Centrale Bank van Aruba (CBA): Questions and Answers (Q&A) regarding the AML/CFT State Ordinance

Introduction

On June 1, 2011, the State Ordinance for the Prevention and Combating of Money Laundering and Terrorist Financing (AML/CFT State Ordinance) was enacted. This state ordinance contains comprehensive rules for, inter alia, the application of customer due diligence (CDD), reporting of unusual transactions, recordkeeping, supervision, and enforcement.

On June 1, 2011, the CBA issued a Handbook for the prevention and detection of money laundering and combating the financing of terrorism for financial and trust service providers regulated by the CBA, (AML/CFT Handbook). This Handbook outlines the legal obligations of the regulated financial and trust service providers (Statutory and Regulatory Requirements). Further, the AML/CFT Handbook provides guidance on ways to comply with the Statutory and Regulatory Requirements and best practices.

In addition, the CBA issued Guidance Notes for designated non-financial service providers and financial non-regulated service providers (Guidance Notes). These Guidance Notes provide guidance to assist service providers to design a policy document and accompanying CDD procedures to risk rate their existing customer base.

On the CBA's website the aforementioned laws, regulations, policy documents, and guidance (http://www.cbaruba.org/cba/do/getPage/page/amlcft-state-ordinance.html) can be found.

This Q&A-document is designed to provide a better understanding of the requirements of the AML/CFT State Ordinance and related rules and regulations and also to give practical guidance in meeting those requirements.

Status of the Q&A

This Q&A document is not legally binding. It is a tool to help service providers interpret and apply the AML/CFT requirements in the particular circumstances of their business, products, services, transactions, and customers. The Q&As must always be read in conjunction with the AML/CFT State Ordinance and the AML/CFT Handbook. In case of contradiction between the Q&A document and the text of the AML/CFT State Ordinance and the AML/CFT Handbook, the AML/CFT State Ordinance and the AML/CFT Handbook prevail.

Updating the Q&A

This Q&A document will be reviewed periodically and, where necessary, questions/answers will be updated and/or added.[1]

Structure of the Q&A

This Q&A document is structured as follows:

- Part A contains general questions regarding the AML/CFT State Ordinance and its background.
- Part B addresses questions concerning CDD.
- Part C addresses the required business risk assessment and policies, procedures, and measures that a service provider must have in place to prevent and combat money laundering and terrorist financing.
- Part D contains questions on the functions of the money-laundering compliance officer (MLCO) and the money-laundering reporting officer (MLRO).
- Part E addresses questions about reporting unusual transactions.

[1] On March 21, 2014, four (4) new Q&A's were added to this document. Please refer to the new Q&A numbers 32, 33, 35 and 36 (bolded for easy reference).

- Part F addresses questions regarding enforcement measures that the CBA can apply in the event of non-compliance.

General

1. What is the purpose of the AML/CFT State Ordinance?

   The purpose of the AML/CFT State Ordinance is to set measures and provisions to prevent and combat money laundering and terrorist financing thus safeguarding the integrity of the financial sector and other sectors vulnerable to money laundering and terrorist financing.

2. Which service providers fall under the scope of the AML/CFT State Ordinance?

   The AML/CFT State Ordinance introduces the generic term "service provider", which in turn is subdivided into "financial service provider" and "designated non-financial service provider". A financial service provider is anyone who on a commercial basis conducts one or more of the activities or operations to or for the benefit of a client as mentioned in article 1 of the AML/CFT State Ordinance. Financial service providers regulated by the CBA fall under the scope of the AML/CFT State Ordinance as well as financial service providers not regulated by the CBA, i.e., insurance brokers, investment business, and stock exchanges.

   Examples of designated non-financial service providers are casinos, lawyers, notaries, accountants, tax advisors, and certain dealers in high value goods such as jewelers, real estate agents, and car dealers.

3. Why were the State Ordinance on Identification when Providing Services (SOIPS) and the State Ordinance on the Reporting of Unusual Transactions (SORUT) replaced by the AML/CFT State Ordinance?

   In 2008, the Financial Action Task Force (FATF[2]), together with the Caribbean Financial Action Task Force (CFATF[3]) conducted an evaluation of the Aruban AML/CFT system. The mutual evaluation report assessed Aruba's level of compliance with the FATF Recommendations. It identified many areas of good practice, and also made recommendations on how to strengthen certain aspects of the system. To implement strong AML/CFT defenses, the SOIPS and SORUT have been replaced by the AML/CFT State Ordinance.

