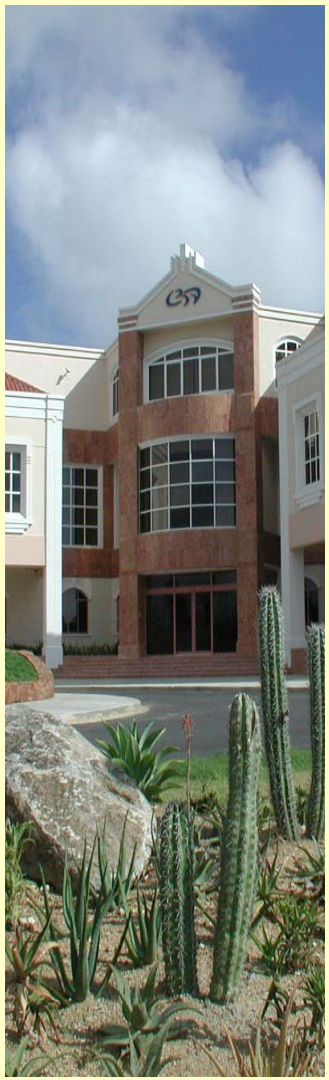
- Reduced CDD will be allowed under certain circumstances, such as:
  - (i) Aruban entities supervised by the CBA;
  - (ii) Public companies that are subject to regulatory disclosure requirements;
  - (iii) Aruban Government-owned companies;
  - (iv) The Government of Aruba (*Land Aruba*) and public entities instituted by law and established in Aruba;
  - (v) Public entities instituted by law in other parts of the Kingdom of the Netherlands;
  - (vi) Life insurance policies where the annual premium does not exceed Afl. 1500.00 or the single premium does not exceed Afl. 4000.00;
  - (vii) A pension scheme or similar arrangement that provides retirement benefits to employees, where the contribution is made through deduction from wages and the scheme does not permit assignment of a participant's interest.
- Service providers must collect sufficient information in order to determine if reduced CDD can be applied.

VII. Customer Due Diligence: other issues



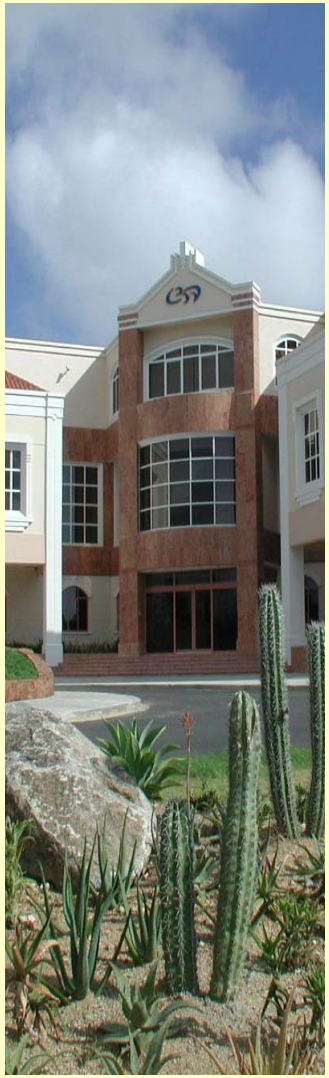
- Service providers will be permitted to rely on intermediaries or other third parties to perform some of the elements of the CDD process or to introduce business, provided certain criteria are met. These include the adequate collection of information from the third party concerning certain elements of the CDD process. The ultimate responsibility will always remain with the service provider.
- When engaging in cross-border correspondent banking relationships, banks should gather sufficient information on the correspondent bank such as its activities, the nature and quality of supervision and the AML/CFT procedures in place.
- Correspondent relationships with shell banks will be prohibited explicitly.
- Verification documents:
  (i) for natural persons and Aruban legal persona: documents, information or data from a reliable and independent source;
  (ii) for foreign legal persons: reliable and internationally accepted documents, information or data.

