Handbook for the prevention and detection of money laundering and financing of terrorism for service providers (financial and designated non-financial)

the Central Bank of Aruba

Version 1.1

COMING INTO FORCE 1 JANUARY 2020

Table of Contents

1. Glossary

In the context of this Handbook the below abbreviations and references have the following meanings. Additionally, reference is made to the definitions contained in Article 1 of the AML/CFT State Ordinance.

AML	Anti-money laundering
CFT	Combatting the financing of terrorism
Amending State Ordinance	State Ordinance amending the Sectoral Supervisory State Ordinances (*Landsverordening herziening sectorale toezichtswetgeving*)
AML/CFT State Ordinance	State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (*Landsverordening voorkoming en bestrijding witwassen en terrorismefinanciering*, AB 2011, no. 28)
AML/CFT Laws and Regulations	AML/CFT State Ordinance, State Decree Regulation Wire Transfers (*Landsbesluit regeling geldelijke overmakingen*, AB 2011, no. 30), Sanctions State Ordinance (*Sanctieverordening 2006*, AB 2007, no. 27), Sanctions State Decree Combating Terrorism and Financing of Terrorism (*Sanctiebesluit bestrijding terrorisme en terrorismefinanciering*, AB 2010, no. 27) and related laws and regulations in the area of AML/CFT
Board	The Executive Board and insofar applicable also the Supervisory Board of a service provider
CBA	Centrale Bank van Aruba
CBCS	Centrale Bank van Curaçao en Sint Maarten
CDD	Customer due diligence
DNB	De Nederlandsche Bank
EDD	Enhanced due diligence
Enactment State Ordinance	Enactment Ordinance State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (*Invoeringsverordening Landsverordening voorkoming en bestrijding witwassen en terrorismefinanciering*, AB 2011, no. 29)
Express trust	A (Anglo-Saxon) trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangement (e.g. constructive trust)
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force
FATF Recommendations	The FATF Forty Recommendations
FIU	Financial Intelligence Unit (Reporting Center Unusual Transactions, referred to in Article 20, paragraph 1, of the AML/CFT State Ordinance)
Guidance notes	Ways of complying with the Statutory requirements or Regulatory requirements presented in this Handbook
Handbook	Handbook for the prevention and detection of money laundering and combating the financing of terrorism for service providers by the Centrale Bank van Aruba
IMF	International Monetary Fund
ML/TF	Money laundering and terrorism financing
MLCO	Money laundering compliance officer as meant in Article 47, paragraph 1, of the AML/CFT State Ordinance
MLRO	Money laundering reporting officer as meant in Article 47, paragraph 2, of the AML/CFT State Ordinance
OFAC	Office of Foreign Assets Control of the US Department of the Treasury

PEP	Politically-exposed person as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance
Regulatory requirements	Directives issued by the CBA that service providers must comply with
SDD	Simplified due diligence
Senior management	An officer or employee with sufficient knowledge of the service provider's money laundering and terrorist financing risk exposure and sufficient seniority and authority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors
Service provider	A financial service provider or designated non-financial service provider as defined in Article 1, paragraph 1, of the AML/CFT State Ordinance
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 particular funds or other assets which are the subject of the business relationship between the client and the service provider (e.g., the amounts being invested, deposited, or wired as part of the business relationship).
Source of wealth	The origin of a person's entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the person would be expected to have, and a picture of how the persons acquired such wealth.
Statutory requirements	Requirements as set by or by virtue of the AML/CFT State Ordinance
Supervisory laws	SOSCS, SOSIB, SOSMTC and SOSTSP
UBO	Ultimate beneficial owner
UN	United Nations
US	United States

2. Introduction

The laundering of criminal proceeds, the financing of terrorism and the financing of the proliferation of weapons of mass destruction through the worldwide financial and business systems is vital to the success of criminal and terrorist operations. To this end, criminals and terrorists seek to exploit the facilities of the world's businesses in order to benefit from such proceeds or financing. Increased integration of the world's financial systems has enhanced the ease with which criminal proceeds can be laundered or terrorist funds transferred and have added to the complexity of audit trails.

Aruba has a strong commitment at political, government and industry level to play an active role in the international fight against ML/TF. Accordingly, the authorities of Aruba take a strong position against any business that assists in ML/TF, whether it acts with knowledge or suspicion of the connection to crime or without proper regard to what it may be facilitating through the provision of its products or services.

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

Each service provider must recognize the role that it must play in protecting itself, and its employees, from involvement in ML/TF, and also in protecting Aruba's reputation of probity.

The CBA strongly believes that the key to the ML/TF prevention and detection lies in the implementation of, and strict adherence to, effective systems and controls, including sound CDD procedures based on international standards. This Handbook therefore sets standards which are aligned with international standards issued by the FATF. The Handbook also has regard to the standards promoted by the Basel Committee on Banking Supervision and the International Association of Insurance Supervisors. The Handbook takes account of the requirements of EU AML/CFT legislation, and the application of standards set by the FATF. The Handbook also addresses compliance with the UN- and EU-sanctions regimes as implemented in the Aruban legislative framework.

Where in this Handbook reference is made to money laundering and terrorism financing, or ML/TF, this is taken to also include and refer to proliferation financing. Proliferation involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programs. Proliferation financing will be further addressed in the Chapters on business risk assessment (Chapter 3.3.3) and Sanctions (Chapter 11.1.2).

2.1 Objectives of the Handbook

This Handbook will assist service providers in complying with the requirements of the AML/CFT Laws and Regulations, financial crime and related offences to prevent Aruba's financial system and operations from being abused for ML/TF.

The objectives of the Handbook are as follows:

- to outline the requirements of the AML/CFT State Ordinance and related legislation;
- to outline the requirements of the AML/CFT State Ordinance which introduces additional obligations for those remitting or receiving fund transfers;
- to outline the requirements of the Sanctions State Decrees and related regulations;
- to set out the CBA's requirements to be followed by all service providers (the Regulatory requirements);
- to assist a service provider to comply with the requirements of the legislation described above (the Statutory requirements) and the CBA's requirements through practical interpretation;
- to provide a base from which service providers can design, tailor and implement their own AML/CFT policies, procedures and measures;
- to ensure that Aruba meets international AML/CFT standards;

- to emphasize the responsibilities of the Board and senior management of the service provider;
- to promote the use of a proportionate risk-based approach to CDD measures, which puts emphasis on an increased allocation of resources towards high risk customers;
- to provide practical guidance on CDD, SDD and EDD; and
- to emphasize the particular ML/TF risks of certain financial services and products.

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

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

The handbook is based on section 48 AML/CFT State Ordinance or "LWTF": the CBA may issue directives and shall provide information regarding the application of Chapters 2, 3, 4 and 6 of the LWTF.

2.2 Structure of the Handbook

The Handbook is structured in a three level approach.

1. **Statutory requirements:** describing the statutory requirements set out in the AML/CFT State Ordinance that apply to service providers.
2. **Regulatory requirements:** providing directives of the CBA regarding the application of the AML/CFT State Ordinance that apply to service providers.
3. **Guidance notes:** presenting ways to comply with the Statutory and Regulatory requirements. The Guidance notes must always be read in conjunction with the requirements.

The Statutory requirements as described in this Handbook often paraphrase the provisions contained in the AML/CFT State Ordinance. Depending on the subject, these can be articles, sections of articles or a combination of articles or sections of articles of the AML/CFT State Ordinance. This should always be read and understood in conjunction with the full text of the AML/CFT State Ordinance (in the Dutch language) and, where applicable, other AML/CFT Laws and Regulations (in the Dutch language). The Statutory requirements are presented in italics.

In the Guidance notes, the Statutory and Regulatory requirements are often repeated or paraphrased. These Notes are further elaborated with examples and additional guidance on how the requirements may be implemented.

These examples in the Guidance notes are intended as guidelines. In a risk-based approach, a service provider may adopt other appropriate and effective measures to those set out in the Guidance notes, including policies, procedures and measures established by the group, so long as it can demonstrate that such measures also achieve compliance with the Statutory and Regulatory requirements. This allows a service provider some discretion as to how to satisfy the requirements. This often depends on the nature and size of the service provider and the types of clients, services, products and transactions. Ultimately, it is the result that the service provider needs to achieve: compliance with the requirements. The manner in which this is done is largely up to the service provider. The result must, however, be demonstrated and documented. If the service provider cannot show that the result is achieved or if a result is not documented, it will be difficult for the service provider to proof that a requirement is indeed satisfied. **The CBA takes the approach that "not documented is considered as not executed".**

"Nature and size" of the service provider involves a combination of factors; not only the size of the service provider by number of employees, but also, for example, by the volume of assets, number of clients, number of foreign or high risk clients and types of products. A service provider with two employees, but with mainly high risk clients, for example, will have to implement stricter compliance, while that is not the case for a similar service provider with only low risk clients.

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

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

2.3 Legal status and sanctions for non-compliance

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

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

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

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

Moreover, the Supervisory Laws set out obligations for certain service providers regulated by the CBA regarding sound and controlled business operations, more specifically to pursue adequate policies and to have procedures and measures in place to, inter alia, ensure compliance with the AML/CFT Laws and Regulations.

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

- a directive (aanwijzing);
- a penalty charge order (last onder dwangsom);
- an administrative fine (bestuurlijke boete);
- publication of a directive, a penalty charge order or an administrative fine (publicatie);
- silent receivership (stille curatele);
- revocation of the license or removal from the registry (intrekking of doorhaling);
- criminal prosecution (strafrechtelijke vervolging).

The AML/CFT State Ordinance and the Supervisory Laws state that violations can be committed by natural persons and legal persons. Article 53, paragraph 1 and 2, of the Criminal Code of Aruba applies mutatis mutandis. This means that violations by a legal entity may be attributed to the individuals who ordered the act constituting the violation or who were “de facto in charge” at the time when the violation occurred.

2.4 Scope of the Handbook

The AML/CFT State Ordinance applies to many categories of persons carrying on business in or from Aruba. Therefore, this Handbook is applicable to all service providers that are covered in the AML/CFT State Ordinance. This includes Aruban-based branches of companies incorporated outside Aruba conducting business in or from Aruba.

The general part of this Handbook (Chapters 1-11) is relevant for all service providers. Chapter 12 of this Handbook provides relevant specific risk factors per sector.

Board and senior management
This Handbook addresses in several instances the Board and/or senior management as responsible for the implementation of specific requirements. Service providers that are a body corporate must have a Board. In case of smaller service providers or when a service provider is a partnership or a branch, there may not always be a Board. In the absence of a Board, senior management is held responsible. Senior management here means an officer or employee with sufficient knowledge of the service provider's money laundering and terrorist financing risk exposure and sufficient seniority and authority to take decisions affecting its risk exposure.

3. Corporate Governance, Risk Assessment and Risk Management

3.1 Introduction

Corporate governance is the system by which businesses are directed and controlled. The responsibilities of the Board/senior management include setting strategic objectives, providing the leadership to put them into effect and supervising the management of the business. This chapter describes a service provider's general framework for adequate corporate governance and risk management systems to combat ML/TF, including:

- an ethical culture;
- conducting a business risk assessment;
- risk management systems, policies, procedures and measures,
- appointing a MLCO and MLRO;
- group compliance; and
- outsourcing.

3.2 An ethical culture

3.2.1 Regulatory requirements

- The Board/senior management must ensure an ethical corporate culture and lead accordingly by example and actions ('tone and behavior at the top').

- The Board/senior management must actively promote a culture of compliance, risk and compliance awareness and the importance of AML/CFT compliance and encourage ethical behavior.

- The Board/senior management must ensure that the service provider's remuneration policy does not negatively impact the ethical corporate culture or compromises the operation of effective AML/CFT policies, procedures and measures.

- The Board/senior management must consider what barriers, including cultural barriers, exist to prevent the operation of effective AML/CFT policies, procedures and measures, and must take effective and adequate measures to potential barriers.

3.2.2 Guidance notes

An ethical business culture and ethical conduct are vital to the effectiveness of integrity control measures. Ethical conduct is a professional, individual responsibility in which the individual is aware and takes proper account of the rights, interests and wishes of other stakeholders, displays an open and transparent attitude, and is willing to take responsibility and render account for his or her decisions made and actions taken. An ethical culture denotes a climate and atmosphere in which a service provider behaves or acts, including in a broader sense, in a way that it can explain and account for – not just according to the letter of the law, but also in the spirit of the law.

Culture is an important internal factor to embed ethical conduct. There are different elements a service provider has to consider guaranteeing an ethical business culture and sound business operations and to promote ethical conduct within the organization, such as:

- weighing of interests and acting in a well-balanced manner: recognizing and visibly including all relevant interests;
- acting consistently: acting in line with objectives and choices;
- negotiability: stimulating a positive critical attitude of employees and allowing the discussion of decisions, other opinions, mistakes, and taboos;

- exemplary behavior: tone and behavior at the top, professional integrity, including avoiding (the appearance of) conflicts of interests;
- feasibility: setting realistic targets and removing perverse incentives and temptations;
- transparency: recording and providing information on targets and fundamental choices to all stakeholders;
- enforcement: consequences are attached to noncompliance.

The service provider has to incorporate the various elements in such a way that ethical conduct becomes a natural element of the business culture.

The culture within a service provider might prevent the operation of effective AML/CFT policies, procedures, and measures. Human and organizational and hierarchical factors, such as the inter-relationships between different employees within a service provider, the interrelationships between employees and customers, insufficient room for dissenting opinions, lack of transparent decision making, can result in the creation of damaging barriers. Unlike policies, procedures, and measures, the prevailing culture of an organization is intangible. As a result, its impact can sometimes be difficult to measure.

The risk that cultural barriers might prevent the operation of effective AML/CFT policies, procedures and measures may be minimized by the Board/senior management. The Board/senior management should take into account that the following factors can play a role:

- An assumption on the part of more junior employees that their concerns or suspicions are not taken seriously.
- Negative handling by managerial staff of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions.
- An unwillingness on the part of employees to subject high value (and therefore important) customers to effective CDD checks.
- Pressure applied by management or customer relationship managers outside Aruba upon employees in Aruba to transact without first conducting all relevant CDD.
- Excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management remuneration or bonus schemes are primarily linked to revenue-based targets.
- The familiarity of employees with certain customers resulting in unusual or higher risk activity and transactions within such relationships not being identified and reported as such.
- The inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential ML/TF activity.
- A tendency for line managers to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily.
- A desire on the part of employees to provide a confidential and efficient customer service.
- Non-attendance of senior employees at AML/CFT training sessions due to the mistaken belief that they cannot learn anything new or because they have too many competing or time consuming demands.

3.3 Conducting a business risk assessment

3.3.1 Statutory requirements

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

3.3.2 Regulatory requirements

- The Board/senior management is responsible for managing the service provider effectively and is in the best position to understand and evaluate all potential integrity risks to the service provider.

The Board/senior management must therefore take ownership of, and responsibility for, the periodical evaluation in order to assess if and to what extent the service provider is vulnerable to ML/TF because of its activities and operations (the “business risk assessment”).

- The Board/senior management must conduct a business risk assessment in which it identifies and assesses the ML/TF risks and other integrity risks, taking into account risk factors including those relating to, at a minimum, the customers, countries and/or geographic areas, products, services, transactions and delivery channels.

- The Board/senior management must consider in the business risk assessment the extent of the service provider’s exposure to risks by reference to its organizational structure, its corporate culture, its customers, the jurisdictions with which its customers are connected, its products and services, and how it delivers those products and services.

- The business risk assessment shall be proportionate and tailor-made to the nature and size of the service provider.

- The business risk assessment shall be documented, kept up-to-date (which requires a periodic and documented update of the business risk assessment, typically, at a minimum, every 1 to 2 years and/or following a ‘trigger’ event such as a (serious) compliance incident that has taken place at the service provider) and made available without delay to the CBA upon request.

- Following the business risk assessment, the Board/senior management must also establish a documented AML/CFT strategy in accordance with its business risk assessment. In case of a service provider forming part of a group operating outside Aruba, that strategy must protect both its global reputation and its Aruba business. Hence, an automatic adoption by the service provider of the global and/or regional business risk assessment is unacceptable: explicit attention should always be given to the specifics of Aruba and the Aruban operations of the service provider.

3.3.3 Guidance notes

AML/CFT compliance begins with a risk-based approach to identifying the risks to which a service provider is exposed. The business risk assessment is an integral part of the risk management process. This risk management process includes in short, the following tasks and processes:

1. identifying and analyzing ML/TF and other integrity risks;
2. the management of risks through policies, procedures and systems;
3. monitoring and checking that policies and procedures are actually being implemented and systems are working properly;
4. assessing whether the risks are adequately and effectively controlled;
5. reviewing policy and procedures where necessary;
6. informing employees about risks and revised policies and procedures.

A risk-based approach allows for the Board/senior management to apply its own approach to the policies, procedures and controls of the service provider in particular circumstances, enabling the Board/senior management to differentiate between its customers in a way that matches the risk to its particular business. It also helps to produce a more cost-effective system of risk management and promotes the prioritization of AML/CFT efforts.

It is important to note that various sectors and types of business, whether in terms of products, services, delivery channels or types of customers, can differ significantly. An approach to preventing ML/TF that is appropriate in one sector may be inappropriate in another.

Risk appetite
The determination of the service provider’s risk appetite is an important element in carrying out the business risk assessment, setting out the amount of ML/TF risk it is prepared to accept in pursuing its

strategic objectives. The Board/senior management is responsible for setting the service provider's risk appetite, together with the overall attitude of the service provider to risk-taking. The primary goal of the risk appetite is to define the amount of risk that the service provider is willing to accept in the pursuit of its objectives, as well as outlining the boundaries of its risk taking, beyond which the service provider is not prepared to accept risk.

Identifying the amount of such risk that it is willing to take on is an integral part of the design and implementation of appropriate and effective policies, procedures and controls to manage and mitigate risk. The service provider's risk appetite includes a qualitative statement (for example, detailing those categories of customers or countries that are deemed to pose too great a risk) as well as quantitative statements on the service provider's risk limits, the maximum level of risk that can be accepted.

In developing a risk appetite, the following questions can be posed:

- What kind of clients do we want to accept?
- What kind of clients do we not want to accept?
- Which jurisdictions are we avoiding?
- Which jurisdictions are not acceptable?
- Which percentage of our client base can be high risk?
- Which core services do we want to provide?
- What risks will we treat on a case-by-case basis?

Examples of qualitative risk appetite statements:

- We have no appetite for clients from ultra high risk/sanctioned countries.
- We have no appetite for transactions where a tax benefit is the main driver.
- If after applying control measures to PEPs from high-risk countries there remains an unacceptable residual risk, these clients must be avoided.
- We do not enter into relationships with clients that deal in weapons, products that are made with child labor, or with corporate social responsibility (CSR) unacceptable activities.
- We have no tolerance for the loss of, or unauthorized or accidental disclosure of, customer information.

Business risk assessment

The first step is to identify and analyze the ML/TF and other integrity risks by means of a business risk assessment. This assessment enables the service provider to comply with (legal) requirements in a risk-based manner. To adequately carry out a business risk assessment, a service provider will conduct and document an assessment of its overall exposure to risks 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. A service provider analyses those risks that may expose the service provider to risks such as money laundering, terrorism financing, but also proliferation financing, corruption, violations of sanctions regulations, and tax evasion. With a tailor-made business risk assessment, the service provider can make informed decisions about the risks that the service provider is willing to take and the control measures that have to be taken.

Risks are not static: both internal and external factors can cause the risks for a service provider to change. Mergers, acquisitions, the purchase or sale of a business, the adoption of a new technological solution, the introduction of a new product or service, a restructuring or a change of legal structure are some of the events which can affect both the type and extent of the risks to which the service provider could be exposed. In light of any such changes the business risk assessment should be reviewed to consider whether the risks to the service provider have changed and to ensure that the controls to mitigate those risks remain effective. Other operational changes, for example, a change in employee numbers or a change to the group policies, can all have an impact upon the resources required to effectively manage ML/TF risks.

A service provider therefore carries out a business risk assessment at least annually and whenever there are trigger events. A service provider needs to consider the possible inherent/gross risks that may arise and the different ways in which they can arise when providing its services to its clients, but also when the client base changes, or when legal requirements or business strategies change. The service provider must assess in a clear manner whether the existing controls are adequate and effective. If these are not (fully) sufficient, amendments must be made to close these gaps in the controls.

When assessing the risks, all relevant employees need to be involved. This means that employees who have client contact or handle and assess client documents and transactions, who are aware of all activities and risks, are actively involved. But all members of the Board, (senior) management and the MLRO and MLCO also have an essential role. The MLRO and MLCO have good knowledge of the risks and can guide the process. But management should also have a clear understanding of ML/FT risks. Moreover, the Board/senior management needs to establish the risk appetite. Information about the business risk assessment should be communicated to management in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions. The risk assessment serves as a steering document for management, on the basis of which management must decide on the actions to be taken.

The business risk assessment should be tailored to the nature and size of the service provider. By considering the nature, scale and complexity of the business, the diversity of the operations (including geographical diversity), the volume and size of transactions, and the degree of risk associated with each area of its operations, the service provider can tailor the risk assessment.

Service providers have different risk profiles depending on the type and number of clients that the service provider focuses on and the quantity and type of services that are provided. A service provider with a high risk profile, for example because it mainly focuses on clients with a high inherent risk or provides products with a high risk for ML/TF, will also have to devote extra attention to this in the business risk assessment, for example by developing more risk scenarios, being even more critical about the effectiveness of the control measures, and also to think ‘out of the box’ about possible scenarios.

Preparation and identification of risk
To make a business risk assessment, a number of steps have to be taken. An important step is drawing up an organization overview: a 'photo' of the service provider. This means that over a period of, for example, one or more years, the number and types of clients are analyzed and how often certain transactions have been done or certain services provided. In the organization overview, it is also identified with which countries the clients and the service provider do business and which roles certain employees or third parties have. It is important that the service provider collects quantitative data about the entire customer base, products, transactions and services.

For this the service provider considers questions as:
- What business type 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?
- How many and what type of customers do we have?
- Where do our customers reside or do business?
- How are our customers introduced to us?
- Do we have mainly non-face to face contact with customers?
- Do we provide complex or simple services or products?
- Do we have multiple or single premises?
- Do we rely on any third party or introducers 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?

The more clients of a certain type there are or the extent to which high risk services or products are provided, the greater the likelihood that a risk manifests itself. But risks can also arise with services that are not core business of the service provider. It is important that the service provider collects quantitative

data about or has a very good knowledge of the entire client base, its products, transactions and services and its delivery channels.

The essence of a business risk assessment is to map threats and vulnerabilities with regard to each integrity risk, and to assess, by way of risk scenarios, the likelihood that a scenario will occur and what the consequences may be. A risk scenario is a description how a risk can materialize, or in other words how the service provider can be used for ML/TF or other integrity issues. Risk scenarios describe the threats and vulnerabilities concerning - combinations of - risk factors such as clients, third parties, employees, delivery channels, countries or services.

Assessing the risks of proliferation financing is an explicit part of the business risk assessment. Proliferation involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapon-related programs. Proliferation financing risks will be different per sector and service provider, and even within a service provider depending on the different business units and different products provided. Proliferation financing vulnerabilities exist among others in global commerce, international trade, free-trade zones, and shipping. Where applicable, the service provider includes in its business risk assessment an assessment of clients trading in dual-use and other sensitive goods, especially when these are exported to individuals and entities that are involved in weapons of mass destruction proliferation-related activities, as well as an assessment of products that would facilitate financing of export.

Examples of risk scenarios in which a service provider may be confronted with ML/TF or other integrity issues:

- A service provider runs a risk of being used for money laundering through clients with ownership structures that include offshore entities or trusts.
- A service provider runs a risk of being used for money laundering through clients whose ultimate control is concealed by the use of nominee shareholders.
- A service provider runs a risk of being used for money laundering through loans to customers by unaffiliated third parties.
- A service provider runs a risk of being used for corruption or money laundering through clients whose UBO is a PEP with unexplained wealth.
- A service provider runs a risk of being used for corruption by clients from sectors such as real estate, construction, pharmaceutical, arms and defense, extraction of natural resources and energy industries.
- A service provider runs a risk of being used for sanction evasion because clients trade with sanctioned countries.

Analysis
The organization overview and the risk scenarios lead to inherent or gross risks. The inherent/gross risks are calculated by determining the likelihood that a risk scenario will occur or can occur and its impact. The likelihood is, for example, the number of times per year that something occurs or could occur. When determining the likelihood, the quantitative information from the organization overview is used. The impact relates to the financial damage or costs and the reputational damage that can occur if a risk materializes. Below are examples of how likelihood and impact can be determined.

Score		Description likelihood	Description impact
4	Very high	The scenario will most likely occur several times per year; the scenario can occur more than four times per year	Severe financial or reputational damage; heavy or several measures from supervisory authority; long-term impact on customers and operational management
3	High	The scenario will most likely to occur a few times per year; the scenario can occur two to three times per year	High financial or reputational damage; heavy or several measures from supervisory authority; medium-term impact on customers and operational management

2	Medium	The scenario may occur once per year, the scenario can possibly occur	Limited financial or reputational damage; simple measure from supervisory authority; loss of confidence, complaints from customers, short-term impact on operational management
1	Low	The scenario occurs less than once per year; the scenario is unlikely to occur	Negligible financial or reputational damage, no measures from supervisory authority negligible loss of confidence, no impact on operational management

Assessing effectiveness of control measures
The effectiveness of the controls per risk scenario also has to be assessed. For this, among others, audit reports, information from the compliance monitoring, incident reports and, if available, reports from the CBA can be used. It is important that a realistic assessment is made whether the existing measures are being effectively applied and implemented.

In assessing the existing level of controls the following criteria can be used:

1. The control is fully operational and fully effective.
2. The control could be improved in certain areas, but works adequately and is effective.
3. Substantial improvement necessary, but the control has some effect.
4. There is no control, or the control has no effect.

Determining additional measures
By comparing the inherent risks with the control measures, the service provider can determine the net risks and gaps in the existing control measures. On the basis of this, the service provider will assess which additional measures have to be taken.

A business risk assessment provides insight into the extent to which a risk can actually occur and if the risk must be further reduced to an acceptable level. The service provider must also consider whether the (gross and net) risks fall within the risk appetite. The risk analysis provides the service provider and its management with clear insight into the risks that need to be controlled and which (additional) measures need to be taken.