4. What are the main differences between the SOIPS/SORUT and the AML/CFT State Ordinance?

   The AML/CFT State Ordinance includes:

   - Introduction of CDD
   - A risk-based approach
   - Obligation to have in place adequate AML/CFT policies, procedures, and measures

[2] The FATF is an intergovernmental body established in 1989 whose purpose is to develop and promote policies to combat money laundering and terrorist financing at both national and international levels. The Kingdom of the Netherlands and, thus, Aruba is a FATF member.

[3] The CFATF is a regional body similar to FATF and with similar functions. The CFATF comprises 29 states of the Caribbean Basin (including Aruba) and was established as the result of meetings convened in Aruba in May 1990 and Jamaica in November 1992. The main objective of the CFATF is to achieve effective implementation of and compliance with its recommendations to prevent and control money laundering and to combat the financing of terrorism.

- Obligation to have a Money Laundering Reporting Officer (MLRO) and a Money Laundering Compliance Officer (MLCO)
- Recordkeeping obligation for 10 years
- An increase in the maximum administrative and criminal fines to Afl. 1 million
- Violations by a legal entity may be attributed to individuals (see Q&A 50)

5. Can the CBA advise me of the course of action I should take in specific cases?

The CBA does not give advice on specific cases. However, the CBA can provide guidance concerning the interpretation of the AML/CFT State Ordinance and related rules and regulations.

A. Customer due diligence (CDD)

6. What are the basic CDD measures required under the AML/CFT State Ordinance?

The basic CDD measures involve:
- Identifying the customer and verifying the customer's identity using reliable, independent source documents, data, or information.
- Identifying the ultimate beneficial owner (UBO) and taking reasonable measures to verify the identity of the UBO such that a service provider is satisfied that it knows who the UBOs are.
- Identifying any third parties on whose behalf the customer is acting.
- Determining the purpose and intended nature of the business relationship.
- Keeping the CDD information up-to-date and monitoring the business relationship and transactions undertaken throughout the course of the relationship to assure that they are consistent with the service provider's knowledge of the customer and the UBO.

Relevant information:
- *AML/CFT State Ordinance: articles 3, 4, 5*
- *AML/CFT Handbook: Sections 3 and 4*

7. Who can be considered a "customer" or "client"?

The AML/CFT State Ordinance uses a broad definition for the term "customer": it means the natural person with whom or the legal person with which a business relationship is established or the person on whose behalf a transaction is carried out.

To avoid any misunderstanding, note that in line with article 8, paragraph 2, part c of the AML/CFT State Ordinance, the beneficiary of a life insurance policy also is considered a customer.

8. What does a "risk-based approach" mean?

A service provider must tailor its CDD measures to the risk-sensitiveness for money laundering or terrorist financing of the type of customer, business relationship, product, or transaction. Therefore, the service provider is required to develop a risk-based approach to determine the type and extent of CDD measures to apply to different types of customers, products, and services. For example, the type and extent of customer identification information and relationship information, the nature of verification of the information obtained, and the level of business relationship monitoring activity depend on the risk of the particular customer.

The resources and attention of the service provider should be geared to where they are most needed, i.e., the higher risk situations. This means that a service provider must do more when needed, but it can (and should) do less when possible. On the one hand, a risk-based approach creates flexibility for a service provider; on the other hand, it implies a greater responsibility.

Notwithstanding a service provider's own responsibility to decide when enhanced CDD measures are needed, or when less will do, the AML/CFT State Ordinance contains predetermined situations in which enhanced CDD measures must be taken (see Q&A 10) and situations in which simplified CDD measures are allowed (see Q&A 11).

Note that being identified as carrying a higher risk for money laundering or terrorist financing does not automatically mean that a customer is a money launderer or is financing terrorism. Similarly, identifying a customer as carrying a lower risk for money laundering or terrorist financing does not mean that the customer is not a money launderer or does not finance terrorism. Note also that over time, based upon the ongoing monitoring and review of the business relationship and customer risk profile, a customer risk level may change, i.e., a lower risk customer may migrate into a higher risk customer and vice versa.

Relevant information:
- *AML/CFT State Ordinance: article 6, paragraph 3*
- *AML/CFT Handbook: Section 1.5*

9. What does a risk profile entail?

A service provider must establish a risk profile of the customer and the UBO. To establish an adequate risk profile, the service provider must assess in any case:
- the purpose and intended nature of the business relationship;
- the nature of the transaction;
- the source and destination of the funds or other assets involved in the business relationship or transaction.

The service provider must obtain information about the customer and the expected business with regard to the following questions: what does the customer want, and why, and does it make sense?

A customer or 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 money laundering or terrorist financing activity.