VIII. The reporting of unusual transactions to the MOT



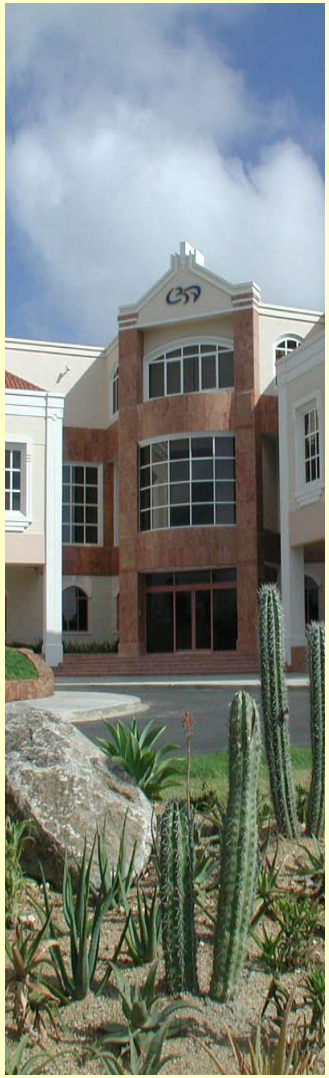
- The present system of unusual transactions reporting will be kept, albeit with certain modifications:
  - (i) The MOT will concentrate on its core activities which are the receipt, analysis and dissemination of unusual transactions;
  - (ii) The Advisory Committee (*Begeleidingscommissie*) will focus on assisting the MOT with expertise and advise;
  - (iii) More emphasis will placed on the reporting of unusual transactions using subjective indicators;
  - (iv) The MOT will be able to exchange information with foreign FIUs without a prior MOU;
  - (v) Authorities in charge with regulation and oversight of financial institutions and DNFBPs will be required to report to the MOT facts discovered during the execution of their duties which might indicate money laundering and terrorist financing.

IX. Record Keeping



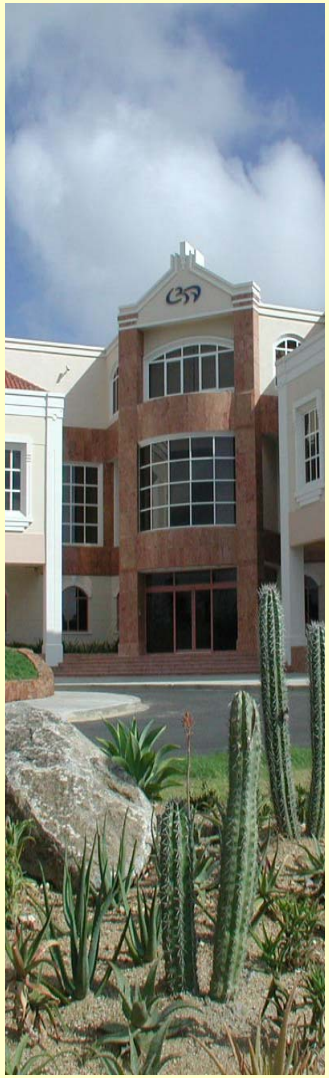
- Record keeping will focus on necessity to permit reconstruction of individual transactions so as to provide, if necessary, evidence for law enforcement authorities.
- Records will include identification data, account files and business correspondence.
- CDD records must be kept for at least 10 years following the termination of a business relationship or the execution of the individual transaction.
- UTR records must be kept for at least 10 years after the date of the filing of the report.
- If necessary, the CBA may set longer record keeping terms.