With a tailor-made business risk assessment, the service provider assesses whether there are gaps in the controls. If a risk has a higher likelihood of materializing, this must also be reflected in (amendments of) the policies and the procedures and the knowledge and awareness of employees. The identified risks will have to be incorporated in various processes of the service provider, such as the customer acceptance, transaction monitoring, reporting of unusual transactions or incidents. If the risk analysis shows that there is a (too) high net risk for certain types of clients, then the client acceptance process, the review process as well as the transaction monitoring on these clients will have to be enhanced.
The service provider must have appropriate mechanisms to document and provide risk assessment information to the CBA.

Summary of steps to be taken

Step 1: business overview and risk scenarios

- Business overview: make an overview for each business unit/branch office/subsidiary of the organization with respect to factors such as products, customers, countries, staff, third parties, et cetera.
- Scenarios: assess which ML/TF/integrity risks may occur and the form that they maytake.
- Scoring system: determine how to assess likelihood andimpact

Risk	Factor	Scenario	Likelihood	Impact

Which ML/TF/integrity risks is the service provider likely to face?	*Which factors play a role for each risk?*	*How is the risk likely to manifest itself?*	*What is the likelihood of a particular scenario occurring?*	*What will be the impact on the service provider if the scenario materializes?*

Step 2: analysis of gross risks and controls

- Gross risks: for each scenario, determine the likelihood of the scenario occurring and the resulting impact.
- Risk appetite: assess the gross risk and verify whether this is within the boundaries of the risk appetite.
- Controls: list and assess the control measures in place for each scenario.

Gross Risk	Risk appetite	Control measures	Assessment of control
Determine the inherent/gross risk by assessing the likelihood and impact of each risk scenario.	*Is the inherent/gross risk within the limits of the risk appetite?*	*Which control measures are in place for each risk scenario?*	*How effective are these control measures?*

Step 3: assessment of net risks and additional measures required

- Net risks: determine the net risk for each scenario by comparing gross risk with the level of control.
- Risk Appetite: determine whether net risk is within the boundaries of the risk appetite.
- Additional measures: determine the type of action to be taken, increase controls or reduce risks.

Net risk	Risk appetite	Gap	Measures required
Determine net risk by assessing gross risk and the relevant control measures in place	*Is the net risk within the limits of the risk appetite?*	*Are there any deficiencies with respect to the control measures?*	*Which measures are required in order to control or avoid this specific risk?*

3.4 Risk Management Systems

3.4.1 Statutory requirements

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

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

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

According to article 46, paragraph 4, of the AML/CFT State Ordinance, the findings of the periodical evaluations must be recorded in writing.

3.4.2 Regulatory requirements

- The service provider identifies a member of the Board/senior management who is primarily responsible for the implementation of the laws, regulations and measures necessary to comply with AML/CFT Laws and Regulations and this Handbook.

- Taking into account the conclusions of the business risk assessment and AML/CFT strategy, the Board/senior management must organize and control the service provider effectively, including establishing and maintaining appropriate and effective AML/CFT policies, procedures and measures.

- The Board/senior management informs all relevant business units and staff of the outcome of the business risk assessment, the policy, procedures, and measures.

- The Board/senior management shall ensure adequate resources to manage and mitigate the identified ML/TF risks taking into account the size, nature and complexity of its business.

- The Board/senior management shall approve the policies, controls and procedures that they put in place and monitor and, where appropriate, enhance the measures taken.

- The Board/senior management must conduct independent assessments of the effectiveness of its policies, procedures and measures on a periodic basis.

- In the assessment of the policies, procedures and measures, the Board/senior management must consider what barriers (including cultural barriers) exist to prevent the operation of effective AML/CFT policies, procedures and measures, and must take effective measures to address these.

- The Board/senior management at least annually commissions and considers a report from the MLCO and MLRO that covers compliance and the AML/CFT requirements, and it must discuss the report in a meeting, minute the meeting, and sign off and retain the report. With bigger service providers, such meetings should take place, at a minimum, on a quarterly basis.

- Where appropriate with regard to the size and nature of the business, the Board/senior management shall in addition engage an independent audit function to test the effectiveness of the internal policies, controls and procedures.

- The frequency and scope of the MLCO and MLRO reports and the audit must be determined based on the risk profile of the service provider as determined in the business risk assessment.

- The Board/senior management must reach an independent conclusion as to the effectiveness of the service provider's policies, procedures and measures. Where changes to policies, procedures and measures are required, the Board/senior management must ensure that the service provider makes those changes in a timely manner, and monitor adequate follow up action.

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

- The service provider must have an ongoing employee training program so that staff is adequately trained to implement the AML/CFT policies and procedures. Training should

typically take place, at a minimum, on an annual basis. In addition, new employees should be trained as soon as possible.

- The service provider has adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.

3.4.3 Guidance notes

Policies and procedures
Based on the AML/CFT State Ordinance, other relevant regulations and international standards, **and using the outcome of the most recent business risk assessment**, the service provider must develop and implement AML/CFT policies, procedures and measures to prevent ML/TF and control ML/TF risks.

The policies and procedures must be implemented through the consistent application of policies and procedures throughout the organization, with adjustments as necessary to address variations in risk according to specific business lines or geographical areas of operation. The policies and procedures are tailor-made to the size and nature of the service provider, clearly specified in writing (as required in article 46 of the AML/CFT State Ordinance), and communicated to all personnel. They contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the service provider in compliance with regulations.

Risk management
Compliance starts at the top. It will be most effective in a corporate culture that emphasizes standards of honesty and integrity and in which management leads by example.

The Board/senior management is responsible for ensuring that the ML/TF risks are effectively managed. The Board/senior management is responsible for establishing a written AML/CFT policy that contains the principles to be followed by management and staff, and explains the main processes by which risks are to be identified and managed through all levels of the organization. Upon reaching an independent conclusion as to the effectiveness of the service provider's policies, procedures and measures, the Board/senior management will discuss the review of its compliance and minute such at a meeting of the Board/senior management at least annually.

Management approves the AML/CFT policy and at least once per year, or whenever material changes to the business of the service provider or the legal requirements occur, assesses the extent to which the service provider is managing its risks effectively.

As a general rule and in the context of AML/CFT, the business units (e.g., front office, customer-facing activity) are the first line of defense in charge of identifying, assessing and controlling the risks of their business. They have to know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. The second line of defense includes the MLRO and MLCO. The third line of defense is the internal audit function.

Ensuring effectiveness of policies and procedures
The Board/senior management takes a risk-based approach when determining on the reviews of the policies and procedures and ensures that those areas deemed to pose the greatest risk to the service provider are reviewed more frequently and in-depth. The Board/senior management therefore commissions the MLCO and MLRO to regularly report on the effective implementation of the AML/CFT policies, procedures and measures. The reports of the MLCO and MLRO include the outcomes of sample testing of the effectiveness and adequacy of the policies, procedures and measures. This includes, among others, information and advice on the adequacy of CDD process and files, the appropriateness of the transaction monitoring system, and the provision of AML/CFT training, including an assessment of the methods used and the effectiveness of the training received by employees.

The MLCO and MLRO also provide information and advice on their own account to assist the Board/senior management in assessing the effectiveness of the service provider's policies, procedures and measures.

In case shortcomings or defects are identified, the Board/senior management will report these to the MLCO. These shortcomings or defects will be timely and appropriately addressed in the policy, procedures, and measures.

Audit
In addition to the MLCO and MLRO, the Board/senior management also considers whether, based on the size, nature, complexity and risk profile of the service provider, it would be appropriate to have an independent audit function to test the AML/CFT policies, procedures and controls. In case there is an internal audit function, this function must be independent and adequately resourced

In principle, all service providers must have their own audit function. Only in cases where this is not feasible, may an entity utilize the services of an external or group auditor to test the appropriateness and effectiveness of their policies, procedures and controls.

The audit also includes an assessment of the ongoing competence and effectiveness of the MLRO and MLCO, for instance the handling of internal disclosures to the MLRO and external disclosures to the FIU.

3.5 MLCO and MLRO

3.5.1 Statutory requirements

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

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

According to article 47, paragraph 3, of the AML/CFT State Ordinance, a service provider must inform the FIU and the CBA of the appointment of the MLCO and the MLRO, within a month after the appointment took place.

3.5.2 Regulatory requirements

- A service provider must appoint a MLCO that:
  - has adequate, relevant and demonstrable knowledge, experience and skills;
  - **is based in Aruba;**
  - has appropriate independence and authority;
  - reports directly to, and has regular contact with, the Board/senior management so as to enable the Board/senior management to ensure that all obligations are being met and that the service provider is taking sufficiently robust measures to protect itself against the potential risk of being used for ML or TF;
  - is responsible for the effectiveness of compliance and conducts independent assessments on CDD and reporting;
  - demonstrates responsibility and ownership of the AML/CFT framework of the regulated entity;
  - has sufficient resources, including sufficient time and (if appropriate) a deputy MLCO and support staff;

- has unfettered and timely access to all business lines, support departments and information necessary to appropriately perform the function
- receives the full co-operation of the staff.

- A service provider must appoint a MLRO that:
  - is employed by the service provider;
  - **is based in Aruba;**
  - is the main point of contact with the FIU in the reporting of unusual transactions;
  - is available on a day-to-day basis;
  - has adequate, relevant and demonstrable knowledge, experience and skills;
  - has appropriate independence and authority;
  - reports directly to, and has regular contact with, the Board/senior management so as to enable the Board/senior management to ensure that all obligations are being met and that the service provider is taking sufficiently robust measures to protect itself against the potential risk of being used for ML or TF;
  - has sufficient resources including sufficient time and (if appropriate) a deputy MLRO and support staff;
  - has unfettered and timely access to all business lines, support departments and information necessary to appropriately perform the function;
  - receives the full co-operation of the staff.

- Where appropriate with regard to the size and nature of the business, the appointment of the MLCO is at management level.

- When considering whether it is appropriate to appoint the same person as MLCO and MLRO, a service provider should demonstrate to the CBA that:
  - the respective demands of the two roles, taking into account the size and nature of the service provider's activities; and
  - whether the individual will have sufficient time and resources to fulfill both roles effectively.

- **Financial service providers have to report the appointment of a new MLCO and/or MLRO to the CBA within one week after the appointment has taken place**.

- The Board/senior management shall demonstrate **upon request** to the CBA that the MLRO and MLCO have adequate knowledge, e.g. by submitting to the CBA upon request certificates or diplomas and/or proof of participation in AML/CFT related training programs.

- The service provider provides the CBA **upon request** with the assessment of the suitability of the appointed MLCO or MLRO, including information on the knowledge, experience and skills of the MLCO or MLRO.

- In the event that the position of MLCO and/or MLRO is expected to fall vacant and a new MLCO and/or MLRO has not been appointed yet, a service provider must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

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

- Specifically with respect to the **designated non-financial service providers** the following applies: further to the assessment of the money laundering and terrorist financing risks a designated non-financial service provider is prone to (the business risk assessment, as discussed in paragraph 3), designated non-financial service providers should take reasonable measures to

meet the requirements of Section 47 LWTF (the appointment of a MLRO and MLCO) which are proportionate to the nature and extent of the (business of the) designated non-financial service provider, as well as the frequency with which the designated non-financial service provider renders the services as referred to in Section 6, second paragraph, of the LWTF. Account can therefore be taken of the fact that a designated non-financial service provider is small in size (a designated non-financial service provider consisting of no more than two employees and with a turnover of less than Afl. 100,000 on an annual basis), and not or only incidentally renders the services to which the provisions of Chapters 2 and 3 of the LWTF apply. In that case, the designated non-financial service provider may decide to appoint (one of the) the policy maker(s) of the designated non-financial service provider as MLCO and/or MLRO.

- In any case the CBA is of the opinion (for example following the findings of an on-site) that the MLCO and/or MLRO function is inadequately staffed by the service provider, the CBA may instruct the service provider to enhance the MLCO and/or MLRO function staffing.

3.5.3 Guidance notes

Management is responsible for establishing permanent and effective MLRO and MLCO functions within the service provider as part of the AML/CFT policy.

As stated in the regulatory requirements, the Board/senior management ensures that the MLCO and MLRO functions are independent. This means that these functions have a formal status within the service provider to give it the appropriate standing, authority and independence. These functions should not be placed in a position where there is a possible conflict of interest between their AML/CFT responsibilities and any other responsibilities they may have. If, due to a small number of employees, the MLCO or MLRO hold another function at the service provider, the Board/senior management ensures that any conflicts of interest are identified, documented and properly managed.

As stated in the regulatory requirements, the appointment of the MLCO must be at management level having regard to the size and nature of the business. “Nature and size" of the service provider involves a combination of factors; not only the size of the service provider by number of employees, but also the volume of assets, number of clients, number of foreign or high risk clients and types of products. A service provider with only few employees, but with a large number of high risk clients, will need to appoint an MLCO at management level.

The CBA will assess whether the other position held by the person concerned does not take too much time to enable the person concerned to perform the duties of MLCO or MLRO in an adequate manner. The CBA will also assess whether the interests of the other position are not contrary or could be contrary to the interests of the tasks of the MLCO or MLRO.

The MLCO and MLRO functions are sufficient and appropriate to ensure that ML/TF risks are managed effectively. The MLCO and MLRO have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties. They have a sound understanding of the AML/CFT Law and Regulations as well as international AML/CFT standards and their practical impact on the service provider’s operations. The professional skills of the MLRO and the MLCO, especially with respect to keeping up-to-date with developments in relevant laws, regulations and standards, are maintained through regular and systematic education and training. The MLCO and MLRO (and their staff) have access to the information and personnel necessary to carry out their responsibilities.

The primary role of the MLCO is to assume responsibility over the service provider’s compliance with the AML/CFT requirements, policies and procedures. The MLCO develops a compliance program that sets out its planned activities, such as the implementation and review of specific policies and procedures, the business risk assessment, regular testing and monitoring, and educating staff on AML/CFT matters.

The MLCO advises management on compliance with the relevant laws, rules and standards, including keeping them informed on developments in the area. The MLCO should monitor and test AML/CFT compliance by performing sufficient and representative compliance testing. The MLCO reports periodically, as appropriate, to management on compliance with the service provider's policies, procedures and measures. The report refers to the business risk assessment, including any changes in the service provider's risk profile based on relevant measurements such as performance indicators, summarize any identified breaches and/or deficiencies and the corrective measures recommended to address them, and report on corrective measures already taken.

The MLCO responds promptly to requests for information made by the CBA and the FIU and acts as the liaison point with the CBA and in any other third-party enquiries in relation to ML or TF.

The MLRO maintains a record of all enquiries received from the FIU and law enforcement authorities and a record relating to all internal and external unusual transaction reports. The MLRO manages business relationships effectively post reporting to the FIU to avoid tipping off any third parties, and acts as the liaison point with the CBA and the FIU and in any other third-party ML/TF enquiries.

3.6 Group Compliance

3.6.1 Statutory requirements

Under Article 45, paragraph 1, of the AML/CFT State Ordinance, a service provider that has a branch or subsidiary outside Aruba must take care that the branch or subsidiary applies as much as possible the provisions set by or by virtue of the AML/CFT State Ordinance and the internationally accepted AML/CFT standards.

According to Article 45, paragraph 2, of the AML/CFT State Ordinance, this applies in particular to branches and subsidiaries in countries and jurisdictions that do not or insufficiently apply the international accepted AML/CFT standards.

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

3.6.2 Regulatory requirements

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

3.6.3 Guidance notes

Local laws and regulations to promote the prevention of money laundering and terrorist financing, may differ between jurisdictions. Internationally operating service providers set global minimum standards for the implementation of AML/CFT policies and procedures, which are applicable to the entire group. This means that the AML/CFT control measures will in any event apply to all business operations, all functional activities, and all customers and products worldwide. A service provider may operate in jurisdictions where local laws and regulations set lower AML/CFT standards than the service provider's global minimum standards. Service providers will then apply the group's higher standards to the offices and branches in those jurisdictions. If local laws and regulations impose higher standards for AML/CFT control measures than the minimum standards, the service provider will reassess its minimum standards and adjust them where necessary and apply the more stringent requirements.

3.7 Outsourcing

3.7.1 Regulatory requirements

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

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

- The outsourcing of activities shall not hinder the CBA's supervision of the service provider's compliance with the AML/CFT Laws and Regulations, including direct and full access to all customer due diligence-files (digitally and/or physical).

- A service provider must consider the effect that outsourcing has on the ML/TF risks, in particular where an MLCO or MLRO is provided with additional support from third parties, either from within the group or externally.

- A service provider must assess possible ML/TF risks associated with outsourced activities, record its assessment, and monitor any risk on an ongoing basis.

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

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

- A service provider must in any case regulate the following in the outsourcing agreement:
    - the mutual exchange of information, including agreements about providing information requested by the CBA in connection with the execution of its supervisory tasks;
    - the possibility for the service provider to at all times make changes in the manner in which the activities are carried out by the third party;
    - the obligation of the third party to enable the service provider to continue to comply with the AML/CFT Laws and Regulations;
    - the possibility for the CBA to carry out or have carried out an investigation at the third party's premises; and the manner in which the agreement is terminated, and the manner in which it is ensured that the service provider is able, after the termination of the agreement, to carry out the activities again itself or have another third party carry out these activities.

3.7.2 Guidance notes

Although a service provider can outsource the execution of (parts of) the CDD process, it should take into account that the ultimate responsibility for meeting the CDD requirements remains with the service provider that has outsourced the CDD process. It is thus important that a judgment of the risk is made with regard to the expertise and practical approach of the third party in terms of compliance with the AML/CFT Laws and Regulations. In outsourcing it is important that the outsourcing service provider not only lays down in writing that the third party will comply with all statutory requirements, but also that the service provider will periodically check and verify this. The service provider therefore ensures that the work undertaken by the outsourced service provider is monitored to ensure it complies with the applicable legal requirements.

The service provider ensures, at the commencement of an outsourcing arrangement and on an ongoing basis, that the outsourced service provider:

- has the appropriate knowledge, skill and experience;
- is familiar with the applicable AML/CFT requirements;
- is sufficiently resourced to perform the required activities;
- has in place satisfactory policies, procedures and controls which are, and continue to be, applied to an equivalent standard and which are kept up to date to reflect changes in regulatory requirements and emerging ML/TF risks.

The reports provided by the outsourced service provider contain meaningful, accurate and complete information about the activities undertaken, progress of work and areas of non-compliance identified; and explain in sufficient detail the materials reviewed and other sources investigated in arriving at its conclusions so as to allow the service provider to understand how findings and conclusions were reached and to test or verify such findings and conclusions.

4. CDD

4.1 Introduction

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

Sound CDD measures are vital because they:

- help to identify and mitigate ML/TF risks to which certain clients can expose a service provider;
- help to protect the service provider and the integrity of the financial sector in which it operates by reducing the likelihood of the service provider becoming a vehicle for, or a victim of, financial crime;
- assist law enforcement, by providing available information on customers or activities and transactions being investigated, for instance following an unusual transaction report to the FIU;
- constitute an essential part of sound risk management, e.g. by providing the basis for identifying, limiting and controlling risks, including reputational, operational, legal and concentration risks; and
- help to guard against other integrity risks, such as corruption, sanctions evasion, identity fraud.

CDD thus forms an important part of the measures to prevent money laundering and terrorist financing and to protect the reputation of the service provider. The inadequacy or absence of satisfactory CDD measures can subject a service provider to serious customer and counterparty risks, as well as reputational, operational, legal, regulatory and concentration risks, any of which can result in significant financial cost to the service provider. CDD information is also a vital tool for the MLRO and employees when examining unusual or higher risk activity or transactions, in order to determine whether an unusual transaction report is appropriate.

CDD concerns measures regarding the client, the ultimate beneficial owners (UBO) and the representatives of the client, the ownership and control structure of the client, the purpose and intended nature of a business relationship, and the source of the funds used in the business relationship or transaction. Based on a combination of CDD measures and risk indicators, the service provider makes a risk assessment of the client before accepting the client. During the ongoing monitoring of the activities of the client, such as the transaction monitoring and periodic review, the information on the client is reviewed to assess whether the service provider's understanding of the client and the client's risk profile still match.

The definition of "client" covers all natural persons or legal entities with whom the service provider enters into a business relationship or who causes a transaction to be carried out. A business relationship is any business, professional or commercial relationship with a natural person or legal entity, in relation to the commercial or professional activities of the service provider and which from the time of establishing contact is assumed to continue for a time.

CDD consists of the following (risk-based) measures (where applicable)

- identification and verification of the identity of the client;
- identification and verification of the identity of the representative;
- identification and verification of the identity of the UBO;
- understanding the ownership and control structure of the client;
- determining the nature and intended purpose of the business relationship;
- establishing the source of funds;
- establishing the source of wealth of a PEP or high risk client/UBO;
- determining the risk profile of the client;

- ongoing monitoring of the business relationship and keeping CDD information current and relevant.

4.2 Risk-based approach

4.2.1 Statutory requirements

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 ML or TF in relation to the type of customer, business relationship, product, or transaction. To that effect, a service provider must establish a risk profile of the customer and the UBO.

4.2.2 Regulatory requirements

- A service provider's business risk assessment (see Chapter 3.3) should enable the service provider to determine its initial approach to performing the CDD process, depending inter alia on the type of customer, business relationship, product or transaction involved.

- The customer risk assessment must result in a substantiated determination of a risk profile of the customer and the UBO and the extent of CDD information that is obtained, how that information will be verified, and the extent to which the resulting business relationship will be monitored. Also, the risk profile should indicate how the risks determined will be mitigated by the service provider.

- The process of determining an appropriate risk profile must take into account the absence or presence of relevant risk factors, whether any compensating factors apply, the CDD information held by the service provider, **including information from screening against PEP-list, sanction lists and reliable open sources**.

- A customer and UBO risk profile must, in any event, contain sufficient information to 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 ML/TF activity.

4.2.3 Guidance notes

The AML/CFT State Ordinance allows for a risk-based approach. 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 for ML/TF by focusing resources on higher risk areas.

This means that CDD can be demonstrably attuned to the ML/TF risk according to the type of client, business relationship, product or transaction. To this end, the nature and intended purpose of the relationship is considered; the size of the assets involved in the business relationship and the size of the transactions; and the regularity or duration of the business relationship. Risk factors related to country, client, product, service, transaction and delivery channel are considered. Based on the obtained information, the service provider determines the extent of the CDD measures to be taken and why.

Risk profile
The objective of the CDD process is to determine the risk profile of the customer, including the UBO. This means that sufficient information is gathered in such a way that all relevant risk factors are identified, and a comprehensive picture of the risks associated with a particular business relationship is obtained. Information to be collected includes CDD information and information on adverse news, checks against sanctions lists and PEP lists, bad press and google checks, checks against reliable databases and external sources. On the basis of the information collected during the CDD process, a risk profile of the client is established. A different weight can be assigned to the various risk factors, depending on their

relative importance. The client risk weighting is not unduly influenced by just one factor. For instance, when the only risk factor is that the client has a complex corporate structure, this does not automatically mean that the client has to be assessed as high risk. Equally, the presence of one lower risk factor, for instance a listed company, should not automatically lead to a determination that a customer is lower risk. Assessing the risk of a customer takes a holistic approach to all CDD elements.

In assessing the risk of a client, the service provider considers factors such as (not limitative):

- the business activities, industry type or the profession of the client;
- the country of establishment, incorporation or residence of the client and the UBO;
- the ownership and control structure of the client;
- the reason for the requested services or products;
- the nature and purpose of the account and relationship;
- the source of the funds;
- the source of wealth of a PEP or high risk client/UBO;
- negative or adverse news on the client, the UBO of the client, the representative, or other relevant parties to the business relationship or transaction;
- hits from any of the databases used by the service provider (e.g. Sanctions, PEP)
- the way in which the client is introduced.

The service provider also uses other information obtained, e.g. declared activities, economic rationale of these activities and resulting transactions, expected turnover, main counterparties whose activities should be in line with the client's activities. Based on the risk assessment, clients are for instance classified as low, normal, high or extreme or unacceptable risk.

Being identified as carrying a higher ML/TF risk does not automatically mean that a customer is laundering money or financing terrorism. It does mean, however, that additional CDD measures have to be taken. Similarly, identifying a customer as carrying a lower ML/TF risk does not mean that the customer is not a money launderer or is financing terrorism.

Where it is appropriate to do so, risk may be assessed generically for customers falling into similar categories. For example, the business of some service providers, their products, and customer base, can be relatively simple, involving few products, with most customers falling into similar risk categories. In such circumstances, a simple approach may be appropriate for most customers, with the focus being on those customers who fall outside the norm. However, when such an approach is applied by the service provider. it should be constantly vigilant that the risk categorization may not be too broad and subsequently may lead to a negligence of the important differences that may exist between the clients (e.g. a categorization based on a type of business, while the individual businesses included in the category seriously differ in size, background, market focus, etc). A more complex system may be appropriate for diverse customer bases or service providers with broad ranges of products or services.

Risk factors
Within the holistic approach to risks, factors related to country risk, client risk, product, service, transaction risk and delivery channel risk are taken into account:

Client related risk factors
When identifying the risk associated with clients, including their UBOs, the following risks shall be taken into account (<u>not limitative</u>):

- The client's and the UBO's professional activity. Certain sectors are considered to be more susceptible to ML/TF and other criminal activities and are, therefore, deemed as a higher risk than others. An example is the commercial real estate sector of which by its very nature, its operations entail a greater risk of fraud and money laundering;
- The client's and the UBO's source of funds and/or source of wealth;
- The client's and the UBO's reputation;
- The client's and the UBO's nature and behavior;
- The client's legal form.

In case the client requests or executes transactions that are complex, unusually or unexpectedly large or that have an unusual pattern without an apparent economic or lawful purpose or a sound commercial rationale?

Country and geographical related risk factors
When identifying the risk associated with countries and geographical areas, the following risks shall be taken into account (not limitative):

- The countries in which the client and the UBO(s) are based;
- The countries that are the client's and UBO's main places of business;
- The countries to which the client and UBO(s) have relevant personal links;
- The countries in which the cash flows are generated or assets are located.