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

Relevant information:
- *AML/CFT State Ordinance: article 6, paragraph 3*
- *AML/CFT Handbook: Section 3.8*

10. When must a service provider perform enhanced CDD measures?

Enhanced CDD must be performed if and when a business relationship or a transaction entails a higher risk of money laundering or terrorist financing. Enhanced CDD must be performed prior to

the business relationship or the transaction as well as throughout the course of the business relationship, in any case in the following situations:

- when a customer is not a resident of Aruba, respectively not established in Aruba;
- if a customer is not physically present for identification;
- if it concerns private banking;
- if the customer is a legal person, trust, or comparable entity intended as a private assets holding vehicle;
- if the customer is a body corporate or comparable entity with shares in bearer form or nominee shareholders;
- if the customer is a natural person, legal person, trust, or comparable entity that originates in a country or jurisdiction that does not apply or insufficiently applies the internationally accepted AML/CFT standards;
- if the customer is a politically exposed person (PEP);
- when entering into correspondent banking relations; and
- other situations to be determined by regulation of the Minister of Finance.

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

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

Relevant information:

- *AML/CFT State Ordinance: articles 11, 12, 13, 17, and 18*
- *AML/CFT Handbook: Section 3.12*

11. Pursuant to article 11, paragraph 1 of the AML/CFT State Ordinance, enhanced CDD measures must be applied to, among others, non-residents. However, if a customer resides in the Kingdom of The Netherlands, do I as service provider also have to apply enhanced CDD measures?

Article 11, paragraph 1 of the AML/CFT State Ordinance prescribes the situations in which a service provider must apply enhanced CDD measures. Unlike articles 12 and 17 of the AML/CFT State Ordinance, which prescribe the measures that should be taken with regard to PEPs and correspondent banking relationships, article 11 of the AML/CFT State Ordinance does not prescribe the nature of the enhanced CDD measures to apply. This means that the extent to which a service provider must apply enhanced CDD measures may vary depending on the nature of the risk; one size does not fit all. Based upon the service provider's own risk assessment, it can be the case that the enhanced CDD measures for customers residing in the Kingdom of The Netherlands differ from those applied for customers residing in other countries. In the end, a service provider must be satisfied that the higher risk is adequately mitigated by the enhanced CDD measures it applies.

Relevant information:

- *AML/CFT State Ordinance: article 11*
- *AML/CFT Handbook: Section 3.12*

12. What is a Politically Exposed Person (PEP)?

PEPs are understood to be individuals who are or have been entrusted with prominent public functions, as well as direct family members or close associates of these individuals.

Examples of individuals entrusted with prominent public functions include heads of state, heads of government, ministers, state secretaries, members of parliament, members of the supreme court, constitutional courts, other high tribunals that render judgments that generally are not open to appeal, member of courts of auditors, boards of directors of central banks, ambassadors, chargés d' affaires, high ranked army officers, members of executive management or supervisory bodies of state companies, and individuals holding positions at an international level, such as representatives with the United Nations.

"Direct family members" are understood to be (i) the husband or wife or partner who according to the relevant national law is considered equivalent to a husband or wife; (ii) the children and their husbands or wives or partners; and (iii) the parents.

"Close associates" are understood to be natural persons who (i) are known as a joint ultimate beneficiary of legal entities or legal constructions together with a PEP, or have other close business relationships with said persons; or (ii) are the sole beneficiary of a legal entity or legal construction known to have been established for the factual benefit of a PEP.

Relevant information:
- *AML/CFT State Ordinance: article 1 (and relevant explanatory notes to the AML/CFT State Ordinance)*
- *AML/CFT Handbook: Glossary and Section 3.12.3*

13. Pursuant to article 12, paragraph 2 of the AML/CFT State Ordinance, the decision to enter into a business relationship with or carry out an individual transaction for a PEP must be made or approved by senior management. Does this mean that all transactions carried out on behalf of a PEP require senior management approval?

It is important to point out that prior approval of senior management is required before entering into a business relationship with a PEP or carrying out an individual transaction for a PEP. If the service provider has a business relationship with a PEP, which has been approved by senior management, then no (additional) approval is required for individual transactions carried out as a part of that business relationship. This may be different if the individual transaction falls beyond the scope of the approval previously obtained. For example, if senior management approved the opening of a bank account for a PEP, separate approval is not required for each individual transfer or deposit. However, the granting of a mortgage loan, which is an unrelated financial service, requires prior approval from senior management.

Relevant information:
- *AML/CFT State Ordinance: article 12, paragraphs 2 and 3 of the AML/CFT State Ordinance*
- *AML/CFT Handbook: Section 3.12.3*

14. Will the CBA publish a list of PEPs?

The CBA is not going to publish a list of PEPs. Whether or not a customer is a PEP must be assessed by the service provider itself.