X. Supervision and Enforcement



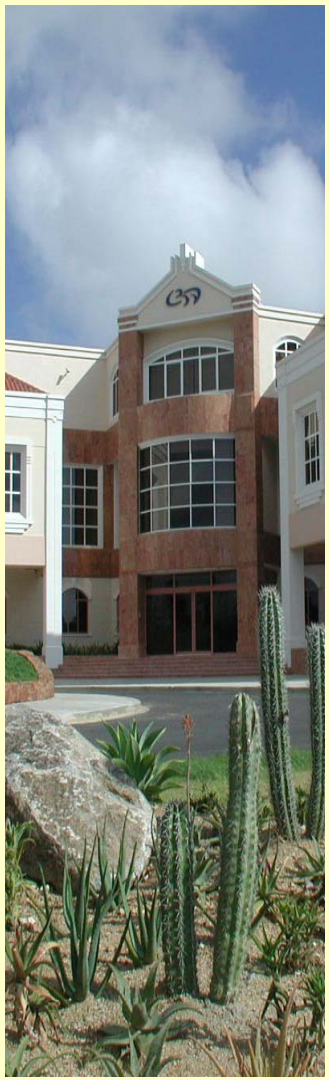
- The CBA will supervise compliance by the service providers (including DNFBPs) with the provisions of the AML/CFT State Ordinance.
- The AML/CFT State Ordinance will continue the sanctions regimes of the SOIPS and the SORUT (the penalty charge order and administrative fine), albeit with some modifications:
  - (i) the CBA will be the sole authority in charge of imposing administrative sanctions;
  - (ii) the maximum amounts of the penalty charge order and the administrative fine will be increased substantially;
  - (iii) senior management officials will also be liable for administrative sanctioning;
  - (iv) criminal sanctions will also be increased substantially.
- The MOT will be able to exchange FIU-related information with other FIUs without a prior MOU.
- The CBA as the supervisor will be able to exchange information with other supervisors on CDD and UTR/STR matters.

XI. Procedures and Measures

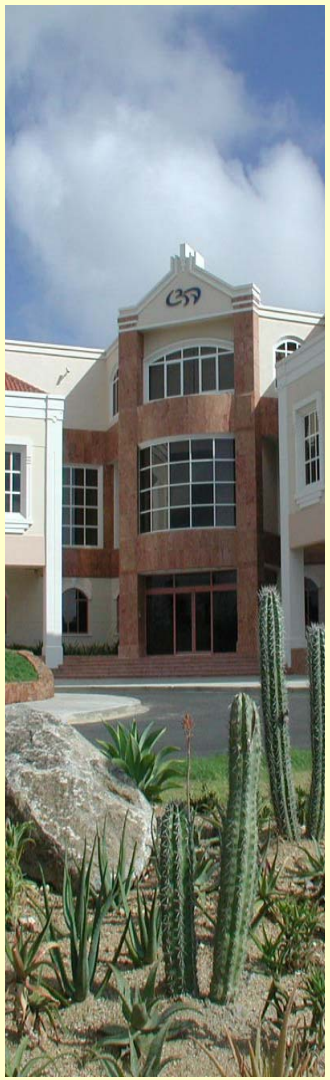


- Service providers will be required to have written procedures in place for the prevention and combat of money laundering and terrorist financing, e.g. on the internal organization, relevant staff, the application of CDD, the reporting of UTRs, record keeping.
- Service providers will be required to periodically evaluate these procedures and measures on their effectiveness.
- The AML/CFT State Ordinance will require the presence of a Money Laundering Reporting Officer (MLRO) and Money Laundering Compliance Officer (MLCO) with each service provider.
- The AML/CFT State Ordinance will require the regular training of staff on AML/CFT issues.
- The AML/CFT State Ordinance will require regular business risk assessments by service providers.
- The CBA will issue directives in the form of handbooks to the various categories of service providers.

XII. Implementation



- The introduction of the AML/CFT State Ordinance will be accompanied by a separate state ordinance that will bring other existing state ordinances (such as the regulatory state ordinances for financial institutions) in line with the content and purpose of the AML/CFT State Ordinance and will contain transitional provisions for the existing service providers.
- Effective date: January 1, 2011



Thank you