Product, service, transaction related risk factors
When identifying the risk associated with product, service, transaction, the following risks shall be taken into account (not limitative):

- The level of transparency of the product, service or transaction;
- The complexity of the product, service or transaction;
- The value or size of the product, service or transaction;
- Is the proposed transaction in line with the economic activity of the client or does it concern a non-routine activity?
- To what extent does the transaction involve multiple parties or multiple jurisdictions?
- To what extent do products or services allow payments from third parties or accept prepayments or overpayments where this would normally not be expected?

Delivery channel related risk factors
When identifying the risk associated with the delivery channel, the following risks shall be taken into account (not limitative):

- The extent to which the business relationship is conducted on a non-face-to-face basis (without any safeguards related to the CDD process);
- The introducers or intermediaries via which the service provider obtains its business;
- A client is introduced by a third party and the service provider is unaware whether that third party is subject to equivalent AML/CFT obligations in the country where the service provider operates;
- Client contact takes place through agents or intermediaries and the service provider relies on the completeness and correctness of the information provided by these agents or intermediaries.

See also Chapter 12 for risk factors per sector.

4.3 Timing of initial identification and verification of identity

4.3.1 Statutory requirements

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.

Article 8, paragraph 2, of the AML/CFT State Ordinance provides the following exceptions:

A service provider may verify the identity of the customer and the UBO during the establishment of the business relationship, if this is necessary not to disrupt the normal conduct of business, and there is little ML/TF risk; in this case, the service provider must verify the identity as soon as practicable after the first contact with the customer;

A service provider being a life insurer may identify the beneficiary of a policy and verify the identity, after the business relationship has been entered into; in this case, the identification and the verification of the

identity must take place on or before the date of payment, or on or before the date on which the beneficiary wants to exercise his rights arising from the policy;

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

A designated non-financial service provider who is a civil notary can establish the identity of the client and verify the ultimate beneficial when identification is required pursuant to article 20, first section, of the State Ordinance on Civil Notaries (AB 1990 No. GT 69).

4.3.2 Regulatory requirements

- The CDD process, including the verification of the identity of the UBO('s), should be finalized before accepting the client. It is not permitted to enter into or continue a business relationship with a client and to provide services without the CDD process having been completed.

- In exceptional cases, for instance not to interrupt the normal conduct of business, CDD can be completed shortly after the start of the service. This is only permitted where there is a low risk for money laundering or terrorist financing and the CDD process is completed as soon as possible.

- Where the verification of the identity of the client or the UBO takes place after the establishment of a business relationship, the service provider must have taken appropriate and effective measures to manage the risk arising from the delay:
    - establishing that it is not a high risk relationship;
    - ensuring that CDD is completed as soon as reasonably possible; and
    - ensuring funds are not paid out or accounts are or remain blocked.

- The service provider highlights to its customer its obligation to terminate the relationship in case the customer is not able to provide the information necessary to meet the CDD requirements within a reasonable period of time.

- In case the customer is not able to provide the information necessary to meet the CDD requirements, a service provider must terminate the relationship (See Chapter 4.5).

4.3.3 Guidance notes

In principle, CDD is completed before the business relationship is established and the service provision commences. However, there are exceptions in cases where the provision of services, for instance, certain advisory services to customers, cannot be interrupted. In some cases, the nature of the service provider or of the services offered creates technical or organizational reasons why preliminary and limited services may be provided before CDD is completed. In these exceptional cases, the purpose of the law should still be kept in mind: to prevent the service provider's services from being used for money laundering or terrorist financing. This is subject to the condition that the risk of money laundering or terrorist financing is low and that the service provider will complete CDD as soon as possible after the first contact with the customer.

This implies that the service provider performs a preliminary risk estimation to assess whether the ML/TF risk is sufficiently low. Examples of indicators to be used in such an estimation exercise are the customer's country of origin, the customer's line of business or the product or service. The service provider remains obliged to complete the identification and verification process as soon as possible after the initial contact.

Banks may also open an account in such cases, with verification of identity being carried out later, provided the service provider ensures that the account cannot be used in the interim. This also applies to credit cards issued by banks. As long as the credit card is blocked (comparable to an account that cannot

yet be used), the bank can still perform CDD, but once the credit card is unblocked and the card can be used (regardless of whether it is actually used), the CDD procedures should have been completed.

Similarly, on taking out a life insurance policy, it is permitted to identify the policy's beneficiary and verify his/her identity after the business relationship has been entered into. In that case, identification and verification of identity should take place on or before the time of payout, or on or before the time that the beneficiary wishes to exercise his/her claims under the policy. The payout to a beneficiary of a life insurance policy is not an occasional transaction but is the result of the business relationship into which the service provider has entered with the policyholder. If the beneficiary of a life insurance policy is a legal entity, the UBO('s) of that legal entity needs also to be identified and his/her identity verified, using risk-based and adequate measures.

For some non-financial service providers, such as lawyers, notaries or tax advisors, it will be necessary to determine adequately which services are requested. Therefore, an initial interview with the client can be required that takes place in confidentiality. This guarantees that a client can present all the information that is important for assessing whether legal assistance is requested in connection with any legal proceedings, or whether services are required that fall within the scope of the AML/CFT State Ordinance. This initial interview will be sufficient to gain insight into the client's motives. Insofar as it subsequently becomes clear that it concerns services that are not related to any legal dispute, the AML/CFT State Ordinance will most likely apply. This means that in that case the non-financial service provider will have to suspend the execution of the services until the CDD measures have been applied. If the actual service provision starts during the initial interview, the service provider will have to conduct CDD at that moment.

4.4 Situations in which CDD must be applied

4.4.1 Statutory requirements

Article 6, paragraph 1 and 2, of the AML/CFT State Ordinance prescribes that service providers must apply CDD measures in the following cases:

All service providers

- *when entering into a business relationship in or from Aruba;*
- *if there are indications that the client is involved in ML or TF;*
- *if it doubts the soundness or reliability of data obtained from the client previously, or*
- *if the risk of involvement of an existing client in ML or TF gives reason to do so.*

Financial service providers

- *when carrying out an occasional transaction in or from Aruba for the benefit of a customer of at least Afl. 25,000.-, or of two or more transactions related to each other with a combined value of at least Afl. 25,000.-;*
- *when carrying out a money transfer as meant in Article 1 of the SOSMTC in or from Aruba.*

Article 6, paragraph 2, of the AML/CFT State Ordinance prescribes for non-financial service providers specific circumstances when CDD measures must be applied. These specific sectoral requirements are addressed in Chapter 12.

4.4.2 Guidance notes

The AML/CFT State Ordinance requires that CDD has also to be carried out if there are indications that the client is involved in ML/TF; if there are doubts about the soundness or reliability of data obtained from the client previously; or if the risk of involvement of an existing client in ML/TF gives reason to do so. This will often be the case for existing clients and will be a reason for an event driven review.

A financial service provider must perform CDD when two or more related transactions are conducted with a minimum combined value of Afl. 25,000. This will be assessed by the financial service provider on the basis of the type of transaction and the amounts involved. To begin with, the transactions should be one-off transactions, which means that no business relationship exists. It is also logical that the transactions should be similar in nature. For instance, someone who, through several transactions conducted in a single day or within a few days, makes cash payments into an account without being its account-holder (or acting on behalf of the account-holder), the overall amount of which exceeds Afl. 25,000. By contrast, this provision is most likely not applicable to a customer that pays the cash proceeds from its regular business operations into its own account daily, as such payments are made as part of the business relationship.

4.5 Failure to complete CDD

4.5.1 Statutory requirements

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 a transaction, if it has not applied CDD measures, if it is not able to apply CDD measures or if the CDD measures did not lead to the result envisaged by Article 3, 4 and 5 of the AML/CFT State Ordinance.

According 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.

4.5.2 Regulatory requirements

- Where the immediate termination of a business relationship is not possible for whatever reason, the service provider must ensure that the risk is managed and mitigated effectively until such time as the business relationship can be terminated.

- When terminating a business relationship where funds or other assets have been received, a service provider should return the funds or assets to the source from which they originated, for example by returning funds to the account from which it was received.

- Where the service provider has been unable to return the funds to the account from which they were received, for instance because the originating bank account has been closed, the service provider must take appropriate steps to return the funds to the same party.

- Where the customer requests that money or other assets be transferred to third parties, or to a different account in the customer's name, or by way of a different payment method, the service provider must assess whether this warrants a report to the FIU.

4.5.3 Guidance notes

A service provider may only enter into a business relationship if it has conducted the full CDD process, this CDD process has led to the result that the AML/CFT State Ordinance has intended, and the service provider is in possession of all required CDD information.

Under the AML/CFT State Ordinance, it is prohibited to enter into a business relationship or carry out a transaction if no CDD has been performed or if the CDD, including on the UBO, has not produced the intended result. A service provider can for instance conclude on the basis of a risk assessment that an existing or prospective relationship with a customer carries too high a risk. It can also occur that the CDD procedures have not been completed and the service provider is unable to determine precisely who its customer is and/or what the purpose of the proposed business relationship is. The service provider does

not embark on a business relationship in those cases or discontinues an existing relationship at the earliest opportunity. A service provider also reports these instances to the FIU if there are also indications that the customer is involved in money laundering or terrorist financing.

To ensure that all these obligations are met and that relationships with existing customers are ended properly, the service provider may formulate a customer exit policy. Among others, this policy states the circumstances under which the relationship with a customer will be ended, and the procedures for doing so.

A service provider may demonstrate that it has a right to terminate a relationship where the terms of business which govern the relationships with customers include the termination of relationships in case the customer is not able to provide the information necessary to meet the CDD requirements.

The immediate termination of a business relationship may not always be possible due to contractual or legal reasons outside the control of the service provider. The timing of the termination of an established business relationship will depend upon the nature of the underlying products or services. As an example, while a bank can close an account and return deposited funds to a customer relatively easily, the compulsory redemption of an investment or a cancellation of a life insurance may be more problematic.

If unable to terminate the business relationship, the service provider takes additional adequate measures to perform (enhanced) customer due diligence. In case the termination of a business relationship cannot be completed (for example, because the service provider has lost contact with the customer) the service provider has procedures and controls in place to ensure that funds or assets held are 'blocked' or placed on a 'suspense' account until such time as contact with the customer is re-established or the service provider has otherwise dealt with the funds or assets in accordance with its policy for dormant accounts. If this is not possible (for example, if the relevant party no longer exists), the service provider takes appropriate steps to return the funds to an appropriate third party and document the reasoning for the steps taken.

4.6 Identification and verification of the identity of the client

4.6.1 Statutory requirements

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

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

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

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

4.6.2 Regulatory requirements

- When, as part of the identification and verification process, determining that a customer is the person that he, she, or it claims to be, a service provider must be satisfied that:
    - a person exists - on the basis of appropriate identification information; and

- the customer is that person - by verifying from reliable, independent source documents, data or information, satisfactory confirmatory evidence of appropriate components of the customer's identity.

- The extent of identification information to be obtained, what to verify, and how to verify it in order to be satisfied as to a customer's identity, must depend on the risk assessment for that customer.

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

- Where a service provider is not familiar with the form of the evidence obtained to verify the identity, appropriate measures are necessary to ensure that the evidence is genuine.

4.6.3 Guidance notes

Identifying the customer and verifying the customer's identity, means that the client states the identity for identification purposes. Verification of the identity means that the service provider establishes that the stated identity corresponds to the actual identity of the client. The general rule is that verification of the identity takes place on the basis of documents, data or information from a reliable and independent source. A copy of a document that is not authenticated is generally not accepted as information from a reliable and independent source because it is easy to make a fraudulent copy.

Natural persons
Where the client is a natural person, the service provider can use several ways to verify the identity:

- An employee of the service provider verifies in person the identity of the client on the basis of the original identification document and indicates on the copy of the identification document that the original was seen and compared to the person (the following can be indicated: 'true copy of the original', including his/her name, function, as well as the date of verification).
- Another service provider (for instance bank, insurer or trust and company service provider) in a country that is adequately supervised for AML/CFT compliance that has carried out CDD on the customer provides the service provider with the identification and verification data, for example when the customer is introduced or when the service provider collaborates with another service provider.
- The client provides a certified copy of the identification document of the client. The certification can be done by an independent and reliable party. These can be a civil-law notary, a lawyer, a registered accountant, a member of the judiciary, an officer of an embassy or consulate.
- Based on an outsourcing agreement, an intermediary can verify the identity of the client. In this case, the service provider must have performed CDD on the intermediary and the intermediary will follow the service provider's procedures and ensures that the service provider is provided with the relevant data and documents.
- Other methods of verification, for instance any secure, remote or electronic measures can also be used as long as these measures provide safeguards that the verification is based on information from a reliable and independent source. This should be done in line with processes established by the service provider for, for instance, video conferencing.

In case a copy of an identification document is certified by an independent and reliable party, this party certifies that the original documentation verifying identity has been seen and that the copy of the document (which is certified) is a complete and accurate copy of that original; and that the photograph contained in the document certified bears a true likeness to the natural person requesting certification. The copy of the document is signed and dated.

Documents that can be used to verify the identity of a natural person

- A valid travel document in the sense of the Passport Act (Paspoortwet, Stb. 1991, 498; AB, 121);

- A valid driver's license as referred to in Article 10, first or second section, of the State Ordinance on Road Traffic (Landsverordening wegverkeer, AB 1997, no. 18);
- A valid identity card as referred to in the Identity Cards Ordinance (Landsverordening identiteitskaarten, AB 2001, no. 8).

Other documents, information or data can only be accepted for the purpose of verifying the identity of a natural person, provided they originate from a credible and independent source. If these documents do not originate from credible and independent sources, such as public authorities, the service provider will question whether the documents are sufficiently reliable. An example is the verification of identity of a natural person who is not in possession of a passport or a driver's license. An existing bank account in the name of the person in question in combination with other data on that person, may in some cases be accepted. This is a matter for the risk assessment of the service provider wishing to accept the relevant person as a customer. Documents in respect of which it is not certain that they are themselves based on adequate identification and verification, such as student and staff passes, generally do not suffice to verify identity.

Legal entities
Legal entity refers to any entity with legal personality, for instance it can sue and be sued, it can own property and it can enter into contracts. This can include companies (e.g., NV, BV, Ltd.), foundations, associations, or other similar entities which are not legal arrangements.

Legal arrangements do not have separate legal personality and therefore form business relationships through their trustees (or equivalent). With regard to trusts, it is the trustee of the trust who will enter into a business relationship or occasional transaction on behalf of the trust. Similar for entities without legal personality, such as partnerships, the partners will be the contracting parties.

Documents that can be used to verify the identity of a legal entity
The following documents and information sources can be used to identify and verify the identity of legal entities:

Where the client is an Aruban legal entity, or a foreign legal entity established in Aruba:
- An extract from the Aruban Chamber of Commerce;
- A deed or declaration from a notary established in Aruba or a country that applies adequate AML/CFT measures;
- Certificate of Incorporation (or other appropriate certificate of registration or licensing);
- Memorandum and Articles of Association or of Incorporation (or equivalent);
- Recent audited financial statements.

Where the client is a foreign legal entity that is not established in Aruba:
- Reliable documents and data or information that are customary in international business;
- On the basis of documents, data or information recognized by law as a valid means of identification in the state in which the legal person is established.

For foreign legal entities, the documents to be used will generally be similar as the documents for Aruban legal entities. In case of a reliable foreign company register, an extract from this register suffices. In other cases, documents such as the founding documents and articles of association will be obtained.

Foundations
In case the customer is a foundation, the service provider shall, at least,also obtain:

- Name of foundation.
- Date and country of incorporation.
- Type of foundation - charitable or otherwise.
- Official identification number.
- Registered business address.

- Mailing address (if different).
- Principal place of business/operations (if different).
- Control structure and beneficiaries.
- Nature of activities undertaking.
- Geographical sphere of the foundation.
- Identification information for all council members who have authority to operate a business relationship or to give the service provider instructions concerning the use or transfer of funds or assets - in line with guidance for natural persons and legal persons.
- Identification information for the founder, a person (other than the founder of the foundation)
- Information on who has endowed the foundation, and, if any rights a founder of the foundation had in respect of the foundation and its assets have been assigned to some other person, that person - in line with guidance for natural persons and legal entities.

In case the customer that is a foundation is assessed as higher risk, the service providers at a minimum also need to obtain (if applicable):

- Identification information for all council members and, if any decision requires the approval of any other person, that person - in line with guidance for natural persons and legal entities.
- Identification information on any beneficiary entitled to a benefit under the foundation in accordance with the charter or the regulations of the foundation - in line with guidance for natural persons and legal entities.
- Identification information on any other beneficiary and person in whose favor the council may exercise discretion under the foundation in accordance with its charter or regulations and that have been identified as presenting higher risk - in line with guidance for natural persons and legal entities.

4.7 Identification and verification of service provider in case of trusts

4.7.1 Statutory requirements

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

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

4.7.2 Regulatory requirements

- A service provider must collect relevant identification information on the trustee(s) and on the express trust (and any subsequent changes).

- A service provider must collect relevant identification information on the natural persons who are concerned with the trust (and any subsequent changes).

- A service provider must verify the name and date of establishment of the express trust. Whilst there is no requirement to review an existing trust instrument (or similar instrument) as a whole, satisfactory evidence of the appointment of the trustee(s), and the nature of his duties must be obtained.

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

- A service provider must take reasonable measures to verify the identity of the natural persons who are concerned with the express trust and any subsequent changes (in line with guidance for natural persons and legal persons).

- A service provider must take reasonable measures to verify the identity of a beneficiary with a vested right at the time of or before distribution of trust property or income.

- A service provider must take reasonable measures to verify the identity of any other beneficiaries and persons who are the object of a power and that have been identified as presenting higher risk, at the time that the risk is identified.

- In the case of beneficiaries of trusts are designated by particular characteristics or class, for instance “the lawful heirs” or “(grand)children and unborn (grand)children”, this needs to be properly recorded in the client file. Where the beneficiaries of a trust are designated by such characteristics or by class, the service provider needs to obtain sufficient information concerning the beneficiary to make sure that at the time of the payout or at the time of the exercise by the beneficiary of its rights, the identity of the beneficiary can be established.

4.7.3 Guidance notes

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

Where a service provider seeks to verify the identity of natural persons who are concerned with a trust on a non-face to face basis, for example, through copy documentation provided by the trustee(s), the service provider ensures that these copies are verified/validated by an independent and reliable third party, such as a notary. Examples of relevant information that the service provider can collect on a trust are a trust deed, letters of wishes and underlying documents.

4.8 Identification and verification of identity of the representative

4.8.1 Statutory requirements

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

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

4.8.2 Regulatory requirements

- A service provider collects identification information of directors, principals (or equivalent) who have authority to operate a relationship or to give the service provider instructions concerning the business relationship, the use or transfer of funds or assets.

- The extent of identification information to be obtained, what to verify, and how to verify it in order to be satisfied as to the identity of a customer's representative, must depend on the risk assessment for that customer.

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

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

4.8.3 Guidance notes

When a natural person acts as a representative of a client, the service provider determines whether that person is authorized to represent the client. This applies, for example, when a natural person acts as a director of a legal entity. When a natural person acts on behalf of a legal entity who is a director of another legal entity, then the chain of representative authority is established. An advisor to the client (for instance a mortgage advisor) is not necessarily the representative.

The signatories to the contract and persons who are in direct contact with the service provider and can bind the client need to be identified. The identity of the representative can be verified in the same way as the client (verification of the identity by the employee of the service provider, by another service provider supervised for AML/CFT purposes, or certification by an independent, reliable third party).

When the authorization to represent the client is not clear from for instance the Chamber of Commerce extract, it is necessary to establish the authorization in another way, for instance by requesting a power of attorney.

A service provider must be alert to the fact that a client can use a so-called 'straw man construction'. These are constructions where people are deployed to carry out transactions in their own name but for the benefit of (criminal) third parties. When the service provider suspects that a client is using a straw man, it will take additional measures to determine whether the person acts for himself or for others. If it is clear that the customer is acting for someone else, this third party also qualifies as a client. If there seems to be a straw man construction purposely to hide a third party, this may be a reason for enhanced customer due diligence or even not entering into or terminating the relationship with the client.

4.9 Identification and verification of identity of the UBO

4.9.1 Statutory requirements

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

Pursuant to Article 19, paragraph 5, of the AML/CFT State Ordinance, a service provider must verify the identity of the UBO using reliable and internationally accepted documents, data, or information or on the basis of documents, data, or information that have been recognized by law in the state of origin of the UBO as a valid means of identification, in such manner that it is convinced of the identity of the UBO.

4.9.2 Regulatory requirements

- When, as part of the identification and verification process of the customer, determining that the UBO is the person that he, she, or it claims to be, a service provider must be satisfied that:
    - the UBO exists - on the basis of appropriate identification information; and

- the UBO is that person - by taking reasonable measures to verify from reliable, independent source documents, data or information, satisfactory confirmatory evidence of that person's identity.

- The extent of identification information to be obtained, what to verify, and how to verify it in order to be satisfied as to a UBO's identity, must depend on the risk assessment for that UBO.

- In assessing the risk of the UBO, the service provider also takes into account and documents the UBO's **source of funds and source of wealth** as well as the fact if there is negative news on the UBO.

- Where a service provider verifies the identity of the UBO(s) on a remote basis, the service provider ensures that these copies are verified by an independent and reliable third party.

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

- **In case of a legal person:** if no natural person is identified as a UBO, the identity of the relevant natural person(s) who hold(s) the position of senior managing official(s) should be established.

4.9.3 Guidance notes

A UBO is a natural person:

1. who holds an interest of more than 25% of the capital interest or can exercise more than 25% of the voting rights in the shareholders meeting of a customer, or can in another way exercise actual control over such a customer;
2. who is beneficiary to 25% or more of the assets of a legal arrangement, including a foundation and a trust, or can exercise actual control over a such a legal arrangement.

Accurate and up-to-date information on the UBO is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. It is essential that the service provider has a full picture of the customer (that is a legal entity), including the natural persons with ownership or control over the customer's affairs, in order to fully assess and mitigate risk and understand the purpose and rationale of the business relationship. The UBO has to be identified and reasonable measures have to be taken to verify the identity so as to know who the UBO is.

Ownership and control
A UBO is the natural person who ultimately owns or controls the customer, and a person on whose behalf the business relationship, transaction or activity is to be or is being conducted.

The definition of UBO extends beyond legal ownership and control and focusses on ultimate or actual ownership and control. Legal ownership means the natural persons who, directly or indirectly, own the legal person.

Control refers to the ability to make relevant decisions within the legal person, including the natural persons who actually take advantage of the capital or assets of the legal person, as well as those who really exert effective control over it (whether or not they occupy formal positions within that legal person). Control through other means may also include the criteria of control used for the purpose of preparing consolidated financial statements, such as through a shareholders' agreement, the exercise of dominant influence or the power to appoint senior management.

When there are indications, for instance from contact with the client or information from open sources, that a person other than the persons holding more than 25% of the shares or interest in the capital, controls the service provider, then also this person is to be designated as the UBO.

A natural person can also indirectly own a legal entity. For example, a person owns a legal entity through another legal entity or a legal arrangement. When a legal entity or legal arrangement owns the legal entity that is the client, the UBOs of that legal entity or arrangement are the UBOs of the legal entity that is the client.

It is therefore necessary to always determine the type of legal entity or arrangement at the top of the structure (the legal entity or arrangement that is directly linked to the UBO) to establish the natural persons who have to be regarded as the UBOs.

Nominees
A nominee shareholder is a natural or legal person recorded in the shareholders' register as the shareholder of a legal person who holds the shares or interest in that legal person on behalf of another. The identity of the true owner is not disclosed on the register. The use of nominee shareholders and nominee directors can provide a means to obscure ultimate ownership and control of a legal person. For example, a natural person may indirectly hold a majority interest in a legal person through the use of nominee shareholders4re who each hold a minimal interest and thereby obscure the identity of the natural person who actually has control.

A nominee shareholder or nominee director would not be considered to have ultimate ownership or control of the customer. The service provider will therefore look through the nominee shareholder or nominee director and identify from whom instructions are being taken by a nominee director and for whom shares or interests are held by the nominee shareholder.

To minimize the risk of providing products or services to a customer using such arrangements, it is critical that legal and beneficial ownership is recorded thoroughly and that appropriate steps are taken to establish the true identity of those persons with ultimate ownership and control of a customer.

Trusts
In the context of a trust or a legal arrangement comparable to a trust, beneficial ownership includes both the natural persons receiving benefit from the trust (for example, a beneficiary, those in a class of beneficiaries or any other person who benefits from the trust) as well as those connected with, or having control over, the trust's affairs, including the settlor(s), trustee(s), and protector(s).

Ultimate control can for instance refer to having the powers to appoint or remove any of the trust's trustees; direct the distribution of funds or assets of the trust; direct investment decisions of the trust; amend the trust deed; or revoke the trust.

The service provider obtains relevant extracts of the trust deed, deeds of amendments and letter(s) of wishes in order to be able to determine the UBOs.

CDD measures regarding the UBO
As required under the AML/CFT State Ordinance, the service provider must identify the UBO and take reasonable measures to verify that person's identity so that it is satisfied that it knows who the UBO is. Verification of the identity serves to protect the service provider from the risk of it relying upon data and information that is fraudulent or misleading, or that does not correspond to the person whose identity is to be verified.

Reasonable measures to verify the identity refer to taking measures that are commensurate with the ML/TF risks which have been identified within the business relationship under the CDD process. This means that the intensity of the verification measures should be tailored to the ML/TF risk of the specific business relationship or transaction. Where the business relationship poses a high risk, the measures will be greater than for low risk relationships.

Determining the nature and scope of the ultimate interest

The service provider also establishes the nature and scope of the ultimate interest held by the UBO in order to know why this person qualifies as UBO.

The verification of the UBO needs to be substantiated by documents from independent sources, such as UBO information from public registers (such as Chamber of Commerce to the extent the information is available), shareholders registers evidencing the interests of the UBO(s) in the top holding, information from other service providers that have performed CDD, declarations by independent and reliable third parties such as an accountant, lawyer or notary. A UBO-declaration signed by the client regarding the ultimate interest is not considered as a document from an independent source.

Verification of the identity of the UBO
The identity of the UBO is verified in such a way that the service provider is convinced that it knows who the UBO is and that the indicated identity matches the actual identity. There are several options to obtain identification data for verification purposes from reliable and independent sources.

For low risk clients with a 100% shareholder an extract from the Chamber of Commerce can be used that states the registration and name of the 100% shareholder.