15. How can I identify a PEP?

Service providers must have an adequate policy and risk-based procedures to establish whether a (prospective) customer or UBO is a PEP. To identify PEPs or their direct family members or close associates, the following measures may be appropriate in addition to the standard CDD measures: (i) make inquiries regarding the PEP status of prospective customers during the customer acceptance process; (ii) consult publicly available information (i.e., the Internet); (iii) screen prospective customers against (electronic) databases of PEPs, developed internally or obtained from a reputable third party; and (iv) provide PEP-related training to relevant employees.

Relevant information:
- *AML/CFT State Ordinance: article 12, paragraph 1 of the AML/CFT State Ordinance*
- *AML/CFT Handbook: Section 3.12.3*

16. How should I monitor my business relationship with a PEP?

Service providers that have PEPs as customers or UBOs of customers must conduct ongoing monitoring of these business relationships. This includes, fund transfers to PEP accounts or to the accounts of their direct family members or close associates. Also service providers must be alert to these transactions and the risk that these transactions could include bribes or the proceeds from other illicit activity.

Service providers may set up their internal procedures for ongoing monitoring of these business relationships in a risk-based manner. It is important to understand that not all PEPs present the same level of risk. In assessing the risk of a PEP account holder, service providers should take into account various risk factors. Risk will vary depending on numerous factors, including the PEP's country of origin, the industry sector involved, and the products and services used. Risk also will vary depending on factors such as the nature of the position and the nature/purpose of the account. For instance, the parents of a member of the board of management of a foreign central bank with an ordinary payment account in Aruba will be less risk-sensitive than the wife of a head of state of a country with an increased risk of corruption, who opens a private banking account and deposits large sums of money. After the risk is established, care must be taken to ensure that the account transactions are consistent with the customer or UBO risk profile (see Q&A 9).

Relevant information:
- *AML/CFT State Ordinance: article 12, paragraph 2, part b*
- *AML/CFT Handbook: Sections 5.2 and 5.3*
- *FATF report: Specific Risk Factors in Laundering of Proceeds of Corruption (assistance to Reporting Institutions), June 2012 (http://www.fatf-gafi.org)*

17. When can a service provider apply simplified CDD measures?

Article 10, paragraph 1 of the AML/CFT State Ordinance describes types of customers that constitute a lower risk of money laundering and terrorist financing. A simplified CDD regime applies to customers so designated. They consist primarily of service providers governed by the AML/CFT State Ordinance or equivalent legislation and customers with a specific legal status. In addition, article 10, paragraph 2 of the AML/CFT State Ordinance states a number of products for which a simplified regime may be applied.

Relevant information:
- *AML/CFT State Ordinance: article 10*
- *AML/CFT Handbook: Section 3.11*
- *Ministerial Regulation recognized stock exchanges AML/CFT State Ordinance (Regeling erkende*
- *aandelenbeurzen LWTF) (2011, no. 66)*

18. How to determine whether you can proceed with applying CDD measures?

Service providers should gather sufficient data to assess whether a customer meets the requirements for a simplified regime. The service provider may ask for an extract from the trade register, entries in public registers, or other public listings.

Monitoring of these business relationships is always necessary to assess whether the account is indeed used for the reasons specified. If, for instance, there are indications that the customer is, or risks being involved in money laundering or terrorist financing, then the institution must perform a full CDD review.

The institution also should assess whether the account is held and used by the customer for his/her own use. For instance, credit institutions sometimes hold an account in their own name with another institution, but the funds in that account are from the credit institution's customer or group of customers and the transactions are carried out for the account and risk of that customer or group of customers. In these cases, the institution should consider whether the purpose of article 10 of the AML/CFT State Ordinance (i.e., simplified CDD due to low risk) is still being met or whether the institution must observe the provisions of article 3 of the AML/CFT State Ordinance vis-à-vis the customer(s) for whose account and risk it is acting or whether the relationship with the other bank must be treated as a higher risk.

Relevant information:
- *AML/CFT State Ordinance: article 10*
- *AML/CFT Handbook: Section 3.11*

19. Do I have to establish the purpose and intended nature of the transaction for every transaction?

No. As part of the basic CDD measures, a service provider is obliged to assess the purpose and intended nature of the *business relationship*. By gathering information about the purpose and envisaged nature of the business relationship, a service provider will be able to estimate possible risks that may arise from the provision of services to the customer and identify a pattern of expected business activity and transactions within the business relationship. Usually, some of the required information will already have been obtained during contact with the customer prior to the establishment of a business relationship. Also, the purpose of the relationship often will be apparent from the services or products used by the customer. If a transaction does not fit within the customer's risk profile (i.e. the expected business activity and transactions), additional measures must be taken. Understanding the source of funds and in higher risk relationships, the source of wealth, also is an important aspect of CDD**.**

Relevant information:
- *AML/CFT State Ordinance: article 3*
- *AML/CFT Handbook: Sections 3.7.1. and 3.7.2*

20. Must I refuse to render a service if I have doubts about the purpose or intended nature of the transaction?

Pursuant to article 9 of the AML/CFT State Ordinance, a service provider is forbidden to enter into a business relationship or carry out an individual transaction if a service provider has not applied or is not able to apply CDD measures or if the CDD review did not lead to the result envisaged by articles 3, 4, and 5 of the AML/CFT State Ordinance. As long as appropriate CDD measures are completed, the AML/CFT State Ordinance does not prohibit carrying out (unusual) transactions. Obviously, a service provider should ensure that he himself cannot be held liable for (complicity to) money laundering, including negligent money laundering (*schuldwitwassen*) or terrorist financing. Negligent money laundering would include any person receiving or holding monies who must reasonably suspect that the funds are the proceeds of crime.

Relevant information:
- *AML/CFT State Ordinance: article 9*
- *AML/CFT Handbook: Section 3.5*
- *Criminal Code: article 430d*

21. When must CDD measures be applied?

Article 6, paragraphs 1 and 2 of the AML/CFT State Ordinance prescribes the various situations per category of service providers in which CDD measures must be applied. In general, this means that all service providers must apply CDD measures if a business relationship is entered into. In addition, certain specific transactions (and thresholds) per category of service providers are prescribed.

Pursuant to article 8, paragraph 1 of the AML/CFT State Ordinance, CDD must be conducted before the start of the business relationship or before an occasional transaction is carried out. However, article 8, paragraph 2 of the AML/CFT State Ordinance provides for some exceptions. Under certain conditions, the verification of the identity of the customer and the UBO can be completed at a later stage if this is essential to avoid interrupting the normal conduct of business. In such exceptional cases, the purpose of the law should still be observed, namely, to prevent the use of service providers' services for money laundering or terrorist financing purposes.

Relevant information:
- *AML/CFT State Ordinance: articles 6 and 8*
- *AML/CFT Handbook: Sections 3.3 and 3.4*

22. In accordance with article 6, paragraph 1, subsection b of the AML/CFT State Ordinance, a service provider also must perform CDD when carrying out two or more related transactions with a combined value of at least Afl. 25,000.-. What criteria can be applied to determine whether several transactions are related?

Whether transactions are related will be assessed by the service provider on the basis of the type and specific circumstances of the transaction(s). This provision concerns transactions that are equivalent in a way that they can in fact be considered as one transaction. This provision aims to ensure that the structuring of transactions (*i.e. smurfing.*) does not lead to circumvention of CDD scrutiny. For instance, making several cash payments into a bank account during the day or within a few days may be considered related transactions. By contrast, this provision is not applicable to a company that daily pays the cash proceeds from its regular business operations into its own account, as such payments have an apparent economic purpose and are in line with the identified pattern of expected business activity and transactions (customer's risk profile).

Relevant information:
- *AML/CFT State Ordinance: article 6*

23. Can a service provider rely on CDD performed by a third party?

Each service provider is required to comply with the CDD requirements. Notwithstanding the obligation of other service providers involved with the customer or the transaction, every service provider has its own responsibility to apply appropriate CDD measures.

However, you may (partly) rely on the CDD measures, meant in article 3, paragraph 1, parts a, b and c of the AML/CFT State Ordinance that are performed by certain other service providers that have an established relationship with the customer and want to introduce that customer to you. This reliance may apply only for customers that are introduced by a financial service provider or by notaries, lawyers, tax advisors, or accountants (or persons exercising a similar legal profession) established in Aruba, other countries within the Kingdom of the Netherlands, the United States of America, or Canada. Note that you remain ultimately responsible for compliance with article 3, paragraph 1, parts a, b and c of the AML/CFT State Ordinance. Moreover, you must apply appropriate (enhanced) CDD measures and conduct ongoing CDD on the business relationship and scrutinize transactions carried out during the business relationship.

Relevant information:
- *AML/CFT State Ordinance: articles 15 and 16*
- *AML/CFT Handbook: Section 3.13*
- *Ministerial Regulation recognized introduction countries (Regeling erkende introductielanden LWTF) (2011 no. 65)*

24. Which documents are required for verification of the customer's identity?

A service provider must verify the identity of a natural person or a legal person domiciled in Aruba using documents, data, or information from a reliable and independent source. Moreover, the identity of a foreign legal person who is not domiciled in Aruba must be verified using reliable and internationally accepted documents, data, or information, or documents, data, or information recognized by law in the state of origin of the customer as valid means of identification.