In case of medium and high risk clients, data and documents from reliable and independent sources need to be used for the verification of the identity of the UBO. This means that the service provider will need to ask the customer more questions and require additional information about the customer's UBO, to ensure that it has accurately verified the UBO's identity. A UBO-declaration signed by the client is not considered as a document from an independent source and no way of accurately verifying the UBO's identity.

The verification of the identity can be done in the same way as for natural persons (see Chapter 4.6).

If the service provider does not receive or have the proper documentation to verify the identity and where instead copy documentation is provided, the service provider must ensure that documentation is obtained according to the abovementioned measures.

If the service provider is not familiar with the form of the identification data obtained to verify the identity, measures should be undertaken to check that the identification data is genuine. In the EU PRADO database (Public Register of Authentic travel and identity Documents Online) the authenticity features of documents may be checked. (https://www.consilium.europa.eu/prado/en/search-by-document-country.html)

Risk factors regarding the UBO
In assessing the customer risk, the service provider takes into account several risk factors related to the UBO, among others:

- The customer requests unnecessary or unreasonable levels of secrecy. For example, the customer is reluctant to share UBO identification data, or appears to want to disguise the UBO.
- The UBO's source of funds and/or source of wealth is unclear or has been generated in a jurisdiction associated with higher ML/TF risk.
- There is negative media on the UBO.

- The UBO is a PEP from a high risk country.
- The settlor and beneficiary of an express trust are the same person.

4.10 Ownership and control structure of the customer

4.10.1 Statutory requirements

According to Article 5, paragraph 2, of the AML/CFT State Ordinance, a service provider must, if a customer is a legal person or arrangement, take reasonable measures that in any case lead to the service provider understanding the ownership and control structure of the customer.

4.10.2 Regulatory requirements

- A service provider's CDD file contains an up-to-datecorporate structure overview for all clients that are legal entities or legal arrangements. The overview includes all shareholdings (legal entities, foundations or trusts and other legal constructions) up to and including the UBO, including percentages of ownership.

- A service provider ensures that the structure of the client is made sufficiently transparent as to understand it. The structure needs to be dated and confirmed by, (the representative of) the client or the (external) auditor of the client or an employee of the service provider. Also, the purpose of the structure should be elaborated upon in the client file and substantiated with documentation from a reliable and relevant source (referral is made to paragraph 4.11). The structure needs to be confirmed periodically (at least once per year in cases of medium and high risk) and/or further to an incident and/or any other 'trigger' event, to make sure the structure in file is still adequate. If a structure has been changed, the ML/TF-risks have to be reconsidered as well vis-à-vis the new structure and persons involved.

4.10.3 Guidance notes

In the case of a customer that is a legal person, a legal entity without legal personality or a legal arrangement, the service provider takes reasonable measures to gain insight into the whole ownership and control structure of the customer. On the basis of the ownership and control structure of the client, the service provider determines whether all persons who qualify as UBO have been identified, their identity verified, and the nature and extent of their interest determined.

It is not necessary to verify the identity of every legal person or legal arrangement within a structure. However, the service provider takes reasonable measures to gather sufficient information on any intermediate entities to allow it to identify those natural persons falling within the UBO definition and to identify whether any intermediate legal entity has issued bearer shares. The service provider also takes into consideration an overall understanding of affiliated companies in the structure. Less transparent or more complex structures require additional evidence on the intermediate entities.

The ownership and control structure of the client has to be transparent and logical. If the ownership and control structure of the client is complicated or opaque, there must be a clear commercial or legal reason for this. To establish the purpose of a structure, the service provider can for instance ask the client to provide a tax advice explaining the purpose of the structure.

The service provider may need to investigate why the client uses a complex structure. Complex structures can be used to hide the origins of proceeds of crime or corruption or can be tax driven. Examples of complex structures are when the entities in the structure are located in several countries, including high risk countries, or when there are entities in the structure with which control and ownership can be concealed. This can for instance be through foundations, trusts, limited partnerships, and similar entities.

Risk factors regarding the control structure
In assessing the client risk, the service provider takes into account several risk factors related to the control structure:

- *The customer's ownership and control structure is not transparent and does not make sense.*
- *The customer's ownership and control structure is complex or opaque, and there is no obvious commercial or lawful rationale.*

- *The customer has a complex structure, for example a structure with entities in high risk countries or a structure with trusts.*
- *There is no sound reason for changes in the customer's ownership and control structure.*
- *The customer issues bearer shares or has nominee shareholders.*
- *The customer is a legal person or legal arrangement that could be used as a personal asset holding vehicle.*

Less transparent and/or more complex structures present higher risks which require additional information or research to determine an appropriate risk classification. A complex structure that appears to be tax-driven, has no rationale, or is designed to disguise the UBO, is a risk indicator.

4.11 Purpose and intended nature of the business relationship

4.11.1 Statutory requirements

According to Article 3, paragraph 1, subsection a, of the AML/CFT State Ordinance, a service provider must establish the purpose and intended nature of the business relationship.

4.11.2 Regulatory requirements

- The service provider ensures that the information with regard to the purpose and intended nature of the business relationship is adequately described in the CDD file of a client and contributes to the risk assessment of the client.

4.11.3 Guidance notes

By gathering information about the purpose and intended nature of the business relationship, the service provider will be able to estimate any risks that may arise from the provision of services to the customer. Therefore, information on the purpose and the intended nature of the business relationship needs to be requested. Part of this information will usually come up during the contacts with the (prospective) client prior to establishing the business relationship. The products provided to the client will to a large extent indicate the purpose of the relationship. Additional queries from the service provider can be aimed at obtaining clarification on the product user or service recipient. For customers not located or residing in Aruba, the service provider should be clear as to why the customer intends to use its services or products in Aruba. For medium and high risk client, the purpose and intended nature of the business relationship should be documented extensively and, especially in cases of high risk clients, substantiated with documents from a reliable and relevant source.

For low risk clients, the nature and purpose of the business relationship can be implicit, for instance, for retail savings accounts. For this type of accounts, the purpose and intended nature of the business relationship is understood to be the legitimate wish of customers to keep funds that are not intended to spend immediately, safe and accessible.

In high risk situations, the service provider also checks what kind of transactions (such as quantity, frequency and size) the client will execute. Several questions can be asked for this:

- Why does the client come to the service provider?
- What does the client expect from the service provider?
- What kind of products and services does the client seek?
- Are these products and services logical for this client / in line with the economic activity of the client?
- What amounts can be expected?
- Are any payments from or to third parties expected?

4.12 Source of funds

4.12.1 Statutory requirements

According to Article 3, paragraph 1, subsection d, of the AML/CFT State Ordinance, a service provider must investigate, where appropriate, the source of funds involved with the transaction or business relationship.

4.12.2 Regulatory requirements

- Before acceptance of a client as well as during the business relationship, a service provider makes a risk-based assessment to determine the extent of the examination into the source of funds. Attention must be given to the possibility that the funds may not originate from a legitimate source.

- The information obtained on the source of funds needs to be reliable, substantive, relevant and the service provider should be able to establish the funds' origin and the circumstances under which the funds were acquired.

4.12.3 Guidance notes

The ability to follow the audit trail for criminal funds and transactions flowing through the financial and non-financial sector is a vital law enforcement tool in ML/TF investigations. Understanding the source of funds and, in higher risk relationships, the customer's source of wealth is also an important aspect of CDD. The service provider needs to be sure that money it receives in the course of providing services to a client is received from a legitimate source.

The source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between the client and the service provider (e.g., the amounts being invested, deposited, or wired as part of the business relationship). Normally it will be easier to obtain this information, but it should not simply be limited to knowing from which service provider it may have been transferred.

The service provider can follow a risk-based approach when establishing the source of funds, being the origin of the particular funds or other assets, which are the subject of the business relationship between the client and the service provider. This means that the information on the source of funds can be established and verified on a risk-sensitive basis depending on the client's risk profile.

Depending on the risk profile of the client, the service provider needs to ensure that the source of funds is logical and evidenced by supporting reliable documentation. The information obtained needs to be substantive and establish an origin or reason for having been acquired. The source of the client's funds must be easily explained, and the explanation must be plausible. A general statement on the source of funds such as 'inheritance', 'investments' or 'generated by own business' **is not sufficient**. The fact that the funds come from another service provider does not mean that the source of funds is not from illicit sources and that no further examination needs to be done.

The level of evidencing depends on the client's risk profile and the evidence should resolve any red flags. In order to establish the plausibility of the source of the funds, the following combinations of indicators are relevant on the basis of which the depth of the examination into the source of the funds is determined, among others:

- the amount involved in the transaction or service;
- the reason given by the client for the origin of the funds;
- age and profession or business activities of the client;
- country of origin or destination of the funds; and

- the product or service provided.

Examples of evidence
The following types of information can be obtained as evidence (non-exhaustive). In case of high risk clients, it would be necessary that this information comes from a reliable, independent source.

In case the source of funds comes from real estate:
- Information publicly available at official property registers or land registers;
- Information on value of the property and rental income;
- Title or transaction, contracts of sale, certified by an independent party such as a notary;
- Confirmation from regulated professionals with knowledge of the client (accountants, lawyers etc.).

In case the source of funds comes from business activities
- Copies of the company's audited annual financial accounts or statements;
- Independent information from company registers;
- Confirmation from regulated professionals with knowledge of the client (accountants, lawyers etc.);
- Account statements.

In case the source of funds comes from sale of an investment or of a company
- Copy of contracts, certified by an independent party such as a notary;
- Account statements or audited financial accounts;
- Substantiated information on price for which investment or company was sold.

In case source of funds comes from an inheritance
- In case the inheritance has been less than 7 years: copies of notarized deed or settlement statement;
- In case the inheritance has been obtained more than 7 years ago, it is possible that the client will not have any information anymore. In this case, the client can be requested to provide additional proof, for instance bank statements over the past years.

In case the source of funds comes from employment income including profits from business activities and investment returns or savings
- Documents confirming salary, tax returns and bank statements.

In case the client has been a client for several years, past services and transactions can provide usefulinsight into the source of funds. Any changes in the clients transaction behavior should be scrutinized and should be incorporated in the risk assessment of the client.

4.13 Updating CDD

4.13.1 Statutory requirements

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

4.13.2 Regulatory requirements

- The service provider keeps CDD data and other information collected current and relevant.

4.13.3 Guidance notes

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

date where it is reviewed and updated on a risk sensitive basis, including where additional factors become apparent.

Events such as the opening of a new account, obtaining a further product or service, or meeting with a customer may also be an occasion to update CDD information.

A comprehensive understanding of the risk presented by a business relationship may only become evident at a later stage following the commencement of the relationship. A service provider may demonstrate that its customer risk assessments remain up to date where its review procedures and its monitoring procedures (Chapter 6) involve consideration as to the ongoing appropriateness of the customer's risk assessment.

It is not necessary to re-verify or re-obtain identification data unless an assessment has been made that the identification data held is not adequate for the assessed risk of the business relationship or there are doubts about the veracity of the information already held.

4.14 Introducing business

4.14.1 Statutory requirements

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

Pursuant to Article 15 and 16 of the AML/CFT State Ordinance, a service provider that relies on an introducer, must ensure that all relevant data, documents and information relating to the CDD conducted by the introducer will be made available to the service provider upon request without delay; and ensure that the introducer has procedures and measures in place to comply with the CDD requirements and to record the relevant CDD information in line with Article 3 and 33 of the AML/CFT State Ordinance, respectively.

In accordance with the Regulation designated introduction countries AML/CFT State Ordinance, the following countries are designated as a country where service providers can be based that introduce customers:

- *the Netherlands;*
- *Curaçao;*
- *Sint Maarten;*
- *United States of America;*
- *Canada.*

4.14.2 Regulatory requirements

- In order to rely on measures that have been conducted by an introducer under Articles 15 or 16, a service provider must obtain sufficient information about the introduced customer:
    - obtain all available and required CDD information from the introducer on the introduced customer in line with requirements for natural persons, legal persons, and trustees set out in Chapters 4.6 and 4.7;

- receive confirmation from the introducer that it will notify the service provider without delay of any material changes in the CDD information on the customer.

- All relevant data, documents and information relating to the CDD conducted by the introducer are provided by the introducer to the service provider on request and without delay, and must be confirmed by the introducer as being a true copy of the original document held on file.

- The service provider should be able to demonstrate that an introducer will provide CDD data, documents and information in relation to introduced customers, without delay where it requires relevant CDD data, documents and information to be made available within 5 working days of a request.

- In the event that an introducer terminates its business relationship with a customer introduced to a service provider, the service provider must require the introducer to provide the service provider with all copies of the relevant data, documents and information relating to the CDD conducted by the introducer. The service provider can also gather its own identification data on the customer.

4.14.3 Guidance notes

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

Introduced business by its very nature has the capacity to be high risk, i.e. relying on a third party to have adequately applied CDD measures to mitigate the risk of the service provider being involved in, or abused for, ML or TF. In this respect, while the service provider is still required to hold sufficient identifying information about its customer and the UBO, the service provider places reliance on a third party to have adequately and appropriately verified the identity of that customer and UBO.

A service provider may rely on introducers to perform elements a, b, and c of Article 3, paragraph 1, of the AML/CFT State Ordinance. This means that a service provider does not need to duplicate certain CDD measures that will have already been conducted by the introducer. The service provider, however, cannot rely on an introducer for the ongoing monitoring of the business relationship and establishing the risk profile of the customer.

Examples of introducers include:

- Insurance broker who arrange for their customers an insurance policy with an insurance company.
- Trust and company service providers who arrange for a bank or investment account to be established in the name of a client company, and not in the name of the trust and company service provider.

Outsourcing arrangements are not included within the scope of this Chapter, as these are distinct from introduced relationships. In an outsourcing arrangement, the customer will have a direct relationship with a service provider and not with the third party carrying on the outsourced activity. Although the third party may have substantial contact with the customer, the customer is a customer of the service provider and not of the outsourced third party. The third party will be carrying on the outsourced activity for the service provider according to the terms of a contract with the service provider (Chapter 3.7 on outsourcing)

A service provider relying on the CDD information by an introducer will proceed carefully. As the responsibility for maintaining an accurate customer file lies with the service provider itself, it is important that the service provider assures itself that the relevant CDD elements have been carried out and that the other service provider has in place adequate AML/CFT procedures and measures. This means that the

procedures of the introducer should be adequate. If a service provider repeatedly accepts customers from the same introducer, it is logical that it assesses the AML/CFT procedures of the introducer in a risk-based way. In the case of new business alliances, the AML/CFT procedures should always be requested for assessment.

When relying on an introducer, the service provider will also look into the risks posed by this introducer, by assessing factors such as:

- the nature of the business conducted by the introducer;
- the stature and regulatory track record of the introducer;
- the adequacy of the AML/CFT framework and the AML/CFT supervisory regime in place in the jurisdiction in which the introducer is based;
- the adequacy of the AML/CFT measures in place at the introducer and whether relationships are conducted by the introducer on a face to face basis;
- previous experience gained from existing relationships connected with the introducer;
- the extent to which the introducer itself relies on third parties to identify its customers and to hold evidence of identity or to conduct other CDD measures, and whether such other third parties are regulated.

When the service provider determines that there is a higher risk involved in the introducer, the service provider may conduct (or commission from an external expert or auditor) periodic sample testing of the adequacy of the introducer's AML/CFT policies and procedures, whether through onsite visits, or through requesting specific CDD information and/or copy documentation to be provided.

Where an introduced business relationship presents a high ML/TF risk, the service provider should consider whether it is appropriate to rely solely upon the information provided by the introducer or whether additional CDD information and documentation is required.

Even though the introducer should keep (copies of) the relevant documents available to provide to the service provider at its first request, it is more practical to make the information available to the service provider immediately on introduction, because the service provider must itself possess the data and is also itself responsible for compiling the risk profile of the customer, for which it requires the correct information. If the introducer cannot provide the information upon request and without delay, the service provider will need to conduct CDD itself.

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

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

4.15 CDD when acquiring a business or block of customers

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

4.15.1 Regulatory requirements

- Before acquiring a business with existing business relationships or a block of business relationships, a service provider must undertake sufficient due diligence on the vendor to establish the level and appropriateness of CDD information and records held in relation to the customers of the business to be acquired.

- A service provider should only rely on the CDD information and records previously obtained by the vendor where the following criteria are met:
  - the vendor is subject to AML/CFT requirements and to supervision for compliance with AML/CFT requirements; and
  - the service provider has assessed that the vendor's CDD measures are satisfactory. This assessment must either involve sample testing, an assessment of all relevant CDD information for the relationships to be acquired, or consideration of the findings of any relevant reviews by the CBA, an overseas regulatory body (where applicable) or other third party.

- A service provider must obtain from the vendor the CDD information and records held for each customer acquired.

- Where the vendor is not subject to AML/CFT requirements and to supervision for compliance with AML/CFT requirements or where deficiencies in the vendor's CDD measures are identified (either at the time of transfer or subsequently), an acquiring business must determine and implement a program to apply CDD measures on each customer and to remedy deficiencies.

- The service provider must agree its remediation program with the CBA.

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

5. SDD and EDD

5.1 Simplified customer due diligence

5.1.1 Statutory requirements

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 service provider domiciled in Aruba, provided it is supervised by the Bank or another public legal person;*
- *a financial service provider with domicile outside Aruba, provided it is subject to the internationally accepted standards for the prevention and combating of money laundering and terrorist financing, and it is supervised effectively with regard to the compliance with these standards;*
- *public limited companies and comparable entities, which are subject to statutory disclosure requirements, and the shares of which are traded on recognized stock exchanges as designated by regulation of the Minister;*
- *public limited companies of which all shares are held by the State;*
- *the State and other public legal persons established in Aruba;*
- *public legal persons established and active in other parts of the Kingdom.*

Pursuant to Article 10, paragraph 1, subsection b, of the AML/CFT State Ordinance simplified CDD measures may be applied when clients carry out a transaction or enter into a business relationship related to:

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

Pursuant to Article 10, paragraph 2 of the AML/CFT State Ordinance, a service provider shall collect sufficient data to be able to establish whether the first section applies to a client.

Pursuant to Article 10, paragraph 3 of the AML/CFT State Ordinance, the first section shall not apply, if the client, business relationship or a transaction subsequently carries a higher risk for money laundering or terrorist financing of if there are indications that the client is involved with money laundering or terrorist financing.

In accordance with the Regulation on designated stock exchanges AML/CFT State Ordinance, a recognized stock exchanges as referred to in Article 10, first paragraph, letter a, under 3, of the AML/CFT State Ordinance are the stock exchanges in:

- *Amsterdam, New York, Lisbon, Brussels, and Paris, held by NYSE Euronext;*
- *Frankfurt, held by Deutsche Bïrse;*
- *London, held by London Stock Exchange;*
- *Toronto, held by Toronto Stock Exchange;*
- *Tokyo, held by Tokyo Stock Exchange.*

5.1.2 Regulatory requirements

- The service provider should keep sufficient evidence in the customer file that SDD may be applied, for instance printouts from reliable websites.

5.1.3 Guidance notes

In cases of established low risk, SDD may be performed on a client. When SDD is applied, it is generally acceptable to rely on information provided by the client or information from open sources or registries.

The service provider should also pay attention to the fact whether there are indicators that could increase the risk, for instance by examining if there is adverse information on the customer, including on the UBO (in those cases where there is a UBO).

If SDD has been applied, it is important to periodically check the activities and risk profile of the client to determine that SDD can still be applied. This means that some monitoring of these business relationships is always necessary to assess whether the business relationship is actually being used for the reasons provided. It can also follow from an event driven review that SDD cannot be applied anymore. When there are facts or circumstances which lead to an increased ML/TF risk or other reasons to re-assess the risk profile of the client CDD or EDD has to be carried out.

As described in Chapter 4.13, a service provider is also required under Article 7 of the AML/CFT State Ordinance to keep the information up-to-date. Accordingly, the service provider needs to gather sufficient data to assess whether a customer still meets the requirements for the SDD. For instance, the service provider may request an extract from the trade register, entries in public registers or other public listings.

Even though the AML/CFT State Ordinance states that SDD can be applied to the ultimate beneficiaries of accounts kept for a designated non-financial service provider intended solely for the keeping of money for third parties, the key word here is **"solely"**. A client account of a designated non-financial service provider (lawyer, notary or similar professional) is a bank account set up in the name of the professional but only intended to hold funds of clients of the designated non-financial service provider in "trust" or for a purpose designated by the client. A client account is segregated from any other bank account held in the name of the professional. No funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the professional is required to account for these funds. In an case, such an account may not be used by the service provider or the client as a regular bank account.

The use of client accounts has been identified as a potential vulnerability, as it may be perceived by criminals as a means to either integrate tainted funds within the mainstream financial system or a means by which tainted funds may be layered in such a way to obscure their source, with fewer questions being asked by a service provider because of the perceived respectability and legitimacy added by the involvement of the legal professional. **If a service provider has any indications that such a client account is also used for other transactions than for which it is intended and without any legal basis, SDD can no longer be applied and CDD or even EDD has to be applied to the persons using the client account of a designated non-financial service provider.**

According to the AML/CFT State Ordinance SDD measures may be applied when it concerns a foreign financial service provider that it is subject to the internationally accepted AML/CFT requirements and is supervised with regard to the compliance with these requirements. The service provider may demonstrate that this, if the service provider has considered the following:

- whether or not the jurisdiction where the foreign financial service provider is based, is a member of the FATF, a member state of the EU, a member of the EEA, or part of the Kingdom of the Netherlands;
- whether the legislation and other requirements in place in that jurisdiction comply with internationally accepted AML/CFT requirements (i.e. the FATF Recommendations);
- 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.

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;
- A service provider established by law of Aruba (e.g. CBA, AZV, SVB).

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);
- A legal entity established by law of the Netherlands, Curaçao or St. Maarten (e.g. DNB, CBCS).

5.2 Enhanced customer due diligence

5.2.1 Statutory requirements

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 ML/TF risk. Enhanced CDD must be performed prior to the business relationship or the transaction as well as throughout the course of the business relationship, in any case in the following situations:

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

5.2.2 Regulatory requirements

- The service provider performs enhanced due diligence when a business relationship or transaction, by its nature, represents a higher risk.

5.2.3 Guidance notes

EDD should be performed when a business relationship or transaction, by its nature, represents a higher risk. On the basis of the risk assessment and risk profile established, prior to entering into the business relationship or conducting a transaction, it is determined by the service provider whether this higher risk manifests or could manifest itself.
A more extensive examination is carried out during the EDD process. This means additional and more comprehensive information has to be requested and assessed about, among other things, the client's business activities, the source of the client's (and UBO's) funds and wealth, the purpose for the corporate structure and the underlying reason for the service.

In the case of EDD, the service provider should always verify the information provided by the customer by way of independent and reliable sources. Where relevant, the client is asked to provide this information from reliable and independent sources to substantiate the information provided. This may include property deeds, sales deeds, annual accounts, financial information, information from the tax authorities,

information from trade registers or other registers. Also, the UBO's source of funds and source of wealth should be scrutinized even more than in a case regular CDD is performed

Source of funds is the origin of the particular funds or other assets which are the subject of the business relationship between the client and the service provider. Source of wealth refers to the origin of the UBO's entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the UBO acquired such wealth. The service provider assesses if the sources are from a legitimate origin. Source of funds and wealth can be established through a combination of sources, such as publicly available information, information provided by the client combined with evidence from a reliable, independent source. A declaration only from the UBO('s) will not suffice.

A more extensive investigation will also take place via open sources or, where possible, by obtaining information from service providers in the client's country of origin. Such addition investigation may relate to the reputation of the customer or the UBO, but also of persons with whom they are associated.

Enhanced CDD measures include:

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

Client risk factors

Client risk is one of the factors that will be taken into account in assessing whether a client is a higher risk. Examples of such risks are:

- The client has a complex ownership and control structure, for example a structure with entities in high-risk countries or where trusts are present.
- The client has an ownership and control structure that is not transparent, tax driven, or has no obvious commercial or lawful rationale.
- There is no sound reason for changes in the customer's ownership and control structure.
- The client is a legal person or arrangement that could be used as a personal asset-holding vehicle.
- The client has nominee shareholders or has issued bearer shares.
- The client uses a so-called 'straw man construction'. These are constructions where people are deployed to carry out transactions in their own name but for the benefit of (criminal) third parties.
- The client is active in a sector that is associated with a higher level of corruption, such as commercial real estate, construction, sports, pharmaceuticals and healthcare, arms trade and defense, extraction industry or public procurement.
- The client is active in a sector where a lot of cash is available, such as ambulatory trade, scrap dealers, car repair companies, massage parlors, betting and gambling-related activities.
- The client is part of an industry that has shown in practice that it may serve as a cover for criminal activities, such as the hospitality industry, the sex industry, modern slavery, workforce exploitation.
- The client has unclear business activities or is frequently changing business activities.

- The customer requests unnecessary or unreasonable levels of secrecy. For example, the customer appears unusually reluctant to share identification data, or appears to want to disguise the UBO.
- The customer (or their advisors) seeks to pressurize or influence the service provider staff to cut corners or postpone CDD checks, knowingly making it difficult for ML/TF risks to be properly evaluated. For example, transaction turnaround times may be unexpectedly tightened, or CDD and documentation requests may be refused (without clear justification) as unreasonable or beyond market practice.
- The client's source of funds or source of wealth is unclear or has been generated in a jurisdiction associated with higher ML/TF risk.
- Client/UBO is refusing to supply relevant information on its source of funds and wealth;
- Client/UBO is providing proof documents of source of funds and wealth, which are noticeably inconsistent with that of comparable clients or clients of comparable size with the same activities;
- There is negative/adverse news on the client or the UBO of the client.
- The client or UBO of the client is on a sanctions list (for further obligations on freezing funds, see Chapter 11).
- The client or the UBO of the client is a PEP (for further obligations on assessing the PEP risk and enhanced measures, see Chapter 5.5).

Product, services or transaction risk factors
Another factor that is included in the assessment whether a client is high risk is the product or service requested or the transaction. Especially when this service falls outside the usual service for these or similar clients, the service provider assesses whether the client should be considered as high risk. Examples of such risks are:

- The requested service is not in line with the economic activity of the client.
- Payment for the service is received from unknown or unassociated third parties.
- Services or transactions are related to petroleum, weapons, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious interest or with great scientific value, as well as ivory and protected species.

Delivery channel risks
The delivery channel is the way clients are accepted or services are delivered to clients. The way a client comes to the service provider can also be a risk-increasing factor. Examples are:

- The (UBO of the) client is introduced by an unknown third party.
- The (UBO of the) client is introduced by a party from a high risk country.
- There has never been personal contact with the (UBO of the) client.
- Client contact may only be conducted via a third party.

5.3 High risk countries and jurisdictions

5.3.1 Statutory requirements

Pursuant to Article 13, paragraph 1, of the AML/CFT State Ordinance, a service provider must pay special attention to:

- *business relationships and transactions with natural persons, legal persons, trusts and comparable entities originating from countries or jurisdictions that do not, or insufficiently comply with the internationally accepted AML/CFT standards;*
- *all complex and unusual large transactions and to all unusual patterns of transactions, which have no apparent economic or lawful purpose.*

If a service provider can reasonably suspect that there is such a transaction as mentioned above it must, pursuant to Article 13, paragraph 2, of the AML/CFT State Ordinance, examine the background and the purpose of such transactions and record its findings in writing.

In accordance with Article 13, paragraph 3, of the AML/CFT State Ordinance, these findings must be kept for at least ten years.

5.3.2 Regulatory requirements

- A service provider must treat countries and jurisdictions listed in the FATF statements (circulated by the CBA), highlighting jurisdictions which do not or insufficiently apply the FATF Recommendations or which are the subject of international countermeasures, **as countries and jurisdictions that do not or insufficiently apply the internationally accepted AML/CFT standards.**

5.3.3 Guidance notes

Special measures need to be taken for customers and their UBOs who live or are established in high risk countries. For example, additional information is gathered about the purpose and nature of the business relationship, the origin of the funds used in the business relationship or transaction and the source of wealth of those customers and UBOs. The details of these customers are also regularly updated, and the business relationship and associated transactions are subjected to additional monitoring. Additional information is also gathered about the background to and reasons for the transactions.

Country risk factors
When identifying the risks associated with countries and geographical areas, the following factors will be taken into account in determining whether the client is high risk:

- The client or the UBO of the client is established or is resident in a high risk country.
- The client is active or has business activities in a high risk country.
- The funds related to the products provided by the service provider come from or are sent to a high risk country.

The following are sources that may be used to determine the risk level of a country.

Links to relevant websites:

- European regulations: https://eur-lex.europa.eu/homepage.html
- EU information on AML/CFT including on high risk countries: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en
- FATF high risk countries: http://www.fatf-gafi.org/countries/#high-risk
- EU sanctioned countries: https://www.sanctionsmap.eu/#/main
- UN sanctions: https://www.un.org/sc/suborg/en/sanctions/information
- Transparency International: https://www.transparency.org/cpi2018#results

5.4 New technologies and non-face to face

5.4.1 Statutory requirements

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

5.4.2 Regulatory requirements

- Where a business relationship is established or occasional transaction conducted remotely, or where the identity of a natural person is to be verified using documentary evidence when the natural person is not physically present, a service provider must perform an additional check to reduce the risks.

- The service provider shall, before adopting and using a new or developing technology for a new or pre-existing product, ensure that its business risk assessment has identified and assessed the risks arising from the technology's use or adoption.

- The risk assessment of a new technology must include an assessment of the ML/TF risks and vulnerabilities inherent in the use or adoption of the technology in order that appropriate controls can be implemented. This includes evaluating the technology itself, together with the anticipated use of the technology and the threats posed by this use.

5.4.3 Guidance notes

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

- relationships established by natural persons through the post, by telephone or via the internet; and
- where identification information is provided through a trustee on persons who are concerned with a trust, or by a company on the persons who are its UBOs.

There is a higher risk in cases where the customer is not physically present for the identification and verification of identity.

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

Additional checks to reduce the risks may include:

- Requiring the first payment for the product or service to be drawn on an account in the customer's name at a bank, provided the bank is subject to the internationally accepted AML/CFT requirements and it is supervised with regard to the compliance with these requirements.
- Electronic methods of verification, for instance any secure, remote or electronic measures can also be used as long as these measures provide safeguards that the verification is based on information from a reliable and independent source. This should be done in line with processes established by the service provider for, for instance, video conferencing.

Since the customer's identity must be verified before entering into the business relationship, the service provider should ensure that the first payment precedes or coincides with the commencement of the business relationship with and the provision of professional services to the customer. The customer may make deposits into the account concerned, but the service provider will keep the account blocked and will not allow the customer to withdraw or transfer funds before the CDD process has been completed.

In the case of joint accounts, the second account-holder's name is not always stated on the transfer of funds. A (printout or copy of a) bank statement or a copy of the bank card may then be requested in order to verify the full title to the account. In this case, it is important that there is sufficient certainty that the customer has provided proof of his/her identity elsewhere and can thus be traced by a paper trail.

A service provider can also take other measures as long as the higher risk of the customer's not being physically present is mitigated. To that end, the service provider can request supplementary documents, data or information. This is supplementary documentation which must be provided in addition to items such as a copy of proof of identity, or a combination of several documents. The service provider will assess the documents submitted for authenticity. The service provider may for example ask the customer to have copies of the documents authenticated.

New technologies
The risk assessment of a technology does not have to include a highly technical, comprehensive report on the specifications and functionality. The objective of the risk assessment is to evaluate the ML/TF risks and vulnerabilities inherent in the use of the technology and to identify the controls necessary to mitigate and limit the service provider's exposure. It will be necessary that, if the service provider decides to proceed with the adoption or use of a new or developing technology for a new or pre-existing product, the Board/senior management is informed of and approves the risk assessment.

5.5 PEP

5.5.1 Statutory requirements

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

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

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

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

5.5.2 Regulatory requirements

- A service provider shall make a determination as to whether the customer or UBO is a PEP, and if so, whether he or she is a foreign PEP, a domestic PEP or an international organization PEP
    - "foreign PEP" is a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, in a country or territory other than Aruba;
    - "domestic PEP" is a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, within Aruba; and
    - "international organization PEP" – a natural person who is, or has been at any time, entrusted with a prominent function by an international organization.

- The service provider will in any case consider the persons who are or have been charged with the following prominent political functions as PEPs:
    - heads of state, heads of government, ministers and state secretaries;
    - members of parliament;
    - members of the governing bodies of political parties;
    - members of supreme courts, constitutional courts and other high tribunals that render judgments that generally are not open to appeal;
    - members of courts of auditors and of the board of directors of central banks;
    - ambassadors and chargés d'affaires;
    - high-ranked army officers;
    - members of executive, management or supervisory bodies of state-owned companies;

    - directors, deputy directors and members of the board or equivalent function of an international organization.

- No public function referred to in points above shall be understood as covering middle-ranking or more junior officials.

- The service provider will also consider **direct family members and close associates of the persons who are or have been charged with the listed prominent political functions as PEPs**. For this purpose
    - family members include the following:
        - the spouse, or a person considered to be equivalent to a spouse, of a PEP;
        - the children and their spouses, or persons considered to be equivalent to a spouse, of a PEP;
        - the parents of a PEP.
    - close associates mean:
        - natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
        - natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

- PEPs should **always** be subject to EDD measures.

- If the customer or UBO becomes or proves to be a PEP during the course of the business relationship, the service provider must take the EDD measures **as quickly as possible**.

5.5.3 Guidance notes

Corruption inevitably involves serious crime, such as theft or fraud, and is of global concern. The proceeds of corruption are often transferred to other jurisdictions and concealed through private companies, trusts or foundations, frequently under the names of relatives or close associates of persons with a political function. Indications that a customer may be connected with corruption include excessive revenue from “commissions” or “consultancy fees” or involvement in contracts at inflated prices, where unexplained “commissions” or other charges are paid to third parties.

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

By their very nature, investigations involving the proceeds of corruption generally gain significant publicity and are therefore very damaging to the reputation of both businesses and jurisdictions concerned. This is in addition to the possibility of criminal charges. Relationships with PEPs therefore present increased risks due to the possibility that individuals holding a prominent political position may misuse their power and influence for personal gain or advantage, or for the personal gain or advantage of close family members and close associates. Such individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption. For similar purpose, PEPs may also seek to use their powers and influence to gain representation and access to, or control legal entities. Therefore, PEPs are treated with heightened scrutiny.

PEP status itself does not, of course, incriminate natural persons. Refusing a business relationship with a person simply on the basis of determination that he or she is a PEP is contrary to the letter and the spirit

of the law and of the FATF recommendations. It is not necessary to exclude transactions with or services to PEPs. It will, however put the customer into a high risk category.

EDD measures
Institutions will have in place risk-based procedures and measures to check if a customer or the UBO of a customer is a PEP. This review is carried out both on acceptance and periodically. To determine whether a particular customer or UBO is a PEP, a service provider may consult public sources. The service provider can also seek confirmation from a customer or UBO as to whether they hold, or have held, a prominent public function. For service providers with an international customer base, it may be efficient to use lists provided by recognized commercial organizations.

Under the AML/CFT State Ordinance, in case the client or the UBO of the client is a PEP, the following measures are necessary:

- Obtain senior management approval for establishing or continuing a business relationship with the PEP.
- Establishing the source of wealth and source of funds that are involved in business relationships or transactions with the PEP.
- Conduct enhanced monitoring of the business relationship.

The depth of the EDD measures vary depending on the risk profile of the customer or UBO who is a PEP. Because the “PEP-risk” emanates from a corruption risk, the “corruption perception index” of Transparency International can be used to determine the country risk of a PEP.

Risk factors are:

- If the PEP is still in function, has been out of function less than five years or although being out of function for more than five years can still exert political influence.
- If the PEP is a PEP because of the political function or because of the relation with a political figure (relative or close associate).
- If the PEP is from a jurisdiction associated with a higher ML/TF or corruption risk, or a country under EU or UN sanctions.
- If there is any negative news/adverse media on the PEP.

The decision to enter into a business relationship with a PEP or to conduct a transaction for a PEP should be taken or approved by persons authorized by the service provider to do so. This also applies to a decision to continue a relationship with a customer who becomes a PEP. Such approval is granted by senior management.

For all PEPs, the source of funds and source of wealth need to be established using reasonable measures. Source of funds is the origin of the particular funds or other assets which are the subject of the business relationship between the client and the service provider. Source of wealth refers to the origin of the PEP’s entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the customer would be expected to have, and a picture of how the PEP acquired such wealth. Based on these measures, the service provider assesses if the sources are from a legitimate origin. An analysis of the PEP’s source of funds and wealth is necessary for assessing and mitigating the risk of getting involved in (possible) money laundering or terrorist financing. The service provider needs to ensure that any funds it receives in the course of providing services to a client or UBO who is a PEP is received from a legitimate source. Source of funds and wealth can be established through a combination of sources, such as publicly available information, information provided by the client combined with evidence from a reliable, independent source.

Red flags related to source of funds and wealth
To be considered when assessing and valuating the source of funds and wealth (non-exhaustive):

- Client/UBO is refusing to supply relevant information on its source of funds and wealth;
- Information available on the client (profession, age, income) does not match with information provided on the source of funds and wealth.

- Client/UBO is providing proof documents of source of funds and wealth, which are noticeably inconsistent with that of comparable clients or clients of comparable size with the same activities;
- Client/UBO is providing information on his/her funds and wealth with documents from high risk jurisdictions, or countries with weak AML/CFT regulations, or known for organized crime, drug trafficking, etc.
- Client/UBO is providing proof documents of source of funds and wealth, which show frequent inconsistencies and are lacking rationale;
- Client/UBO is providing information on his/her funds and wealth through complex, non-transparent structures (e.g. incl. offshore structures, trusts, bank accounts in high risk countries), with the (deliberate) intention for the information to remain unclear.

Institutions that have PEPs as customers may also set up their internal procedures for enhanced ongoing monitoring of these business relationships in a risk-based manner. The ongoing monitoring process generally consists of both periodic review and transaction monitoring. In addition, there might also be occasion for an event driven review. The review focuses on determining whether anything has changed in the risk profile of the PEP. The periodic review will be properly documented. Not documented is considered as not executed. Aspects to consider when reviewing the client are any changes in the role and position of the PEP, whether the PEP is still in function, and also any changes in the involvement of the PEP in the transaction or client structure.

Transactions of PEPs should be monitored more closely. Transactions of the past period need to be reviewed to examine if the transactions fall within the expected pattern. This transaction monitoring process includes assessing, on an ongoing basis, whether the transactional activity of a business relationship with the PEP is consistent with the risk profile of that relationship, the nature of the service or product provided and the service provider's understanding of the customer's and UBO's source of funds and wealth. There could be specific PEP scenarios in the applicable transaction monitoring systems, and for example different thresholds.

In case there is any adverse news concerning an existing client or UBO of a client that is a PEP, the service provider initiates an event driven review.

5.6 Correspondent Banking

5.6.1 Statutory requirements

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

- *it gathers sufficient information about the respondent bank to understand fully the nature of the respondent's business and the reputation of the respondent bank and the quality of supervision exercised over this bank, including information about any investigations regarding ML/TF or supervisory measures taken;*
- *it assesses the respondent bank's AML/CFT procedures and measures and ascertains that these procedures and measures are adequate and effective;*
- *the respective AML/CFT responsibilities of each bank are recorded in writing.*

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

If a correspondent banking relationship involves the maintenance of "payable-through accounts", a service provider, being a bank as meant in the SOSCS, must, pursuant to Article 17, paragraph 3, of the AML/CFT State Ordinance, ascertain that the respondent bank has identified its customers that have direct access to these payable-through accounts, and that it has verified their identity in accordance with the internationally accepted standards for identification and identity verification. The service provider must

also ascertain that the respondent bank is able to provide all relevant customer identification information upon request.

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

5.6.2 Regulatory requirements

- The EDD measures in relation to a business relationship or occasional transaction which is a correspondent relationship, also apply to similar relationships that involve the provision of services, which themselves amount to financial services or facilitate the carrying on of such business, by one financial service provider to another.

- A financial service provider must inform the CBA immediately after senior management has decided to enter into a correspondent banking relationship.

- A financial service provider, being a respondent financial service provider must inform the CBA immediately of any termination or restriction of a correspondent relationship. The reason for the latter must be included in the notice to the CBA.

- In the event of termination or restriction of a correspondent relationship the financial service provider should inform the CBA **immediately therof, as well as regarding** how the termination or restriction will affect the financial service provider. Furthermore, an action plan needs to be presented regarding how any negative impact will be addressed.

5.6.3 Guidance notes

Correspondent banking is a term given to the provision of services by one bank or other financial service provider (the “correspondent”) to another bank or financial service provider (the “respondent”) for the benefit of the customers of the respondent. As a result, the correspondent indirectly makes its services available to the customers of the respondent business; in doing so, the correspondent potentially exposes itself to additional risk.

The service provider exercises due care when entering into correspondent relationships. A bank or other financial service provider should obtain a good picture of the other bank or financial service provider with which they enter into correspondent relationships. In a correspondent relationship, a bank or other financial service provider in reality acts as an agent for another bank or financial service provider by effecting payments or performing other services for a customer of the correspondent. To avoid the or financial service provider being misused by means of these transactions for money laundering or terrorist financing purposes, it is important that a number of conditions are observed.

A financial service provider that is a correspondent gathers sufficient information about the respondent to understand fully the nature of its business. The financial service provider can therefore obtain information concerning the following:

- the geographic location of the customer base;
- the general nature of the customer base;
- the nature of the services which the respondent provides to its customers;
- whether relationships are conducted by the respondent on a non-face to face basis; and
- the extent to which the respondent relies on third parties to identify and hold evidence of identity or to conduct other CDD measures on customers.

A financial service provider that is a correspondent determines from publicly available information the reputation of the respondent, including whether it has been subject to an ML/TF investigation or regulatory action. It can also determine the reputation of a respondent by assessing its stature, using public sources, such as the Bankersalmanac.com Due Diligence Repository.

A financial service provider that is a correspondent determines the quality of supervision exercised over a respondent by considering the independent assessments of that respondent's jurisdiction's AML/CFT framework, such as those conducted by the FATF, the World Bank and the IMF.

It is particularly important to be alert to the potential use of a correspondent account by (unidentified) third parties (transit account or payable-through account), in other words when a customer of the foreign financial service provider has direct access to the account held by that bank or other financial service provider in Aruba. The reason why close attention needs to be paid to this category of accounts is that in reality it entails the provision of services at a distance. The correspondent itself usually has no relationship with the parties involved in the transaction and thus has less opportunity – or no opportunity at all – to verify the source of the funds flows. The FATF defines a payable-through account as a correspondent account that is used directly by third parties to transact business on their own behalf. If a foreign financial service provider gives its customers direct access to the account held with the bank or other financial service provider in Aruba, the foreign financial service provider has conducted equivalent CDD on those customers and can provide relevant information about them to the Aruban bank or financial service provider.

The financial service provider that is a correspondent satisfies itself as to the adequacy of a respondent's CDD measures, and its ability to provide relevant CDD information and documents on request where it obtains a written assurance from the respondent to this effect. The correspondent may also ensure the adequacy of the CDD measures of the respondent and its ability to produce information and documentation on request by periodically requesting relevant CDD information and documents.

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

6. Ongoing monitoring

6.1 Introduction

The ongoing monitoring of a business relationship, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing CDD measures. It is important that the service provider understands a customer's background and is aware of changes in the circumstances of the customer throughout the life-cycle of a business relationship.

Monitoring allows the service provider to gain and maintain an insight into the nature and background of customers and their (financial) conduct. Among other things, the purpose of this monitoring is to detect any changes in the transaction pattern and the possible occurrence of situations that present a higher ML/TF risk.

There are two elements to effective ongoing monitoring:

1. Customer monitoring: the periodic review of the customer to ensure that it continues to have a good understanding of its customers. This is achieved through maintaining relevant and appropriate CDD and applying appropriate ongoing due diligence;
2. Transaction monitoring: the monitoring of transactions and other customer activity which occur on a day-to-day basis within a business relationship and which need to be monitored to ensure they remain consistent with the service provider's understanding of the customer and the product or service it is providing to the customer.

6.1.1 Statutory requirements

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

Pursuant to Article 13, paragraph 1, of the AML/CFT State Ordinance, a service provider must pay special attention to all complex and unusual large transactions and to all unusual patterns of transactions, which have no apparent economic or lawful purpose.

If a service provider can reasonably suspect that there is such a transaction, it must, pursuant to Article 13, paragraph 2, of the AML/CFT State Ordinance, examine the background and the purpose of such transactions and record its findings in writing. In accordance with Article 13, paragraph 3, of the AML/CFT State Ordinance, these findings must be kept for at least ten years.

6.1.2 Regulatory requirements

- A service provider must establish appropriate ongoing CDD procedures that scrutinize the activity and transactions of its customers.

- The procedures set out the frequency with which and way in which the customer data are updated and how the periodic reviews of the customer's risk profile are conducted and kept up to date. **This includes periodic screening against sanctions lists, PEP lists and reliable open sources.**

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

- The monitoring procedures must provide for the identification and scrutiny of:

- Transactions that are deemed unusual transactions based on the subjective and objective indicators;
- Complex or unusually large transactions;
- Unusual patterns of transactions or transactions which have no apparent economic or lawful purpose;
- Business relationships and transactions connected with jurisdictions which do not, or insufficiently, comply with the international AML/CFT standards, including but not limited to the FATF Recommendations;
- Business relationships and transactions connected with jurisdictions which are the subject of Aruban, UN, US or EU sanctions;
- Business relationships or transactions that are designated by Article 11 of the AML/CFT State Ordinance to by its nature entail a higher ML/TF risk;
- Any other activity, the nature of which, causes the service provider to regard it as particularly likely to be related to ML/TF;
- Products and transactions are susceptible to anonymity.

- The monitoring procedures must:
  - Involve a service provider applying its understanding of its business (i.e. the outcome of its business risk assessment - Chapter 3.3) to determine the nature of usual activity and its expectations for unusual and higher risk activity and transactions;
  - Be designed to result in the identification of unusual and higher risk activity or transactions;
  - Require that, in particular, special attention is paid to specific higher risk activity and transactions;
  - Require the examination of any unusual or higher risk activity or transaction to determine the background and purpose of the activity or transaction;
  - In connection with the above examination, involve the collection of additional information (where appropriate);
  - Establish whether there is a rational explanation (an apparent economic or visible lawful purpose) for the higher risk or unusual activity or transaction, and document these findings in writing; and
  - Result in appropriate action being taken as a result of the findings of the above procedures.

6.1.3 Guidance notes

During the customer acceptance process, the service provider draws up a **customer risk profile (1)** and **expected transaction profile (2)**. For the duration of the relationship it is important that the service provider **checks periodically** whether the customer still fits his/her risk profile and whether the transaction profile is in line with expectations. The service provider may tailor the frequency and intensity of the ongoing CDD measures to the customer's risk assessments.

Periodic review
Ongoing CDD ensures that the service provider is aware of any changes in the development of a business relationship. The extent of the ongoing CDD measures can be determined on a risk-sensitive basis. However, the service provider must be aware that as a business relationship develops, the risks of ML/TF may change.

Ongoing CDD is to be conducted on a periodic basis in line with the customer's risk assessments or where a trigger event occurs in the intermediate period. Examples of trigger events could include a material change in the way that the business of the customer is conducted, changes to a customer's or UBO's circumstances, information on negative news or incidents.

The service provider compiles a risk profile of the customer based on the CDD information. This risk profile is dynamic and can therefore change over time. A review serves to determine whether the customer still meets the defined risk profile. To that end, the service provider periodically updates all customer and UBO data, including the customer's risk profile. The basic principle is that the frequency and depth of the review depend on the risks presented by the customer.

In low risk relationships, occasions such as the opening of a new account or the purchase of a further product may present a convenient opportunity to review the CDD information held. For high risk relationships more frequent reviews and updating CDD information on a more regular basis are necessary.

During the periodic review the service provider, at a minimum, verifies and confirms that the information about the client, UBO, representative, structure, nature and purpose of the relationship and source of funds is still accurate and up-to-date, and in conformity with the requirements of the AML/CFT State Ordinance. The service provider also checks whether there are external signals (bad press/adverse news, incidents) that could give rise to a change in the risk profile of the client. Checks against sanctions lists and PEP lists are in any case periodically performed, as well as during the periodic review of the customer. The periodic review also includes checking the transaction behavior of the customer to determine whether unusual activities have taken place, for instance if payments have been received where they would normally not be expected.

Event driven review
In case the products and services change for a customer, the service provider can perform an **event driven review** (EDR) of the customer. An EDR will generally be similar as the periodic review. The service provider will check whether the information on the client, UBO, representative, structure, nature and purpose of the relationship, source of funds is still accurate and up-to-date. However, focus during the EDR can be the reason for the review and it will especially be assessed whether that occurrence can be mitigated sufficiently.

EDR will also be done when there are signals or trigger events. Signals or triggers can relate to the customer, for instance bad press or other adverse information, a change in the client's activities, corporate structure or transaction behavior. The review based on a signal or trigger will especially focus on that occurrence in order to determine whether the risk profile of the customer needs to be amended.

It is also possible that an external trigger can cause EDR, for instance the fact that the country risk changes or the AML/CFT Law. Also, in these cases the client risk profile will be re-assessed.

Transaction monitoring
Transaction monitoring involves the application of scrutiny to large and unusual or complex transactions, as well as to patterns of transactions or activity, to ensure that such transactions and activity are consistent with the service provider's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.

A service provider can tailor its transaction monitoring process to the nature and size of its business as well as its activities and complexity, in line with the risks identified within its business risk assessments. The characteristics of its customer-base and the complexity and volume of expected transactions or activities are also factors to take into account.

An effective transaction monitoring system requires a service provider to identify unusual and high risk activity and to determine whether there is a rational explanation for the activity or transactions identified. The scrutiny of the customer's activities and transactions may involve requesting additional CDD or other information from the customer.

The service provider can generally only determine if it has reasonable grounds to suspect that ML/TF is occurring if it can assess whether a transaction or activity falls outside the normal expectations for a particular business relationship. Particular attention should be paid to high risk customers (for example, those involving PEPs), high risk countries and high risk products. In case of higher risk customers, it is appropriate to undertake more regular reviews of transactions against the profile and expected activity of the business relationship, and apply different monetary thresholds for the monitoring of transactions and activity. The monitoring includes all high-risk countries as identified by the FATF, UN, EU and countries that appear on lists from other reliable and independent sources.

Additionally, the client accounts that designated non-financial service providers as lawyers and notaries hold for the benefit of their clients, can pose a high ML/TF risk, especially when a person uses the designated non-financial service provider's client account for other transactions than for which it is intended and without any legal basis. This means that transaction monitoring of client accounts is always necessary to assess whether the account is actually being used for the reasons provided. No funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the designated non-financial service provider is required to account for these funds.

The transaction monitoring process may involve **both real time and post event monitoring**.

Real time monitoring will focus on activity and transactions when information or instructions are received from customers, before or as the instruction is processed. Real time monitoring of activity will be more effective at reducing a service provider's exposure to ML/TF risk.

Post event monitoring may involve end of day, weekly or monthly reviews of customer activity and transactions. Post event monitoring may be more effective at identifying patterns of unusual customer activity or transactions.

The monitoring frequency is clearly set out and established in a risk-based way. If the monitoring frequency is not daily, it can in principle only be weekly or monthly if **the risks involved are (very) low**. Especially those service providers that only receive transaction information from their clients after the fact (e.g. company service providers that receive bank statements from their client long after the transactions have taken place), will need to develop a transaction monitoring method whereby they have direct and immediate access to the transactions executed by their clients in their bank account; such a service provider should have online viewing rights to all bank accounts of their client.

Transaction monitoring may involve manual and automated processes. Automated monitoring processes generally add value to manual processes, particularly for service providers with large volumes of customer transactions.

The transaction monitoring system preferably has a clear list of rules and parameters with relevant red flags and potential signals in order to identify transactions or activities for further examination that fall outside the parameters for usual activity. It is advisable to also use compound rules to detect activities as 'smurfing' or 'rapid movements'. There should be a well-defined process for translating the rules into system parameters or (manual) queries, updating lists, and testing the system. Where necessary, the monitoring system would need to be adjusted by refining the system's parameters, enhancing controls for more vulnerable products, services or business units.