The Ministerial Regulation verification documents AML/CFT State Ordinance provide non-exhaustive lists of documents that can in any case be used to verify the identity of a customer as required by article 19 of the AML/CFT State Ordinance.

Relevant information:
- *AML/CFT State Ordinance: article 19*
- *AML/CFT Handbook: Section 3.6*
- *Ministerial Regulation Verification Documents AML/CFT State Ordinance (Regeling verificatiedocumenten LWTF) (2012, no. 11)*

25. Copies of passports on file are expired. Should I obtain copies of valid ones?

A service provider must identify the customer and the UBO and verify their identity. "Identification" is the process whereby the customer's identification information is collected with

the objective to 'know your customer'. Depending on the risk category of the client, you do have to collect more identification information on the client. "Verification" is the process of checking the accuracy of identification information using – in short – trustworthy documents, data, or information on the basis of which the identity can be confirmed beyond a reasonable doubt. Verification also is based on risk: depending on the risk category, you must verify more components of the identification information, eventually also using additional verification methods.

A valid passport may very well be used to verify (certain) identification information. The CDD information obtained must be recorded and retained. In addition, service providers must insure that the CDD information is kept relevant and up-to-date, taking into account the risk associated with the customer. This also means that, where a particular relevant aspect of a customer's identity subsequently changes (such as change of name, nationality, or address), the service provider must take reasonable measures to re-verify that particular aspect of identity. Therefore, it is the responsibility of the service provider to have an adequate review process in place, again, on the basis of risk.

In view of the above, it can be concluded that having a copy of a valid passport on file is not a requirement. However, some service providers choose to make and retain a copy of the passport as proof of correct verification or to comply with recordkeeping requirements. Note that the review process may require you to re-verify changed identification information on the basis of a valid passport.

Relevant information:
- *AML/CFT State Ordinance: articles 3, 7, 19, and 33*
- *AML/CFT Handbook: Sections 3.6, 3.9, and 8.2*
- *Ministerial Regulation Verification Documents AML/CFT State Ordinance (Regeling verificatiedocumenten LWTF) (2012 no. 11)*

26. Who can be considered an ultimate beneficial owner ("UBO"), and why must I know the UBO?

If the customer is a legal entity, such as a legal person, foundation, or trust, then the institution should identify the UBO and verify his/her identity. This is a statutory requirement since criminals often use schemes involving (foreign) legal persons as a means to conceal the criminal source of funds.

The UBO is the natural person (i) who holds an interest of more than 25% of the capital interest or can exercise more than 25% of the voting rights in the shareholder meeting of a customer, or can in another way exercise actual control over a customer; (ii) 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 legal arrangement.

Persons who can "in another way excise actual control" over a customer will be directors (or equivalent persons comprising the mind and management) who have authority to operate a relationship or who can give the service provider instructions concerning the use or transfer of assets.

Relevant information:
- *AML/CFT State Ordinance: article 1*
- *AML/CFT Handbook: Section 3.6.2.2*

27. How far should I go to establish the identity of the UBO?

A service provider must identify the UBO and take reasonable measures to verify the UBO's identity in a way that the service provider is convinced of the UBO's identity. The identification requirement can be met by having the customer declare who the UBO('s) is (are). In addition, the service provider must take adequate risk-based measures to verify the identity of the UBO('s). These verification measures should enable the institution to obtain sufficient information to verify identity and to convince itself of the identity of the UBO('s). The institution does not have a choice as to whether or not to verify the identity of the UBO('s) depending on the risk involved. His/her identity should be verified in all cases, but the manner in which such verification occurs will be risk-based. Reasonable measures are measures that are commensurate with the money laundering and financing of terrorism risks.

Relevant information:
- *AML/CFT State Ordinance: article 3, paragraph 1, part b*
- *AML/CFT Handbook: Section 3.6.2.2.*

28. What do I have to do if I do not get any information or insufficient information about the UBO?

A service provider is prohibited from entering into a business relationship or carrying out a transaction if no CDD has been performed or if the CDD review, including the review of the UBO, has not produced the intended result. Also, if during the course of the business relationship you are no longer able to comply with the CDD requirements, you must terminate the business relationship promptly.

Relevant information:
- *AML/CFT State Ordinance: article 9*
- *AML/CFT Handbook: Sections 3.5 and 3.6.1.2*

29. A service provider must conduct ongoing monitoring of the business relationship and the transactions carried out during the course of this relationship. What is the purpose of monitoring, and how should I do this?

In addition to gathering sufficient information about a customer and UBO during the customer acceptance phase, monitoring of activity and transactions is of major significance to prevent and combat money laundering and financing of terrorism. On the basis of the information obtained on the customer and the UBO, a risk profile must be established. Such a risk profile will contain a pattern of expected business activity and transactions within each business relationship to provide a basis to identify unusual or higher risk activity and transactions that may indicate money laundering or financing of terrorism activity. (see Q&A 9)

A service provider should monitor a customer's account and his/her transactions. Monitoring allows the service provider to gain and maintain insight into the nature and background of customers and their financial conduct. The purpose of such monitoring is to, among other things, detect any changes in the transaction pattern and the possible occurrence of situations presenting an enhanced risk. An effective monitoring system requires a bank to identify unusual and higher risk activity, to maintain up-to-date CDD information, and to ask pertinent questions to determine whether the activity or transactions identified have a rational explanation. The scrutiny of activity

and transactions may involve requesting additional CDD information. Questions that could be asked in this respect are: do the transactions serve an economic or commercial purpose, are exceptionally large amounts of money involved, are deposits or withdrawals disproportionate to the customer's ordinary/expected business, do the account movements and the transactions fit with the customer's operations, are transactions carried out to and from countries that present an enhanced risk?

Monitoring of the relationship with the customer and the customer's transactions may be tailored to the type of relationship, which may vary by sector and product. Monitoring may take place at various levels depending on the risk and size of activities. The higher the risk, the more intensive (in terms of frequency and depth) the monitoring efforts should be.

Examples of monitoring methods are:

- Spot checks: targeted checks of accounts and transactions, e.g., of specific groups of customers, or of accounts and transactions earlier deemed to pose an enhanced risk on the basis of reports to the *Meldpunt Ongebruikelijk Transacties* (MOT) or otherwise.
- Manual monitoring: the account manager knows his/her customers and their financial behavior. Deviations from the customer's normal behavior will immediately be spotted by the account manager. Key factors in this type of monitoring are an effective and realistic number of customers to be controlled as well as the expertise and competence of the persons carrying out the control operations.
- Periodic management surveys/reports: this type of monitoring is used when the numbers of customers and transactions is fairly manageable. A daily, weekly, or monthly printout of turnover, balance, exceeding of limits, fees charged, and so forth may indicate which accounts require closer scrutiny.
- Monitoring by "hard indicators": this method is used for an initial filtering on the basis of turnover, maximum balance, transaction amounts, countries of origin or destination, risk sectors and so forth.
- "Intelligent" transaction monitoring: this type of monitoring is based on the profiling of each account or customer. Such a profile can be made up of turnovers, transaction amounts, contra accounts, transaction frequency, transaction particulars, and so forth. Each element of the profile can be assigned a particular weight. Each new transaction will be checked against the profile, with the transaction that differs the most from the profile getting the highest risk grade. All transactions that exceed a chosen risk grade call for further investigation. Only then can it be determined whether a transaction should be considered unusual.

Depending on the risks involved, the service provider may employ one or more of these monitoring methods.

Relevant information:

- *AML/CFT State Ordinance: article 3, paragraph 1, subsection d*
- *AML/CFT Handbook: Chapter 5*
- *Monitoring Screening and Searching Wolfsberg Statement (*http://www.*wolfsberg-principles.com)*

30. Can computer records be maintained in lieu of original documents if all of the same information is captured?

Yes, as long as the recordkeeping requirements are complied with. The records must in all cases be accessible and kept in a way that transactions can be reconstructed at all times and be

submitted to the competent authorities on first demand. Note that the recordkeeping requirements are essential to facilitate effective investigation, prosecution, and confiscation of criminals. If law enforcement agencies, either in Aruba or elsewhere, are unable to trace criminal proceeds due to inadequate recordkeeping, then prosecution for money laundering and confiscation of criminal proceeds may not be possible. With this in mind, records may be kept (i) as original documents; (ii) as photocopies of original documents (certified where appropriate); (iii) in scanned form; or (iv) in computerized or electronic form.

Relevant information:
- *AML/CFT State Ordinance: article 33*
- *AML/CFT Handbook: Section 8.1*

B. AML/CFT business risk assessment and policies, procedures, and measures

31. A service provider must carry out periodic evaluations to assess if and to what extent it is vulnerable to money laundering and terrorist financing because of its activities. How broad must this business risk assessment be?

The business risk assessment must cover 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.