Alerts are assessed in accordance with the described procedure (preferably involving the officer with responsibility for the customer and the MLRO), in which an escalation pathway is also defined. Appropriate factors to consider in determining whether activity or transactions are unusual include:

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

The service provider can pose questions as

- Do the transactions serve an economic or commercial purpose?
- Are the amounts involved exceptionally large?
- Are the deposits, withdrawals or transfers out of proportion to the normal/expected business of the customer?
- Is the account and transaction activity in line with the activities of the customer?
- Are there transactions from and to countries with a heightened risk?

The persons examining the alerts can only perform its task appropriately and effectively, if they have access to relevant CDD information. The enquiries made and the conclusions reached by the examiner have to be recorded in a clear and understandable way.

Appropriate follow up action may include:

- Where the transaction does not have a rational explanation, reporting the case to the MLRO for further assessment and reporting to the FIU (Chapter 7);
- Updating CDD information to record the results of the enquiries made;
- Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and/or additional information obtained;
- Applying increased levels of monitoring to the business relationships;
- Considering whether the customer's risk profile, after re-assessment, is still acceptable and the business relationship with the customer can be continued or must be terminated.

7. Unusual transactions

7.1 Introduction

Service providers have the duty to report any unusual transaction to the FIU. This includes intended transactions (transactions that are not or not yet executed). Unusual transactions are transactions where there is reason to believe that they may be connected to money laundering or terrorist financing. The service provider needs to be aware that tipping off a client about the reporting of an unusual transaction to the FIU is forbidden, seen as a criminal offence and can be subject to (personal) penalties, imprisonment or a fine.

7.1.1 Statutory requirements

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

Pursuant to Article 26, paragraph 2, of the AML/CFT State Ordinance, a service provider must include, in any case, the following information in an unusual transaction report:

- *the identity of the customer;*
- *the nature and number of the identity document of the customer;*
- *the nature, time, and place of the transaction;*
- *the amount and destination and source of the monies, securities, precious metals, or other values involved in a transaction;*
- *the circumstances based on which the transaction is considered unusual.*
- *if it concerns a transaction regarding a high value object, a description of the object in question.*
- *the indicator or indicators pursuant to which the transaction has been designated as unusual.*

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

Pursuant to Article 28 of the AML/CFT State Ordinance, a service provider must make unusual transactions reports to the FIU in accordance with the directions of the FIU.

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

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

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

The following objective and subjective indicators are applicable:

- *130101 A transaction reported to law enforcement authority or justice department*
- *130102 A transaction made by or on behalf of a natural person or a legal person, group or service provider, located in countries of jurisdictions, which are mentioned on lists referred to by the Sanction Ordinance 2006 (AB 2007 no. 24) or mentioned on lists appointed to by the Head*
- *130103 A funds transfer of Afl. 500.000,= (or equivalent) or more*
- *130104 A cash transaction of Afl. 25.000,= (or equivalent) or more*
- *130105 A cash transaction of Afl. 5.000,= (or equivalent) or more (indicator is only applicable for casino's)*
- *130201 A transaction which gives reason to presume that it might be related to money laundering*
- *130202 A transaction which gives reason to presume that it might be related to terrorist financing*

7.1.2 Regulatory requirements

- A service provider must establish and maintain reporting procedures which:
  - communicate the identity of the MLRO (and any deputy MLROs) to the service provider's employees;
  - encompass the reporting of attempted transactions and business that have been turned away;
  - require that an internal unusual transaction report is promptly made to the MLRO (or to a deputy MLRO) of any information or other matter coming to the attention of any member of staff handling transactions which, in the opinion of that person, (possibly) meets the objective indicators or the subjective indicators;
  - require that a report is considered promptly ("without delay" in the meaning of Article 26, paragraph 2, subsection e, of the AML/CFT State Ordinance) by the MLRO (or a deputy MLRO) in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report constitutes an unusual transaction;
  - allow the MLRO (or a deputy MLRO) to have access to all other information which may be of assistance in considering the report; and
  - provide for the information or other matter contained in a report to be disclosed as soon as is reasonably practicable by the MLRO (or deputy MLRO) to the FIU in writing, where the MLRO (or deputy MLRO) has determined that the information or other matter contained in the report constitutes an unusual transaction.

- A service provider must ensure that:
  - all relevant information regarding a possible unusual transaction is promptly made available to the MLRO (or deputy MLRO) on request so that internal unusual transaction reports are properly assessed;
  - each possible unusual transaction report is considered by the MLRO (or deputy MLRO) in light of all relevant information;
  - with regard to the unusual transaction reports made according to the subjective criteria the MLRO (or deputy MLRO) must document the evaluation process followed and reasons for the decision to report or not to report to the FIU;
  - where a customer fails to supply adequate CDD information (including information on UBOs), consideration is given to making an unusual transaction report;
  - unusual transactions reports include a statement of the information giving rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion of ML/TF activity and full details of the customer;
  - internal unusual transactions reports are not filtered out by supervisory staff or managers such that they do not reach the MLRO (or deputy MLRO).

- A service provider must establish and maintain arrangements for disciplining any member of staff who fails, without reasonable excuse, to make an internal unusual transaction report where he or

she is aware of any information or other matter that (possibly) meets the objective indicators or the subjective indicators for the reporting of unusual transactions.

- A service provider must ensure that its employees are regularly reminded of the tipping off prohibition via training sessions or otherwise.

7.1.3 Guidance notes

An important precondition for the recognition of an unusual transaction is for the service provider to know enough about the business relationship or transaction to recognize that a transaction is unusual. Such knowledge would arise from complying with the (ongoing) CDD requirements and contact with the customer.

The service provider bases its decision to file an unusual transaction with the FIU on the objective and subjective indicators. The objective indicators describe situations in which transactions must always be reported; these indicators are generally related to a specific limit. When an objective indicator could apply, the service provider should also assess whether there is a connection between two or more transactions. This can be done on the basis of the type of transaction and the amounts involved. If a connection is shown to exist, these transactions could (also) be reported under the subjective indicators.

However, **the emphasis in the reporting obligation lies on the subjective indicators.** The subjective indicators require a service provider to report a transaction if it has reason to suspect that the transaction may be related to money laundering or terrorist financing. These indicators apply to every service provider that falls under the scope of the AML/CFT State Ordinance. The service provider will consider whether a particular transaction needs to be reported because of a possible link to money laundering or terrorist financing. The service provider thus has its own responsibility for the adequate reporting of unusual transactions.

When evaluating a possible unusual transaction, the MLRO (or deputy MLRO) reviews all transaction patterns and volumes and other relevant information such as previous transactions and activities, the length of the business relationship and CDD information, other connected accounts or relationships.

Such connectivity can arise through commercial connections, such as transactions to or from other customers or common introducers, or through connected natural persons, such as third parties, common ownership of entities or common signatories. However, the need to search for information concerning connected accounts or relationships should not unnecessarily delay the filing of a report to the FIU. The MLRO can also make further enquiries to obtain any further information required to enable a determination as to whether the transaction has a rational explanation.

Unusual transactions may be identified as transactions that are inconsistent with the expected pattern of transactions within a particular relationship, or with the normal business activities for the type of product or service that is being delivered. Unusual or higher risk transactions may indicate ML or TF activity where there is no apparent economic or visible lawful purpose.

Transaction is defined in the AML/CFT State Ordinance as an act or a combination of acts by or on behalf of a customer in connection with the procurement or provision of services, or of which a service provider has taken notice within the framework of his provision of service to a client. The definition of transaction is intended to make clear that an unusual transaction by the customer or by a third party acting on behalf of the customer must always be reported if the service provider has become aware of in the course of providing services to that customer. It is not a prerequisite that there is a direct or causal connection between the unusual transaction and the activities of the service provider. The words 'act or combination of acts by or on behalf of a customer' should be interpreted in such a way that the passive involvement of the service provider (by virtue of its knowledge of the transaction) can also trigger the reporting obligation.

An attempted transaction could be considered as one that a customer intended to conduct with the service provider and took some form of action to do so but failed to complete. An attempted transaction is

different from a single request for information, such as an enquiry as to the fee applicable to a specific transaction. The obligation to report unusual transaction applies to all types of attempted transactions, including circumstances where there is no existing business relationship with the customer and no such business relationship is subsequently established.

A good way to ensure that unusual transaction reports are promptly made to the FIU is by having internal reporting lines that are as short as possible with the minimum number of people between the employee initiating the internal unusual transaction report and the MLRO (or deputy MLRO). In the process of deciding to file an internal report, staff can discuss relationships and transactions with line managers before making an unusual transaction report, but it will be the decision of the staff member whether to make the internal report to the MLRO.

In short, the processes for detecting unusual transactions could look as follows

- The service provider has identified clear internal indicators or 'red flags' that can help employees determine whether a transaction is unusual.
- The internal indicators focus on unusual transaction patterns, deviating behavior on the part of the customer, and activities that are illogical based on knowledge of the customer or sector.
- The business is responsible for detecting potentially unusual transactions.
- The MLRO is involved in assessing a possible unusual transaction and is responsible for reporting to the FIU.
- The assessment of possible unusual transaction takes account of the customer risk assessment, the available CDD and other information.

When a report of an unusual transaction is or is to be filed with the FIU, it will also be necessary to carefully consider other transactions or activity of the customer and the risk and nature of the continuing relationship.

To ensure that there are appropriate arrangements for disciplining staff, employment contracts or employment handbooks could provide for the imposition of disciplinary sanctions for failing to make an internal unusual transaction report without a reasonable excuse. Appropriate staff training in the recognition of unusual activity is therefore vital.

Tipping off
Where the ongoing monitoring of a customer's transactions indicates possible ML/TF activity, and the process of undertaking identification procedures is managed without due care, contact between a service provider and a customer (or his advisors) could unintentionally lead to the customer being tipped off.

Where the service provider has queries for the customer to assist the MLRO in formulating or negating a possible suspicion, any enquiries of the customer or other persons should be made having due regard to the tipping off provision.

Indemnification
Article 29 of the AML/CFT State Ordinance provides for criminal indemnification and Article 30 for civil indemnification. Criminal indemnification ensures that data or information provided by a service provider that reports an unusual transaction cannot be used in a criminal investigation or prosecution of that service provider on suspicion of money laundering or terrorist financing as long as the service provider acted on the reasonable assumption that it was implementing the reporting duty. The law extends this indemnification to those who have submitted the report, such as a bank employee who submitted or helped compile the report.

The civil indemnification means that a service provider cannot be held liable under civil law for the loss suffered by another party (the customer or a third party). For instance, claims in civil proceedings could be brought for breach of contract if the service provider decided not to carry out a transaction but to report it. Legal action over an unlawful act is also possible, to claim alleged loss suffered as a result of a service provider's unusual transaction report. The indemnification will of course only apply if the unusual

transaction report has been submitted in good faith and correctly in accordance with the requirements of the law.

Confidentiality
The AML/CFT State Ordinance imposes a strict duty of confidentiality. This means that a service provider is obliged to observe confidentiality in respect of an unusual transaction report. Exceptions are possible in so far as they arise from the purpose of the law.

Red Flags
The following is a non-exhaustive list of possible red flags that the service provider can take into account when dealing with a business relationship or occasional transaction. The list is provided to reflect examples of possible red flags. The existence of one or more red flag does not automatically indicate an unusual transaction and there may be a legitimate reason why a customer has acted in the manner identified.

1. The deposit or withdrawal of unusually large amounts of cash in or from an account.
2. Deposits or withdrawals at a frequency that is inconsistent with the service provider's understanding of that customer and its circumstances.
3. Transactions involving the unexplained movement of funds, either as cash or funds transfers.
4. Payments received from, or requests to make payments to, unknown or unassociated third parties.
5. Personal and business related money flows that are difficult to distinguish from each other.
6. Financial activity which is inconsistent with the legitimate or expected activity of the customer.
7. An account or business relationship becomes active after a period of dormancy.
8. The customer is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting a transaction.
9. The customer holds multiple accounts for no apparent commercial or economic reason.
10. Cash deposited domestically with the funds frequently withdrawn from ATMs in another jurisdiction.
11. Early surrender of an insurance policy incurring substantial loss.
12. Unexplained early repayment of loans.
13. Transfers indicated as loans from relatives or apparently unrelated third parties.
14. Funds transferred to a charity or NPO with suspected links to a terrorist organization.
15. High level of funds placed on store value cards.
16. Insurance policy being closed with a request for the payment to be made to a third party.
17. Large amounts of cash from unexplained sources.
18. Loans that are repaid in cash.
19. Purchase of high value assets followed by immediate resale.
20. Request by a customer to pay cash for purchase of high value assets.

8. Record Keeping

8.1. Introduction

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

Sound record keeping is also essential to facilitate effective supervision, allowing the CBA to supervise compliance by the service provider with its statutory obligations and regulatory requirements. If there is no documentation or any records that requirements are met and CDD performed, the CBA could consider the requirement as not executed.

8.1.1 Statutory requirements

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

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

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

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

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

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

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

- *all account files and business correspondence.*

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

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

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

8.1.2 Regulatory requirements

- A service provider must keep, for a period of at least ten years from the date that a business relationship ends, or, in relation to an occasional transaction, for at least ten years from the date that a transaction was completed, orderly records containing:
  - internal unusual transactions reports and supporting documentation;
  - the decision of the MLRO (or deputy MLRO) concerning whether to make an unusual transaction report to the FIU and the basis of that decision; and
  - any unusual transactions reports and receipt confirmations from the FIU,

  in relation to that business relationship or occasional transaction.

- A service provider must record and store all CDD information. This is done in such a way that facilitates periodic updating of the information and access by the CBA to the CDD information.

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

- A service provider must keep adequate and orderly records containing the findings of reviews of:
  - complex transactions;
  - unusual large transactions; and
  - unusual patterns of transactions, which have no apparent economic or visible lawful purpose, for a period of at least ten years from the date the business relationship ends, or, if in relation to an occasional transaction, for ten years from the date that the transaction was completed.

- A service provider must record all CDD and transaction information in a way that facilitates ongoing monitoring of each relationship - in order to meet obligations that are set out in Chapters 4-6.

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

- The records retained by a service provider must be readily accessible. Unless otherwise specified, records relating to CDD and transaction information must be accessible within 5 working days (whether held in Aruba or outside Aruba), or such longer period as agreed with the CBA. Other records must be accessible within 10 working days (whether held in Aruba or outside Aruba), or such longer period as agreed with the CBA.

- A service provider provides the CBA with the complete customer file upon request, without delay.

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

- A service provider must periodically review the accessibility of, and condition of, paper and electronically retrievable records and consider the adequacy of the safekeeping of records.

- A service provider must periodically review the procedures relating to retrieval of records.

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

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

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

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

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

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

- Where a service provider terminates activities, or disposes of business or a block of customers to other service providers, record keeping requirements are unaffected by the termination or disposal. In such cases, record keeping arrangements must be agreed with the CBA where a service provider terminates activities, or disposes of business or a block of customers to another service provider.

8.1.3 Guidance notes

A service provider has to retain customer and transaction data. This concerns all data obtained during the CDD process, e.g. copies of identity documents, account particulars, correspondence, memos of conversations about and with the customer, risk assessments, transactions effected by and other services provided to that customer. The customer file should also reveal how the decision-making process surrounding customer acceptance and risk rating has taken place.

For legal entities, records should include the particulars of the natural persons representing the legal entity vis-à-vis the service provider. For the UBO, the person's identity and the method by which the identity was verified should be recorded. If a customer acts as a trustee, the service provider also records data in a retrievable manner concerning the settlors, protectors, trustees and beneficiaries. Where a customer acts as partner in an unincorporated partnership, the service provider should record the

particulars of all partners, the persons authorized with respect to the management of the unincorporated partnership and the persons who are able to exert considerable influence on or have considerable interests in the partnership.

Additionally, all transactions carried out on behalf of or with a customer in the course of business, both domestic and international, has to be recorded by the service provider. In every case sufficient information needs to be recorded to permit the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. With respect to transactions, documentation includes details of the customer, the amounts and types of currency involved in the transaction (for monetary transactions); the account name and number or other information by which it can be identified, details of the counterparty, including account details, the nature of the transaction, and the date of the transaction. For some transactions, it may be relevant to keep records of valuations and prices, memoranda of purchase and sale, custody of title documentation, and other records in support of transaction records where these are necessary to enable a clear and complete audit trail of funds or asset movements to be established.

The purpose of the data retention obligation is to enable the authorities to gain an understanding of a customer's activities, e.g. in the event of a (criminal) investigation. The various records and files should therefore be easily accessible to the authorities. It makes no difference whether the data are stored electronically or as a physical document. Records may be kept by way of original documents; photocopies or scans of original documents (certified where appropriate), or in electronic form.

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

When original vouchers or documents are used for account entry, for example, and are not returned to the customer, it is of assistance to the authorities if these original documents are kept for at least one year to assist investigations.

With respect to adequate records on the assessment of effectiveness of policies, procedures and measures the service provider keeps its business risk assessment, compliance reports to the Board/senior management, details of testing programs conducted by the MLCO, and where relevant the audit reports.

Where documentation is held overseas or by third parties, such as under outsourcing arrangements, or where reliance is placed on introducers, this will present additional factors for a service provider to consider. Where record keeping is outsourced, a service provider remains responsible for compliance with all requirements.

9. Training, awareness and screening of employees

9.1 Introduction training and awareness

One of the most important tools available to the service provider to assist in the prevention and detection of financial crime is to have appropriately screened employees who are alert to the potential risks of ML/TF and who are well trained in the requirements concerning CDD and the identification of unusual activity.

9.1.1 Statutory requirements

Pursuant to Article 46 of the AML/CFT State Ordinance, a service provider must pursue adequate policies and have procedures and measures in place regarding, inter alia, the recruitment, change of position, background, education, guidance and ongoing training of employees.

9.1.2 Regulatory requirements

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

- A service provider must, in relation to relevant employees take regular and appropriate measures to ensure they are aware of and trained in the CDD process, record keeping and internal reporting procedures, and such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing ML/TF as well as the enactments in Aruba relating to ML/TF, including the AML/CFT Laws and Regulations and the relevant AML/CFT provisions of the Criminal Code of Aruba (AB 1991 no GT 50).

- A service provider must have appropriate measures in place to make relevant employees aware of:
  - the service provider's policies, procedures and measures designed to prevent and detect ML/TF;
  - the statutory and regulatory obligations under which the business operates and under which the service provider and/or its employees may be held personally liable;
  - the implications of failing to report information in accordance with procedures may result in criminal, regulatory and/or disciplinary sanctions.

- The service provider must ensure that the training provided to relevant employees is comprehensive and ongoing and that employees are aware of ML/TF risks and the vulnerabilities of the service provider to it, new developments and risk factors connected with ML/TF, and their obligations in relation to controlling those risks, including the ability to recognize unusual transactions. The training must be tailored to the service provider and relevant to the employees to whom it is delivered.

- Relevant employees, include
  - board members and senior management;
  - MLRO, MLCO, the internal audit function (where relevant);
  - employees undertaking any customer facing functions;
  - employees responsible for the handling of, business relationships or occasional transactions, or transactions conducted in respect of such;
  - employees directly supporting a colleague who carries out any of the above functions;

    - employees in a position where they might see or hear anything which may lead to a suspicion.

- Employees that, in view of their particular responsibilities, should receive additional and specific training, appropriate to their roles, are the Board and senior management as well as the MLRO and MLCO, their deputies, and where relevant the internal audit function.

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

- The service provider will keep records of the training provided, the persons who attended the training, and their test result. The service provider provides these records to the CBA upon request, without delay.

9.1.3 Guidance notes

Training and awareness
The guiding principle of all training should be to encourage employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the service provider against the threat of ML/TF.

While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practices in the area of AML/CFT. The precise approach adopted will depend upon the size, nature and complexity of the service provider's business. Classroom training, videos and technology-based training programs can all be used to good effect, depending on the environment and the number of relevant employees to be trained.

Training of Board and senior management would also address the conducting and recording of ML/TF business risk assessments and the formulation of a risk appetite, together the establishment of appropriate, relevant and effective policies, procedures and controls.

The MLRO needs to be trained in among others the handling of internal disclosures of unusual activity, the making of high quality disclosures to the FIU and the management of the risk of tipping off.

The training provided to the MLCO must address the monitoring and testing of compliance systems and controls (including details of the service provider's policies and procedures) in place to prevent and detect ML/TF.

An adequate training promotes a culture of compliance and an awareness of the threat of ML/TF, and stresses that CDD and reporting procedures should be followed. An adequate training addresses among others:

- ML/TF threats and vulnerabilities of services and products offered by the service provider, as assessed in the business risk assessment.
- AML/CFT Laws and Regulations (and by extension, also the Handbook) and the relevant AML/CFT provisions of the Criminal Code of Aruba (AB 1991 no GT 50) (Articles 140a, 430b, 430c and 430d);
- AML/CFT policies, procedures and measures, their application, and employees' responsibilities.
- Recognition of and dealing with unusual or higher risk activity and transactions, such as activity outside of expected patterns, unusual settlements, abnormal payment or delivery instructions and changes in the patterns of business relationships.
- ML/TF developments, including techniques, methods, trends and typologies.
- Management of business relationships or transactions which have been the subject of an unusual transaction report, e.g. risk of committing the offence of tipping off, and dealing with questions from such customers or their advisers.

In order to measure the effectiveness of the AML/CFT training, the service provider could consider it appropriate to incorporate an exam or some form of assessment into its training program, either as part of the training provided to relevant employees or during the intervening period between training. The effectiveness of training can also be assessed by monitoring the compliance of employees with AML/CFT policies, procedures and measures.

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

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

Consideration should be given by the service provider to establishing an appropriate minimum period of time by which, after the start of their employment, new employees should have completed their AML/CFT induction training. Satisfactory completion and understanding of any mandatory induction training could be a requirement of the successful completion of a relevant employee's probationary period. Additional training could also be relevant when there is a change in an employee's role.

It goes without saying that the service provider informs employees of the identity of the MLRO, ensures that the AML/CFT procedures are available to all employees, and informs them of the consequences if the AML/CFT obligations are not adhered to. It is not sufficient to provide employees with a copy of the Handbook, as the Handbook is designed to provide a base from which a service provider can design and implement and tailor its own policies, procedures and measures appropriate to its business.

There may be some employees who, by virtue of their function, fall outside of the definition of a relevant employee, for example, receptionists, filing clerks, messengers etc. The service provider should consider, on a case-by-case basis, whether an employee falls within the definition of a relevant employee, as the scope of a person's role and the tasks undertaken will vary from person to person. The service provider should also be aware that an employee's function may change over time.

Also, with regard to non-relevant employees, it would be necessary to inform this staff of the identity of the MLRO and the procedures to make internal unusual transactions reports and provide them with a document outlining the service provider's and their own obligations and potential criminal liability under articles 430b, 430c, 430d and 140a of the Criminal Code of Aruba (AB 1991, no. GT 50).

Ongoing training
The Board/senior management ensures that it is provided with adequate information on a sufficiently regular basis in order to be sure that the service provider's relevant employees are suitably trained to fulfil their personal and corporate responsibilities.

With the passage of time between training initiatives, the level of employee awareness of ML/TF risks can decrease. The utilization of techniques to maintain a high level of awareness can greatly enhance the effectiveness of a service provider's defenses against ML/TF.

A service provider therefore maintains awareness by keeping employees informed of AML/CFT developments, such as updates issued by the CBA, or developments in international AML/CFT standards, typologies and case studies illustrating how products or services provided by the service provider may be abused.

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

9.2 Screening of staff

9.2.1 Statutory requirements

Pursuant to Article 46 of the AML/CFT State Ordinance, a service provider must pursue adequate policies and have procedures and measures in place regarding, inter alia, the recruitment, change of position, background, education, guidance and ongoing training of employees.

9.2.2 Regulatory requirements

- A service provider must screen and monitor the competence and probity of relevant employees.
- The service provider shall maintain appropriate and effective procedures, proportionate to the nature and size of the service provider and to its risks, when hiring employees or admitting any person as a partner in the service provider, for the purpose of ensuring high standards of employee and partner probity and competence.
- When there is a change in an employee's role, the service provider assesses whether re-screening is necessary.
- The service provider must ensure that the results of any checks undertaken, are documented and retained.

9.2.3 Guidance notes

Appropriate screening procedures (at the time of recruitment or subsequent change in role) include one or more of the following activities (as appropriate for the nature of the employee's role and responsibilities):

- obtaining and confirming appropriate references;
- obtaining and confirming employment history and qualifications;
- obtaining a Declaration of Good Conduct or an equivalent declaration;
- obtaining details of any regulatory action taken against the individual (or absence of such action)
- obtaining and confirming details of any criminal convictions (or absence of such convictions).

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

The service provider should give consideration to consulting the lists of specified countries and persons against whom sanctions have been imposed by the UN and the EU to ensure that a prospective employee does not have suspected or known involvement in terrorist activity.

10. Funds transfers

10.1 Introduction

The Statutory requirements set out in this Chapter follow from the State Decree Regulation Wire Transfers, which is based on Article 6, paragraph 4, of the AML/CFT State Ordinance. The Statutory requirements apply to financial service providers as meant in Article 1, paragraph 1, of the AML/CFT State Ordinance whose business includes carrying out funds transfers (payment service providers as meant in Article 1 of the State Decree Regulation Wire Transfers).

The State Decree Regulation Wire Transfers is based on FATF Recommendation 16. The FATF's principle purposes for developing standards on the payer and beneficiary information to accompany funds transfers are to prevent terrorists and criminals from having unfettered access to funds transfers for moving funds and to enable the detection of the misuse of funds transfers when it occurs. Key parts of FATF Recommendation 16 include requiring that information about the payer and beneficiary accompany funds transfers throughout the payment chain. This is to ensure the traceability of funds to assist in preventing, detecting and investigating ML/TF and to facilitate the effective implementation of restrictive measures against persons and entities designated under UN and EU sanctions legislation. The standards also require the payment service providers to have appropriate risk-based procedures in place to determine where a transfer lacks the required information so as to enable the payment service provider to decide whether to execute, reject or suspend a transfer and to determine the appropriate action to take.

10.1.1 Regulatory requirements and Guidance notes

As the State Decree Regulation Wire Transfers is based on the FATF Recommendation 16, payment service providers may find it of benefit when developing their policies, procedures and controls for funds transfers to review guidance issued by the FATF on the measures payment service providers should take to detect missing or incomplete information on the payer or the beneficiary and the procedures they should put in place to manage a transfer of funds lacking the required information.

The requirements apply to cross-border funds transfers and domestic funds transfers.

These requirements do not apply to the following transfers:

- Any transfer that flows from a transaction carried out using a credit or debit or prepaid card for the purchase of goods or services, so long as the credit or debit or prepaid card number accompanies all transfers flowing from the transaction. However, when a credit or debit or prepaid card is used as a payment system to effect a person-to-person funds transfer, the transaction is covered by Recommendation 16, and the necessary information should be included in the message.
- Payment service provider-to-payment service provider transfers and settlements, where both the payer and the beneficiary are payment service providers acting on their own behalf.

Funds transfer refers to any transaction carried out on behalf of a payer through a payment service provider by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary payment service provider, irrespective of whether the payer and the beneficiary are the same person.

Domestic transfers

Information accompanying domestic funds transfers should include payer information as indicated for cross-border funds transfers below, unless this information can be made available to the beneficiary payment service provider and the authorities by other means.

In this case, the ordering payment service provider needs only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the payer or the beneficiary.

The information should be made available by the ordering payment service provider within three business days of receiving the request either from the beneficiary payment service provider or from appropriate competent authorities.

Cross-border transfers

Ordering payment service provider
The ordering payment service provider means the payment service provider which initiates the funds transfer and transfers the funds upon receiving the request for a funds transfer on behalf of the payer.

The ordering payment service provider should ensure that funds transfers contains the following information:

- Information accompanying all funds transfers above the threshold of USD/EUR 1000/Afl 1790 always contain:
  - the name of the payer;
  - the payer's account number where such an account is used to process the transaction;
  - the payer's address, or national identity number, or customer identification number, or date and place of birth;
  - the name of the beneficiary; and
  - the beneficiary account number where such an account is used to process the transaction.

- Funds transfers under the threshold of USD/EUR 1000/Afl 1790 should include:
  - the name of the payer
  - the name of the beneficiary; and
  - an account number for each, or a unique transaction reference number.

The threshold also applies to linked transactions which together exceed the threshold.

For funds transfers under the threshold, this information need not be verified for accuracy, unless there is a ML/TF suspicion, in which case, the payment service provider should verify the information pertaining to its customer.

The information on the payer as contained in the funds transfer should be accurate, which means that the information has been verified for accuracy. If the abovementioned information on the payer and beneficiary is not available or if the payment service provider cannot ensure that the information is contained in the funds transfer, the ordering payment service provider should not execute the funds transfer.

If there is no account from which the transfer is executed, a unique transaction reference number should be included to permit traceability of the transaction. The payment service provider will in those cases also need to obtain customer identification information on the payer and beneficiary and record that information and verify the customer information on the payer.

Where the payer is an existing customer of the payment service provider, the payment service provider may deem verification to have taken place. A national identity number can be any government issued personal identification number or other government issued unique identifier. Examples of such would include a passport number, national identity card number or social security number.

A customer identification number may be an internal reference number that is created by the payment service provider which uniquely identifies a customer, and which will continue throughout a business relationship, or it may be a number that is contained within an official document.

In case funds transfers from a single payer are bundled in a batch file for transmission to beneficiaries, the batch file contains accurate payer information, and full beneficiary information, that is fully traceable within the beneficiary country.

Intermediary payment service provider
The intermediary payment service provider means the payment service provider in a serial or cover payment chain that receives and transmits a funds transfer on behalf of the ordering payment service provider and the beneficiary payment service provider, or another intermediary payment service provider. This can for instance be payment service providers acting as agents for other payment service providers or who provide correspondent banking facilities.

In case this is an Aruban intermediary payment service provider, the payment service provider should ensure that all payer and beneficiary information that accompanies a cross-border funds transfer is retained with it.

The intermediary payment service provider has policies, procedures and measures to identify cross-border funds transfers that lack payer or beneficiary information and to determine when to execute, reject, or suspend a funds transfer that lacks the required payer or required beneficiary information. Such measures do not need to include the stopping of the transaction when this is not consistent with straight-through processing (payment transactions that are conducted electronically without the need for manual intervention).

Where a cross-border transfer becomes a related domestic transfer and the intermediary payment service provider cannot, due to technical issues, retain the payer and/or beneficiary information with the transfer, the payment service provider makes a record of this, and keeps all the information for at least five years.

Beneficiary payment service provider
The beneficiary payment service provider means the payment service provider which receives the funds transfer from the ordering payment service provider directly or through an intermediary payment service provider and makes the funds available to the beneficiary.

When a beneficiary payment service provider receives a funds transfer (above the threshold) the payment service provider should verify the identity of the beneficiary, in case this has not been done before.

The beneficiary payment service provider has policies, procedures and measures to identify cross-border funds transfers that lack payer or beneficiary information and to determine when to execute, reject, or suspend a funds transfer that lacks the required payer or beneficiary information.

Policies, procedures and measures on missing information
The intermediary and beneficiary payment service providers should have established policies, procedures and measures to determine when to execute, reject, or suspend a funds transfer that lacks the required payer or beneficiary information. These policies, procedures and measures also include appropriate follow-up action, for instance reporting to the FIU when there are indications of ML/TF. They may include post-event monitoring or real-time monitoring where feasible.

These policies, procedures and measures can be risk-based. Based on the ML/TF risks to which the transaction is exposed, the payment service provider can determine which transfers will be monitored in real time and which can be monitored ex-post and why. The payment service provider also sets out what employees should do where required information is missing or incomplete.

The payment service provider will need to be able to identify empty message fields, have procedures in place to detect whether the required customer identification information is missing on the payer or the beneficiary (for example, by undertaking sample testing to identify fields containing incomplete information on the payer and beneficiary) and where information is incomplete, take specified action.

Consideration should be given to areas such as:

- the value of the transaction;
- the country where the payment service provider is established;
- the country of the payer;
- the history of previous transfers with the payment service provider of the payer, i.e. whether it has failed previously to comply with the customer identification requirement; and
- the complexity of the payment chain within which the payment service provider operates.

Where an ordering payment service provider becomes aware subsequent to processing the payment that information on the payer or beneficiary is missing or incomplete either as a result of random checking or other monitoring mechanisms, it will seek the complete information on the payer and beneficiary relevant to the type of transfer. If a decision is made to ask for complete information on the payer, a payment service provider should also consider, on the basis of the perceived risk, whether to make the payment or to hold the funds until such time as complete information has been received.

Where a payment service provider has sought complete information on the payer and it has not been provided within a reasonable time frame, the payment service provider must consider, on a risk-based approach, the most appropriate course of action to be undertaken. Where an ordering payment service provider regularly fails to fulfil the information requirements, then the beneficiary payment service provider must notify the CBA of that fact and the steps it has taken to attempt to ensure that such information is supplied. The fact that information on the payer or the beneficiary is missing or incomplete can also be taken into account in assessing whether a transfer is unusual and should be reported to the FIU.

Money transfers

The State Decree Regulation Wire Transfers also applies to money transfer companies, regardless whether they operate directly or through agents. In the case of a money transfer company that controls both the ordering and the beneficiary side of a money transfer, the company:

- should take into account all the information from both the ordering and beneficiary sides in order to determine whether an unusual or suspicious transaction has to be filed; and
- should file an unusual or suspicious in any country affected by the unusual funds transfer, and make relevant transaction information available to the FIU.

Record keeping

The record keeping requirements of Article 33 and 34 of the AML/CFT State Ordinance and as described in Chapter 8 of this Handbook are applicable.

11. Sanctions

11.1 Introduction

Sanctions are political instruments in the foreign and security policy of the United Nations (UN) and the European Union (EU). They are mandatory instruments, used in response to breaches of international laws and human rights, or to effect change when legal or democratic principles are not being adhered to. Sanctions also play a role in the fight against terrorism.

Sanctions measures imposed by the UN, EU or a country concern restrictive measures against a country, regime, individual, service provider, industry or type of activity believed to be violating international law and could include one or more of the following:

- the freezing of funds;
- the withdrawal of financial services;
- a ban or restriction on trade;
- a ban or restriction on travel; or
- suspension from international organizations.

The ultimate objective of a sanction varies according to the situation. For instance, an arms embargo and a ban on the export of certain items or raw materials could be aimed at supporting a peace process and restricting the financing of weapons by combatants. Sanctions may also be aimed at preventing the proliferation of weapons of mass destruction, disrupting terrorist operations, or trying to change the policies and actions of the target. Sanctions are a tool used for enforcing foreign policy by putting pressure on a state or service provider in order to maintain or restore international peace and security. Often, sanctions are used as an alternative to force. All recent UN and EU sanctions contain information as to their intended aim or purpose.

The two key supranational bodies to determine sanctions measures relevant to the sanctions regime within Aruba are the UN and the EU. The UN Security Council can take measures to maintain, or restore, international peace or security. Such measures range from economic sanctions to international military action. Each UN member state is then called upon to implement the requirements of a sanctions measure in its own territory. The EU applies sanctions in pursuit of the specific objectives of the Common Foreign and Security Council as set out in the Treaty of the European Union. EU sanctions are either adopted to ensure compliance with UN sanctions requirements or enacted autonomously by the EU to advance specific EU objectives. European sanctions regulations imposing sanctions apply directly in EU member states.

In Aruba, further legislation is required to impose penalties for sanctions breaches under EU regulations. On the basis of the Sanctions State Ordinance 2006, UN and EU sanctions can be incorporated into Aruban legislation.

Financial sanctions impose restrictive measures in respect of designated persons, that is, persons, groups or entities designated by the UN Sanctions Committee or the EU. There are several financial sanctions:

- an order to freeze funds and assets of designated persons or entities;
- a ban on making resources available to these persons or entities directly or indirectly;
- a ban or restrictions on providing financial services.

In fulfilment of a treaty or international decree, which Aruba is obliged to comply with, rules will be laid down by State decree containing general rules, in so far as this compliance entails that rules must be laid down which apply or might apply in this country and which constitute a prohibition for the residents or impose an obligation on them. The rules laid down in a sanction decree may contain restrictions of the international services and financial transactions, shipping traffic, aviation traffic and post and telephone communications from and to Aruba; they may differ from rules laid down in State ordinances.

Aruba has enacted several pieces of legislation which implement EU and UN sanctions measures. These is done via the Sanctions State Decrees on Sudan, South Sudan, Libya, Central African Republic, North Korea, Syria, Ukraine, and Yemen. These Sanctions State Decrees require all funds or other assets present in Aruba that belong directly or indirectly to, are owned by, are in possession of or are under the control of a natural person, legal entity or service provider, mentioned in the UN or EU sanctions regulation to be frozen.

The Sanction Decree Combat Terrorism and Financing Terrorism requires the freezing of all funds and other assets of persons and entities mentioned on the lists kept by the UN regarding Al Qaeda and the Taliban, as well as on the Aruban domestic list. The domestic sanctions list, which has been established by Ministerial Decision dated November 20, 2013 consists of individuals, legal persons and other entities to which Council Regulation (EU) No. 2580/2001 of the European Union applies.

Aruba may also impose sanctions unilaterally as an extension of its own foreign policy and can request that other jurisdictions implement sanctions against a person, group or service provider.

The legislative frameworks of some jurisdictions contain provisions which have extraterritorial effect, so that they may apply to some of the parties involved in an Aruban transaction on the grounds of nationality or place of incorporation even if the jurisdiction in question is not involved in that transaction. Whilst not directly enforceable in Aruba, a service provider should be aware, in particular, of sanctions implemented by OFAC. OFAC regulations apply to any persons or entities, wherever based, trading in US Dollars, as well as:

- US citizens and permanent resident immigrants regardless of where they are located;
- persons and entities within the US;
- US incorporated entities and their foreign branches;
- In the cases of certain sanctions, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by US companies; and in certain cases, foreign persons in possession of US origin goods.

11.1.1 Statutory requirements

In accordance with the Sanctions State Decrees, all funds or other assets in Aruba, which directly or indirectly belong to, are owned by, are in possession of or are controlled by a natural person, legal person, entities or bodies listed in the relevant sanctions decrees and sanctions regulations, shall be frozen.

The freezing shall equally apply to representatives of the natural persons, legal persons, entities or bodies referred to in in the relevant sanctions decrees and sanctions regulations.

A designated person may be granted access to his frozen funds or assets for credit balances, financial assets or economic resources that:

- *are necessary to cover expenses for the basic needs of the natural persons or legal persons, entities or bodies listed in the relevant sanctions decrees and sanctions regulations, and the family members dependent on these natural persons, such as payments for food, rent or mortgage charges, medicines or medical treatments, taxes, insurance premiums and public utility services;*
- *are exclusively intended for the payment of reasonable fees or the payment of costs incurred in connection with the provision of legal services;*
- *are exclusively intended for the payment of fees or costs for only maintaining or managing frozen credit balances or economic resources; or*
- *are necessary for the payment of extraordinary charges, provided the Minister has been given notice at least two weeks in advance of the reasons why he feels that specific permission should be granted.*

Access to frozen funds or assets shall only be granted with the approval of the Minister charged with financial matters.

It is prohibited for anyone to provide services or to perform acts that lead to it or can reasonably lead to it that a natural person, legal person or other service provider listed in the relevant sanctions decrees and sanctions regulations, gains access in any way to funds or other assets.

It is prohibited to participate intentionally or deliberately in activities of which the purpose or consequence is that the sanctions measures are directly or indirectly circumvented.

Anyone having funds or other assets in his custody of a natural person, legal person or other service provider listed in the relevant sanctions decrees and sanctions regulations shall take such measures that these funds and assets cannot be used, or that these funds and other assets cannot be transferred, converted, relocated or be made available.

If it concerns a service provider supervised by the CBA pursuant to a state ordinance, it shall immediately inform the CBA of the funds or other assets it has in its custody. Other service providers shall immediately inform the FIU.

Freezing means a prohibition to transfer, convert, move or make available.

Funds or other assets means property, acquired in any way, as referred to in Article 1 of Book 3 of the Civil Code of Aruba, all documents and data carriers in any form or capacity whatsoever, showing full or shared ownership or title to any property, and products or increases in value of a property.

11.1.2 Regulatory requirements and Guidance notes

Policies, procedures and measures
A service provider must have in place appropriate and effective policies, procedures and measures to identify, in a timely manner, whether a prospective or existing customer, UBO, key principal, representative or other connected party, is the subject of a sanction issued by the UN, EU or Aruba.

The basic principle for the policies, procedures and measures is that these enable the service provider to act in line with the objectives of the sanctions regulations. This means that the service provider should be able to check its records in such a way that natural persons, legal persons and arrangements (and their funds or assets) designated in the sanctions regulations can be detected. The service provider must be able to freeze the funds or assets immediately and/or to prevent fund or assets and/or services being made available to these designated person and entities.

This requirement **cannot be met using a risk-based approach** (in other words, the service provider cannot choose whether or not to implement the sanction regulations). The method used to asses a transaction or business relationship in relation to the sanction regulations (e.g. manually or electronically) and the frequency of this assessment can however be carried out using a risk-based approach. This means that explicit attention is also devoted during the business risk assessment to the necessary frequency of the periodic screening against the sanction lists.

Service providers takes adequate measures to ensure that they are always kept informed of the contents of the sanctions lists and all changes in these lists and to otherwise ensure that they comply with the requirements and prohibitions set in sanctions regulations in a timely and adequate manner.

Customer screening
As a minimum the service provider should undertake sanctions screening for all new business relationships and occasional transactions, including the customer, UBO, representative and other key principals, at the time of acceptance, during periodic reviews and when there is a trigger event generating a business relationship review. This screening should be documented.

During the identification process, information is recorded such as the name, date of birth, place of residence and address of establishment of these persons and entities. This information enables the

service provider to perform proper checks. The absence of a date of birth or address, for example, can make it more difficult to assess a possible match against the sanctions lists.

The service provider should have appropriate procedures and measures in place to ensure that the customer base (including UBOs, principals and representatives) is checked against accurate and current lists of the designated persons and entities. Where a positive match is identified, the service provider should ensure that funds or assets are blocked without delay and that a report is immediately filed with the FIU and/or the CBA using the prescribed reporting form. The reported data must be kept for a period of five years after the relevant sanctions regulation has ceased to have effect or has been rendered inoperative.

In the event that new sanctions regulations are issued or when changes occur in the sanctions lists, the service provider must ascertain whether the persons and entities designated are part of their customer base. The same applies to each request for the rendering of a service in which a designated person or entity acts as the other party or is involved in another way.

Transaction filtering
The service provider must also have in place systems and measures to detect and block transactions connected with those natural persons and entities designated under the sanctions regimes. The transaction filtering systems used should enable the service provider to identify transactions, both incoming and outgoing, involving designated persons and entities.

Freezing of funds
Both the direct and indirect provision of funds, economic resources, assets or services fall under the sanction measures. This means that funds of persons or entities that are not on the sanction lists but are under the control or ownership of persons or entities that are designated, should in principle be regarded as the indirect provision of funds to the sanctioned person or entity. It qualifies as indirect provision, in case a person has 50% or more ownership in an entity or in case a person has control over the entity. If the person who holds 50% or more or property rights or who exercises control is listed on a sanctions list, the assets of the legal entity must be frozen and the entity should be prevented from receiving funds.

It is not permitted to exit an existing client or return funds or assets. Assets should remain frozen until the relevant sanctions regulation is changed and the obligation to freeze the funds and assets is lifted, an exemption is granted or if otherwise notice to the contrary is received from the Ministry charged with financial matters or the supervisory authorities. If the service provider does not hear anything, it should assume that the funds and assets are to be considered an actual ‘hit’ and should remain frozen until further notice.

Exemptions
In some cases, an exemption by be requested from the Minister charged with financial matters. Exemptions are possible in some cases (this may vary depending on the sanction regulation). The Minister is authorized to decide on this. A substantiated request for exemption can be sent to the ministry.

Audit trail and testing
Where an automated method of sanctions screening is used, the service provider should maintain, or have access to, an audit trail of the screening conducted by the system. The audit trail should enable the service provider to demonstrate the dates on which screening checks have been undertaken and the results of those checks, thus allowing the service provider to ensure and demonstrate to the CBA and other relevant authorities, that the system is operating effectively. Where the service provider is part of a wider group and utilizes a group-wide screening system, the service provider should seek written confirmation from its head office that such an audit trail exists and that the service provider can have access to any specific records upon request.

Testing undertaken in respect of any sanctions screening system should cover the following:

- ensuring that the screening system has been correctly configured and that the relevant pre- set rules have been activated;
- assessing the accuracy of the screening system or method utilized, for example, through an analysis of the matches generated, to ensure that designated persons and entities are promptly identified;
- determining the appropriateness of the controls for the business undertaken, including the method and frequency of testing;
- where upgrades have been applied, ensuring that the system performs as expected;
- where reliance is placed upon a third party for sanctions screening, the service provider should verify
    - the effectiveness of the screening being undertaken by that party; and
    - determine the appropriateness of the action taken by the service provider where a sanctions match has been identified to ensure that the proceeds associated with designated persons or entity are controlled and the necessary reporting undertaken in compliance with applicable regulatory requirements.

Part of the testing is also testing the “fuzzy logic” used. Such tests could be conducted by using real-life case studies, entering the name of sanctioned natural or legal persons to ensure that the expected results are achieved.

Proliferation financing
As mentioned in Chapter 3.3.3 on the business risk assessment, explicit attention is also devoted during the business risk assessment to proliferation financing. Based on this assessment, the service provider can tailor its measures regarding sanctions controls and proliferation financing.

Proliferation financing can involve trade finance products and transactions related to international trade. As part of the sanction controls, the service provider can take into account indicators of possible proliferation financing, among others:

- transactions involving persons or entities in country of proliferation concern;
- the customer or counterparty or its address is similar to one of the parties found on publicly available lists of designated persons or has a history of export control contraventions;
- customer activity does not match business profile, or end-user information does not match end-user’s business profile;
- order for goods is placed by firms or persons from countries other than the country of the stated end-user;
- a transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped;
- a transaction involves possible shell companies;
- a trade finance transaction involves shipment route through country with weak export control laws or weak enforcement of export control laws;
- inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.

12. Specific legal requirements and risk indicators per sector

12.1 Introduction

This Chapter provides sector-specific risk indicators which a service provider must consider when undertaking business risk assessments and customer risk assessments.

This Chapter must be read in conjunction with other Chapters in this Handbook which detail the requirements in relation to the identification and management of risk, including the undertaking of business risk assessments and customer risk assessments.

Chapters 4.4 ad 5.2 also provide more general risk factors which should be considered by all service providers. These risk indicators will be relevant for all financial and non-financial service providers. Such general risk indicators include for instance clients being PEPs, particularly in conjunction with additional risk factors. Geographical risk factors are generally also applicable to all service providers. These generally relate to the client, the UBO of the client or a beneficiary be based in or associated with a jurisdiction associated with higher ML/TF risk or the funds coming from a jurisdiction associated with higher ML/TF risk.

The sections below provide per type of financial service provider and non-financial service provider a description of risk indicators concerning customers, products and transactions, and delivery channels. These are not exhaustive lists of risk indicators and following them does not guarantee compliance with the AML/CFT requirements. The indicators do not necessarily indicate unusual activity but should be a signal to the service provider to further examine the client or transaction. A service provider should take a holistic view of the risks associated with a business relationship or transaction and note that isolated risk indicators do not necessarily make a business relationship or occasional transaction high or low risk overall.

The sections below also detail specific statutory requirements applicable to the sector concerned.

12.2 Banks

This section focuses specifically on retail banking. Retail banking means the provision of banking services to natural persons and small and medium sized enterprises. Examples of retail banking products and services include current accounts, mortgages, savings accounts, consumer and term loans and credit lines.

Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and business relationships, retail banking is vulnerable to terrorist financing and to all stages of the money laundering process. At the same time, the volume of business relationships and transactions associated with retail banking can make identifying money laundering and terrorist financing risk associated with individual relationships and spotting suspicious transactions more challenging.

12.2.1 Statutory requirements

Pursuant to Article 8, paragraph 2, subsection c, of the AML/CFT State Ordinance a service provider being a bank can open an account, before the identity of the customer has been verified, provided it guarantees that this account cannot be used before verification has taken place.

12.2.2 Risk factors

Customer risks

The following factors may contribute to increasing risk:

- The nature of the customer, for example:
    - legal persons whose structure makes it difficult to identify the UBO;
    - the customer or the UBO of the customer is a PEP;
    - the customer is a cash-intensive undertaking;
    - the customer is an undertaking associated with higher levels of ML risk, for example certain money remitters and gambling businesses;
    - the customer is an undertaking associated with a higher corruption risk, for example extractive industries or arms trade;
    - the customer is a non-profit organization that supports jurisdictions associated with an increased or active terrorism threat;
    - the customer is a new undertaking without adequate business profile or track record;
    - the customer is a non-resident;
    - the customer's UBO cannot easily be identified, for example because the customer's ownership structure is unusual, unduly complex or opaque or because the customer issues bearer shares.

- The customer's behavior, for example:
    - the customer is reluctant to provide CDD information or appears deliberately to avoid face to face contact;
    - the customer's evidence of identity is in a non-standard form for no apparent reason;
    - the client is nervous without a valid reason;
    - the customer's behavior or transaction volume is not in line with that expected from the category of customer to which he belongs, or is not expected based on the information the customer provided at account opening;
    - the customer's behavior is unusual, for example the customer unexpectedly and without reasonable explanation accelerates an agreed repayment schedule, either by means of lump sum repayments, or early termination; deposits or demands pay-out of high-value bank notes without apparent reason; increases activity after a period of dormancy, or makes transactions that appear to have no economic rationale;.

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

- the product's features might favor anonymity;
- the product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected, for example for mortgages or loans;
- frequent deposits by others than the account holder, which are not appropriate for the client's profession or work;
- there is a striking turnover on the account, which is disproportionate to the client's profession or work or business activities;
- the customer seemingly breaks transactions into smaller transactions to avoid raising attention to larger transactions;
- a large cash transaction in small denominations, with uncounted money, in unusual packaging;
- incoming payments from typical offshore financial centers;
- outgoing payments go to parties / countries that do not fit the client's profile;
- the product places no restrictions on turnover, cross-border transactions or similar product features;
- new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products where these are not yet well understood;
- lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identity of parties guaranteeing the loan are hard to verify;
- an unusually high volume or large value of transactions.

Delivery channel risk factors

The following factors may contribute to increasing risk:

- non-face to face business relationships, where no adequate additional safeguards are in place, for example electronic signatures or electronic identification certificates;
- reliance on a third party's CDD measures in situations where the bank does not have a long-standing relationship with the referring third party;
- new delivery channels that have not been tested yet.

Virtual assets risk factors

The following factors may contribute to increasing risk:

- Customers that are active on the Darkweb;
- Large amounts for each virtual asset transaction;
- Large quantities of virtual assets from private persons, which quantities are not common for an average private person;
- The services of a virtual asset provider solely serve to generate anonymity;
- Persons who make use of the services of virtual asset provider are persons who want to prevent their identity from being exposed;
- Paying and willingness to pay high commission fees for converting (selling) virtual assets in exchange for fiat currency or against cash, compared to commission fees charged by normal virtual asset exchanges;
- The virtual assets have a history (above average) of one or more mixers or trade history on the Darkweb;
- A trader cannot be found under his own name on the internet, or is not registered with the Chamber of Commerce or not known with the tax authority for exchange activities.

12.3 Money transfer companies and exchange offices

The nature of the service provided can expose money remitters to ML/TF risk. This is due to the simplicity and speed of transactions, their worldwide reach and their often cash-based character.

Furthermore, the nature of this payment service and type of transactions means that money remitters and exchange offices also carry out occasional transactions rather than establish a business relationship with their customers, which means that their understanding of the ML/TF risk associated with the customer may be limited. The brevity of contacts is a significant vulnerability.

Currency exchanges specifically are an important link in the money laundering chain, particularly during the placement stage. Once the money has been exchanged, it is difficult to trace its origin.

12.3.1 Statutory requirements

Pursuant to Article 6, paragraph 1, subsection c, of the AML/CFT State Ordinance a financial service provider must perform CDD when carrying out a money transfer as meant in Article 1 of the SOSMTC in or from Aruba.

12.3.2 Risk factors

Customer risk factors

The following factors may contribute to increasing risk:

- The nature of the customer, for example:
    - the customer is a legal person whose structure makes it difficult to identify the UBO;
    - the customer or the UBO of the customer is a PEP;
    - the customer owns or operates a business that handles large amounts of cash;
    - the customer is a non-resident.

- The customer's behavior:
    - the customer's needs may be better serviced elsewhere, for example because the money remitter is not local to the customer or the customer's business;
    - the customer appears to be acting for someone else; for example, others watch over the customer or stay visible outside, or the customer reads instructions from a note;
    - the customer's behavior makes no apparent economic sense, for example the customer accepts a poor exchange rate or high charges unquestioningly, requests a transaction in a currency which is not official tender or commonly used in the jurisdiction where the customer and/or recipient is located or requests or provides large amounts of currency in either low or large denominations;
    - the customer requests currency in large denomination notes without a logical explanation;
    - the client is nervous without a valid reason;
    - the customer's transactions stay just below applicable thresholds;
    - the customer's use of the service is unusual, for example he sends or receives funds to or from himself or sends funds on immediately after receiving them;
    - the customer appears to know little or is reluctant to provide information about the beneficiary;
    - several of the service provider's customers transfer funds to the same beneficiary or appear to have the same identification information, e.g. address or telephone number;
    - an incoming transaction is not accompanied by the required information on the payer or beneficiary.
    - the amount sent or received is at odds with the customer's income (if known);

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

- the customer seemingly breaks transactions into smaller transactions to avoid raising attention to larger transactions;
- a large cash transaction in small denominations, with uncounted money, in unusual packaging;
- exchange of large amounts or frequent exchanges that are not related to the customer's business.
- the product or service have a global reach;
- the transaction is cash-based or funded with anonymous prepaid cards;
- transfers are made from one or more payers in different countries to a local payee;
- transfers go to beneficiaries / countries that do not fit the client's profile.

Delivery channel risk factors

The following factors may contribute to increasing risk:

- the delivery channel used provides a degree of anonymity;
- the service is provided entirely online without adequate safeguards;
- the money transfer service is provided through agents who:
    - represent more than one principal;
    - have unusual turnover patterns compared to other agents in similar locations, e.g. unusually high or low transactions sizes, unusually large cash transactions, a high number of transactions that fall just under the CDD threshold, or undertake business outside normal business hours;
    - undertake a large proportion of business with payers or beneficiaries from jurisdictions associated with higher ML/TF risk;
    - appear to be unsure about, or inconsistent in, the application of group-wide AML/CFT policies; or
    - are not from the financial sector and conduct another business as their main business.
- the money transfer service is provided through a large network of agents in different jurisdictions.
- The money transfer service is provided through an overly complex payment chain, for example with a large number of intermediaries operating in different jurisdictions or allowing for untraceable (formal and informal) settlement systems.

12.4 Insurance companies and insurance brokers

Life insurance products are designed to financially protect the policyholder against the risk of an uncertain future event – such as death, illness or outliving savings in retirement (longevity risk). The protection is achieved by an insurer who is pooling the financial risks many different policyholders are faced with. Life insurance products can also be bought as investment products or for pension purposes.

Life insurance products are provided through different distribution channels to customers who may be natural or legal persons or legal arrangements. The beneficiary of the contract may be the policyholder or a nominated or designated third party; the beneficiary may also change during the term and the original beneficiary may never benefit.

Most life insurance products are designed for the long-term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds from crime.

12.4.1 Statutory requirements

Pursuant to Article 10, paragraph 1, subsection b, of the AML/CFT State Ordinance simplified CDD measures may be applied when it concerns the carrying out of a transaction or the entering into a business relationship related to 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.-;

Pursuant to Article 8, paragraph b, of the AML/CFT State Ordinance a service provider being a life insurer may identify the beneficiary of a policy and verify the identity, after the business relationship has been entered into; in this case, the identification and the verification of the identity must take place on or before the date of payment, or on or before the date on which the beneficiary wants to exercise his rights arising from the policy;

12.4.2 Risk factors

Customer and beneficiary risk factors

The following factors may contribute to increasing risk:

- the nature of the customer, for example:
    - legal persons whose structure makes it difficult to identify the UBO;
    - the customer or the UBO of the customer is a PEP;
    - the beneficiary of the policy or the UBO of this beneficiary is a PEP;
    - the customer's age is unusual for the type of product sought (e.g. the customer is very young or very old);
    - the contract does not match the customer's wealth situation;
    - the customer's profession or activities are regarded as particularly likely to be related to money laundering, for example because they are known to be very cash intensive or exposed to high corruption risk.
    - the contract is subscribed by a 'gatekeeper' such as fiduciary company, acting on behalf of the customer;
    - the policyholder and/or the beneficiary of the contract are companies with nominee shareholders and/or shares in bearer form.

- the customer's behavior in relation to the contract, for example:
    - the customer frequently transfers the contract to another insurer;
    - frequent and unexplained surrenders, especially when the refund is done to different bank accounts;

- the customer requests for exemption on the service provider's policies and procedures relating to cash;
- the customer makes unexpected use of 'cooling off' periods, in particular where the refund is made to an apparently unrelated third party;
- the customer incurs a high cost by seeking early termination of a product;
- the customer transfers the contract to an apparently unrelated third party;
- the customer's request to change or increase of the sum insured and/or of the premium payment are unusual or excessive.

- the customer's behavior in relation to the beneficiary, for example:
  - the insurer is being made aware of a change in beneficiary only when the claim is made;
  - the customer changes the beneficiary clause and nominates an apparently unrelated third party;
  - the insurer, the customer, the UBO, the beneficiary or the UBO of the beneficiary are in different jurisdictions.

- the customer's behavior in relation to payments, for example:
  - the customer uses unusual payment methods, such as cash or structured monetary instruments or other forms of payment vehicles fostering anonymity;
  - payments from different bank accounts without explanation;
  - payments from banks which are not established in the customer's country of residence;
  - the customer makes frequent or high value overpayments where this was not expected;
  - payments received from unrelated third parties;
  - catch-up contribution to a retirement plan close to retirement date.

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

- flexibility of payments, for example the product:
  - allows payments from unidentified third parties;
  - allows high value or unlimited value premium payments, overpayments or large volumes of lower value premium payments;
  - allows cash payments.
- ease of access to accumulated funds, for example the product:
  - allows partial withdrawals or early surrender at any time, with limited charges or fees;
- negotiability, for example the product:
  - can be traded on a secondary market;
  - can be used as collateral for a loan.
- anonymity, for example the product facilitates or allows anonymity of the customer.

Delivery channel risk factors

The following factors may contribute to increasing risk:

- non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification documents;
- long chains of intermediaries;
- intermediary is used in unusual circumstances (for example unexplained geographical distance).

12.5 Finance companies, factoring and leasing companies

In addition to the indicators for banks, other financial service providers, such as finance companies and companies providing factoring or leasing services need also take into account additional risk factors.

Loans may be one of the financial instruments that can pose a high risk of money laundering. Loans can be used in typologies such as financial and investment products susceptible to being used for money laundering operations, use of illegal funds to reduce debt or capitalize legitimate companies, and use of prepaid cards linked to savings account for money laundering. Moreover, (personal) loans can also be used to finance terrorist or terrorist acts or activities.

Leasing can pose a high risk of money laundering. Leasing could be used in typologies such as financial and investment products that can be used for money laundering operations, and the use of illegal funds to reduce indebtedness or capitalize legitimate companies.

12.5.1 Risk factors

Customer risk factors

The following factors may contribute to increasing risk:

- persons or entities that frequently close or open loans at the same service provider, without justification.
- loan or leasing applications in the name of several companies with the same UBO or representative and address.
- a loan or leasing application that bears no relation to the customer's normal business operations or that is intended for purposes other than those indicated;
- loan beneficiaries that are not directly associated to or have a justified relationship with the borrower.
- a customer has a lack of interest in obtaining financial advantages (e.g., offer of below-market interest rates).
- borrower gives no importance to the interest charged for early settlement of loan.
- a customer refuses to deliver personal or company information or to receive an official in the offices.
- a customer intentionally defaults on loans, with the purpose of collecting on the loan guarantee.

Product, service and transaction risk factors

The following factors may contribute to increasing risk:

- Loan application secured with assets of unknown origin.
- Early and/or immediate liquidation of the loan or of significant debentures, with no apparent justification.
- Premium payment is occasionally made in cash, with no apparent justification.
- Cash payment of premiums of different loans made by the same person, with no apparent justification.
- Payment of premiums of different loans, assigned to different borrowers, by fund transfers, made from one same bank account, with no apparent justification.
- Continuous cash payments on dates other than the due date, with no apparent justification.

12.6 Investment brokers

Investment management is the management of an investor's assets to achieve specific investment goals. It includes both discretionary investment management, where investment brokers take investment decisions on their customers' behalf, and advisory investment management, where investment brokers advise their customers on which investments to make but do not execute transactions on the customers' behalf.

Investment brokers usually have a limited number of private or institutional customers many of which are wealthy, for example high net worth individuals, trusts, companies, government agencies and other investment vehicles. The customers' funds are often handled by a custodian, rather than the investment broker. The ML/TF risk associated with investment management is therefore driven primarily by the risk associated with the type of customers investment brokers serve.

12.6.1 Risk factors

Customer risk factors

The following factors may contribute to increasing risk:

- the customer's behavior, for example:
    - the rationale for the investment lacks an obvious economic purpose;
    - a customer requests to repurchase or redeem a long-term investment within a short period after the initial investment or before the payout date without a clear understandable rationale, in particular where this results in financial loss or payment of high transaction fees;
    - a customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale;
    - the customer requests for exemption on the service provider's policies and procedures relating to cash.
    - a customer's investments do no correspond to the profile of the customer or history of investment and there is no reasonable explanation.
    - unwillingness to provide CDD information on the customer and the UBO;
    - frequent changes to CDD information or payment details;
    - a customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed;
    - the circumstances in which a customer makes use of the "cooling off" period gives rise to suspicion;
    - using multiple accounts without previous notification, especially when these accounts are held in multiple or high risk jurisdictions.
    - a customer wishes to structure the relationship in such a way that multiple parties, for example nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

- the customer's nature, for example:
    - the customer is a company or trust established in a jurisdiction associated with higher ML/TF risk;
    - the customer is an investment vehicle that carries out little or no due diligence on its own clients;
    - the customer is an unregulated third party investment vehicle;
    - the customer's ownership and control structure is opaque;
    - the customer or the UBO is a PEP or holds another prominent position that might enable them to abuse this position for private gain;
    - the customer is a non-regulated nominee company with unknown shareholders.

- the customer's business, for example the customer's funds are derived from business in sectors that are associated with higher financial crime risk.

Product, service or transaction risk factors

The following factors may contribute to increasing risk:

- transactions are unusually large;
- third party payments are possible;
- the product or service is used for subscriptions which are quickly followed by redemptions possibilities, with limited intervention by the investment manager.

Delivery channel risk factors

The following factors may contribute to increasing risk:

- non-face-to-face sales, such as online, postal or telephone sales, without adequate safeguards, such as electronic signatures or electronic identification documents;
- long chains of intermediaries;
- intermediary is used in unusual circumstances (for example unexplained geographical distance).

12.7 Legal Professional Sector: Lawyers, Notaries, Accountants, Tax advisors

Internationally, there is a widely held perception that some legal professionals are less aware of their AML/CFT obligations and will not report suspicions of ML or FT or at a minimum that suspicion reports by legal professionals are only made where suspicion has become near certainty.

From a criminal's perspective putting illicit funds through a legal professional's client account can clean them, whether the funds are sent back to the customer, on to a third party, or invested in some way. In light of this, legal professionals should only use client accounts to hold funds for legitimate transactions for customers, or for another proper legal purpose. The client account should solely be used for receiving funds intended to pay professional fees and disbursements from clients. No funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the professional is required to account for these funds.

The client account must not be used as a banking facility, as not only does this present an increased money laundering risk, but also a risk for fraud. The monitoring of each transaction to ensure its source legitimacy is critical. Legal professionals can seek to limit their exposure to these risk by developing and implementing policies on the handling of funds as well as restricting access to the client account in order to prevent unauthorized deposits into the client account.

It can be difficult to draw a distinction between holding customer funds for a legitimate transaction and acting more like a bank, but legal professionals should take care to not provide a de facto banking service for their customers. The same applies for other services, for instance trust services.

Accountants perform a number of important functions in helping their customers organize and manage their financial affairs. These services may include the provision of advice to individuals and businesses in such matters as investment, company formation, trusts and other legal arrangements, as well as the optimization of tax situations. Additionally, some may be directly involved in carrying out specific types of financial transactions (for example, holding or paying out funds relating to the purchase or sale of real estate) on behalf of customers.

Money launderers and persons or entities financing terrorism need the same services as legitimate customers, including financial and business advice. Even unaware involvement in money laundering can put the service provider at risk.

12.7.1 Statutory requirements

In accordance with article 1, paragraph 1, of the AML/CFT State Ordinance the following, amongst others, are categorized as "designated non-financial service providers":

- *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;*
- *a natural person, legal person, corporation or partnership that acts as an external registered accountant, an external accountant-administration consultant or a similar profession;*

The AML/CFT State Ordinance must be applied when these "designated non-financial services providers" perform the following activities performed in or from Aruba:

- *the purchase and sale of register objects, as well as the rights to which these objects can be subjected;*
- *the management of money, securities, or other asset components;*
- *the management of bank, savings, or securities accounts;*
- *the organization of contributions for the creation, operation, or management of companies;*

- *the creation, operation, or management of legal persons or similar legal entities, and the purchase and sale of businesses.*

In accordance with article 2, paragraph 2, of the AML/CFT State Ordinance, the CDD and reporting of unusual transactions regulations do not apply to activities of a lawyer, civil notary or tax advisor relating to the legal position of a client, his representation and defense in court, the giving of advice before, during, and after legal proceedings, or the giving of advice on instituting or avoiding legal proceedings.

This article aims to safeguard the professional secrecy of lawyers, notaries and tax advisors with regard to their work related to the legal position of a client, his representation and defense in court, the giving of advice before, during, and after legal proceedings, or the giving of advice on instituting or avoiding legal proceedings. These professions are therefore not obliged to perform CDD and report suspicions if the information in question has been obtained in situations where professional secrecy or professional privilege applies.

Pursuant to article 8, paragraph 1, subsection d, of the AML/CFT State Ordinance a designated non-financial service provider who is a civil notary can establish the identity of the client and verify the ultimate beneficial owner when identification is required pursuant to article 20, first section, of the State Ordinance on Civil Notaries (AB 1990 No. GT 69).

12.7.2 Risk factors

Customer risk factors

The following factors may contribute to increasing risk:

- the customer is excessively obstructive or secretive.
- factors indicating that the customer is attempting to obscure the understanding of its business, ownership or the nature of its transactions, for example:
    - the lack of a face-to-face introduction with the customer.
    - a subsequent lack of contact with the customer when this would normally be expected.
    - the beneficial ownership of the customer is unclear.
    - the position of intermediaries within the relationship is unclear.
    - inexplicable changes in the ownership of the customer.
    - the activities of the customer, where it is a legal person, are unclear.
    - the legal structure of the customer has been altered numerous times (for example, name changes, transfers of ownership or changes of corporate seat).
    - management appear to be acting according to the instructions of unknown or inappropriate person(s).
    - the ownership structure of the customer is unnecessarily complex.
- factors indicating certain transactions, structures, geographical location, international activities or other factors which are not in keeping with the service provider's understanding of the customer's business or economic situation, for example:
    - customer instructions or funds outside of the customer's personal or business sector profile.
    - services or transactions that take place outside the established business profile for the customer, and expected activities and/or transactions is unclear.
    - employee numbers or structure are out of keeping with the size or nature of the customer's business (for example, the turnover of a company is unreasonably high considering the number of employees and assets used).
    - the customer starts or develops an enterprise with unexpected profile or early results.
    - indications from the customer that they do not wish to obtain necessary governmental approvals/filings etc.
    - the customer offers to pay extraordinary fees for services which would not ordinarily warrant such a premium.

- customer industries, sectors or categories where opportunities for ML or FT are particularly prevalent, for example:
    - the customer has a high level of transactions in cash or readily transferable assets, among which illegitimate funds could be obscured.
    - The customer has unusually high turnover and/or profits and it is unclear with which activities this is connected
    - investments in real estate at higher/lower prices than expected.
    - large international payments with no business rationale.
    - unusual financial transactions with unknown sources.
    - the customer has multijurisdictional operations but does not have adequate centralized corporate oversight.

Product, Service and Transaction Risk Factors

The following factors may contribute to increasing risk:

- the instructions received from the customer are unusual in themselves, or they are unusual for the service provider or the customer.
- the instructions or case change unexpectedly with no logical reason for the changes.
- funds are received from an unknown or unexpected third party.
- the customer is reluctant to provide information on the source of the funds;
- the customer requests payment (for example, the proceeds of a property sale) be made to an unknown, un-associated or obscure third party, including a private individual, whose identity is difficult or impossible to check.
- the customer deposits funds into the service provider's client account prior to instructing the service provider.
- the customer requests that funds received into the service provider's client account are returned to another account of the customer or to an unknown or unconnected third party.
- the customer wants to use or uses the service provider's client account, other than for which it is intended (without any legal basis).
- the customer requests loss-making transactions which make no economic sense or where the loss is avoidable.
- the customer's instructions involve dealing with funds where the service provider suspects that they are being transferred to avoid the attention of a trustee in a bankruptcy case or a law enforcement agency.
- advice provided by the service provider on the setting up of legal persons or legal arrangements which may be used to obscure beneficial ownership or real economic purpose (including the setting up of trusts and companies, the change of name/corporate seat or other complex group structures).

12.8 Trust and company service providers

Trust and company service providers (TCSP) are often involved in some way in the establishment and administration of most legal persons and arrangements; and accordingly, in many jurisdictions they play a key role as the gatekeepers for the financial sector. However, TCSPs have often been used, wittingly or unwittingly, in the conduct of money laundering activities.

There has been an increasing international focus on the misuse of legal vehicles and, more specifically, the use of TCSPs to help facilitate this misuse. The use of complex multi-jurisdictional legal structures has continued to cause concern for many international organizations, governments and national regulatory authorities.

12.8.1 Statutory requirements

The AML/CFT State Ordinance is applicable to a trust and company service provider as meant in Article 1 of the State Ordinance Supervision Trust and Company Service Providers (AB 2009 No. 13).

Pursuant to article 6, paragraph 2, subsection d, of the AML/CFT State Ordinance, said State Ordinance must be applied when a trust and company service provider performs one of the following activities in or from Aruba:

- *to act as a founder of legal persons;*
- *the provision of a domicile, business address or accommodation, postal or administrative address to a company, corporation, or partnership, or another legal person of arrangement;*
- *to act or have someone else act as manager or representative of a trust;*
- *to act or have someone else act in the name of a shareholder;*
- *to act as the founder, manager, or liquidator of legal entities or bodies;*
- *to act as a local representative, director, or legal representative of legal entities or bodies;*
- *to make available natural persons living in Aruba or legal entities domiciled in Aruba as local representative, director, or legal representative;*
- *to be the trustee of a trust; e. to liquidate or arrange for third parties to liquidate legal entities or bodies;*
- *to sell or act as an intermediary in the sale of legal entities or bodies.*

12.8.2 Risk factors

Most of the risk indicators described above for the legal professional sector will also be relevant for the TCSP sector.

Customer risk factors

The following factors may contribute to increasing risk:

- the customer is excessively obstructive or secretive.
- unclear relationship between a potential UBO and signatories.
- the structure of the client's company makes it difficult to ascertain who the UBO is.
- the customer uses complex and opaque legal entities and arrangements.

Product, Service and Transaction Risk Factors

The following factors may contribute to increasing risk:

- a transfer from the account in the name of the company managed by the trust service provider into the account of the proxy, which funds are then withdrawn in cash by said proxy.

- payments are made via a company account managed by the trust service provider to other companies (whether or not these are abroad), without any agreement or accounts forming the basis for this.
- the payment of consultancy fees to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies;
- providing or receiving loans to or from apparently unrelated parties;
- multiple intercompany loan transactions and/or multi-jurisdictional transfers that have no apparent legal or commercial purpose.

12.9 Traders, including car dealers, jewelers and real estate agents

The growth of AML and CFT regulation and advances in technology have led to criminals using increasingly complex commercial arrangements that require the services of professionals outside of the financial services industry, including real estate agents. For example, investment of illicit capital in property is a classic method of laundering.

But also, the use of illicit funds to acquire cars, jewelry, art, antiquities or luxury object is a favored method to launder funds. These investments can be made by way of chain transactions in goods or property to disguise the source of funds, but also simply by paying for the goods or property with cash.

12.9.1 Statutory requirements

The AML/CFT State Ordinance is applicable to 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 real estate objects, vehicles, ships, aircraft, objects of arts, antiquities, and the rights to which these objects can be subjected; and to a natural person, legal person, or corporation which trades in precious metals, precious stones and jewels on a commercial or professional basis.

Pursuant to article 6, paragraph 2, subsection d, of the AML/CFT State Ordinance CDD has to be applied when a natural person, legal person or corporation trading in precious metals, precious stones, jewels, vehicles, vessels not being register objects, objects of art or antiquities on a professional or commercial capacity, performs cash transactions with a value of Afl. 25,000.- or more.

CDD must be applied to both the purchase and sale in or from Aruba of register objects, as well as the rights to which these objects can be subjected.

12.9.2 Risk factors

Customer Risk Factors

The following factors may contribute to increasing risk:

- the customer makes an offer on a property prior to conducting a viewing, particularly where the customer has no prior connection to the property.
- the customer buys expensive goods, without being interested in the quality, specific properties of those goods.
- the customer shows no interest in possible defects of the goods or property or has little interest in the possible costs of repairing them.
- the customer is willing to buy the expensive goods or property without attempting to negotiate or without asking for a discount.
- the customer is unable, or unwilling, to explain the source of the funds being used to make a goods or property purchase.
- the customer's finance arrangements appear unusual, for example, they do not involve a mortgage.
- the customer seeks to purchase a property using a complex structure of legal persons and/or legal arrangements, including nominee companies.
- the customer buys more than usual or more expensive goods than is usual for the type of customer.
- the customer tries to sell the newly purchased goods at a lower price without giving a valid reason.

Product, Service and Transaction Risk Factors

The following factors may contribute to increasing risk:

- the customer seeks to make large payments in cash.
- the customer deposits cash directly into the account of the trader at a service provider.
- payments are received from one or more third parties with no prior or obvious connection to the customer.
- the customer makes an offer significantly above the asking price for a property with no obvious economic rationale.
- the funds for purchase are received from one party, with the beneficial ownership of the property assigned to a separate, unrelated party.
- the purchaser of a property seeks to sell the same property shortly after acquiring it.
- funds received from a customer are requested to be repaid to a third party where a property transaction, for whatever reason, does not take place.
- the buyer of the property let a lower price be recorded in the deed than the agreed price, where the difference will be settled between the buyer and seller privately.
- transactions are being made in order to hide origin of the funds.
- the buyer shows no interest in the past or current occupation of the apartment complex similar kind of property.
- the owner of property changes quickly without a profit and client is not interested in making a profit.
- the client shows no or little interest in the property or location before buying. Nor doesn't he show any interest in possible necessary repairs.
- the client is reluctant or has objections to have personal contact with the real estate agent or notary.

12.10 Pawnshops | compra y venta

Pawnshops are covered by the AML/CFT State Ordinance as businesses that grant credits and buy goods such as jewelry, objects of art, antiquities and other valuable objects. With respect to the ML/TF risks, pawnshop must take the risk of dealing in stolen or fraudulent products into account. As with all valuable objects, diamonds, jewels and precious metals are attractive to thieves, and pawnshops must be aware of the risks of trading in stolen products. Pawnshops should remain alert to the possibility of being offered stolen goods or fraudulent goods.

12.10.2 Risk factors

Customer Risk Factors

The following factors may contribute to increasing risk:

- the customer pays objects which unmistakably come from crime.
- the customer often pawns objects but does not pay off his debt or shows no interest in paying off the loan or obtaining the objects.
- the customer pawns objects and accepts a price far below the market value of those objects.
- the customer tries to use fake or falsified identification documents.
- the customer provides incomplete or incorrect information.
- the customer ceases with the transaction when asked about the goods or his/her identity.
- the customer appears to be acting for someone else; for example, others watch over the customer or stay visible outside, or the customer reads instructions from a note.

Product, Service and Transaction Risk Factors

The following factors may contribute to increasing risk:

- a large cash transaction in small denominations, with uncounted money, in unusual packaging.
- the origin of the object is unknown or cannot be explained by the customer.
- a valuation report is submitted with a price that does not correspond with the value of the object as estimated by the pawn shop.
- an object originates from a country known for theft of cultural treasures.
- a rare object of offered that hardly ever is offered.

12.11 Casinos

The nature and expanding scope of the casino sector presents a number of challenges for AML/CFT implementation. For instance, casinos are often cash intensive businesses, often operating 24hrs per day, with high volumes of large cash transactions taking place very quickly. Moreover, sometimes casinos offer financial services (e.g., foreign exchange).

Gaming-related tourism involves movement of funds that may pose particular ML risks, and due to seasonal factors casino staff turnover can be high, which can lead to weaknesses in staff training and AML/CFT competencies.

12.11.1 Statutory requirements

A casino as meant in Article 1, first section, of the State Ordinance Games of Hazard (AB 1990 No. GT 44) has to apply CDD when it performs a cash transaction with a value of Afl. 5,000.- or more.

A casino has to report to the FIU all cash transactions of Afl. 5.000,= or more (objective indicator).

12.11.2 Risk factors

Customer Risk Factors

The following factors may contribute to increasing risk:

- the customer is a high-net worth customer;
- the customer does not want to identify him/herself, or does not want to provide additional information;
- the customer uses third party to buy in and/or cash out;
- customers come in and/or leave together but act like they do not know each other during buy in/cash out/play.
- the customer provides different information regarding profession or employment;
- the amount of casino chip purchases is not in line with the customer's reported profession or employment.

Product, Service and Transaction Risk Factors

The following factors may contribute to increasing risk:

- the incoming flow of funds consists of many small amounts and the outflow of large amounts or vice versa;
- repayment to the client to another account, then the account from which the money was deposited;

- cash buy in with pay out in another currency, in larger denominations, or by means of a check or a fund transfer;
- buy in and cashing out of casino chips with minimal play;
- credit card cash advances in casinos used to buy chips;
- chips redeemed for casino cheques.