Relevant information:
- *AML/CFT State Ordinance article 46, paragraph 3*
- *AML/CFT Handbook: Section 2.3*

32. Why must I carry out an AML/CFT business risk assessment?

The objective of conducting a business risk assessment is to identify aspects of your business that may be susceptible to money laundering and terrorist financing. You understand your business better that anyone else. Therefore, you are best placed to identify the risks your business faces from money laundering and terrorist financing. Without a (proper) assessment of the specific risks applicable to your own business, rather than the generic risks applicable to the sector, it is difficult to develop adequate AML/CFT policies, procedures, and measures to mitigate the specific risks your business confronts or may confront. Subsequently, your business could become inadvertently involved in money laundering and terrorist financing.

Relevant information:
- ***AML/CFT Handbook: Section 2.3***

33. Why is it important for me to understand why money laundering and terrorist financing occur?

In the process of analyzing money laundering and terrorist financing risks, it is crucial to have a general understanding of why money laundering and terrorist financing occur. The acts of laundering money and financing terrorism are done to facilitate crime and terrorism

more broadly. Profit is fundamental to the goals of most crimes, and, therefore, criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds. In order for terrorists to carry out their operations, attacks or maintain an infrastructure of organization support, they need to have the ability to collect, receive, and move funds. The availability of working capital is also fundamental for both criminals and terrorists to sustain their networks.

Relevant information:
- ***AML/CFT Handbook: Section 2.3***

34. What does a business risk assessment entail?

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

Relevant information:
- *AML/CFT Handbook: Section 2.3*

35. How do I set up a business risk assessment? Where do I start?

The business risk assessment process can be divided into three stages: the identification stage, the analysis stage, and the evaluation stage.

Identification stage
The process of identification in the context of an AML/CFT business risk assessment starts by developing an initial list of potential risks or risk factors your business faces when combating money laundering and terrorist financing. The business risk assessment must cover 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. Each of these factors must be addressed separately in the business risk assessment.

Analysis stage
After the list of potential risks or risk factors have been identified they must also be analyzed. Analysis lies at the heart of the AML/CFT risk assessment process. It involves consideration of the nature, sources, likelihood, consequences, and impacts of the identified risks. Ultimately, the aim of this stage is to gain a full understanding of each of the risks - as a combination of threat, vulnerability, and consequence - in order to work towards

assigning some sort of relative value or importance to them. Subsequently, priorities can be determined for addressing the risks. The priorities can contribute to development of an AML/CFT strategy for the mitigation of these risks.

Evaluation stage
It is important that at regular intervals an AML/CFT business risk assessment is performed (e.g., annually) or in case of significant changes, for example, in the client base or environment in which your company operates, the AML/CFT business risk assessment is re-evaluated and, if necessary, adjusted.

Relevant information:
- ***AML/CFT Handbook: Sections 2.3 and 3.8.1***

36. <u>What tools can I use to carry out a business risk assessment?</u>

When carrying out a business risk assessment you must start with describing the risks your business faces from money laundering and terrorist financing. Subsequently, you must consider each of the at-risk areas you have identified, and analyze the likelihood that your business will be used for money laundering and terrorist financing. This involves considering each aspect of the at-risk areas you have identified, together with your business experience, information published by the CBA and MOT, and publications of international organizations, such as reports of the Financial Action Task Force (FATF).

Relevant information:
- ***FATF Typologies reports, Guidance and best practices reports, and Risk Based Approach reports (www.fatf-gafi.org)***
- ***Report of the National money laundering and terrorist financing risk assessment conducted by Aruba in 2012 (www.cbaruba.org, under the heading 'Supervision' and then under the section 'AML/CFT framework')***

37. <u>The AML/CFT procedures and measures of a service provider must, inter alia, consider the periodic evaluation of the effectiveness of those procedures and measures. By whom and how often must the effectiveness be evaluated?</u>

It is important that the management of the service provider be able to reach an independent conclusion as to the effectiveness of the AML/CFT procedures and measures and monitor adequate follow-up action. Management may wish to use the MLCO and MLRO to provide information and advice to assess the AML/CFT procedures and measures. Depending on the size, nature, and risks of the business (in any case if it concerns regulated financial and trust service providers), a periodic assessment of the effectiveness of the AML/CFT procedures and measures by a dedicated, independent, and adequately resourced internal audit function is required. If the service provider does not have an internal audit department, the assessment must be conducted by an independent third party.

The frequency and scope of the assessment must be determined by the service provider's business risk assessment.

C. Money Laundering Compliance Officer (MLCO) and Money Laundering Reporting Officer (MLRO)

38. Must the MLCO and the MLRO be Aruba residents?

Service providers must have a person in charge of oversight of compliance with the laws and regulations in the area of the prevention and combatting of money laundering and terrorist financing (the MLCO). The MLCO function (not to be confused with the internal audit function, see Q&A 33), must be established to ensure adequate execution of its tasks and responsibilities.. MLCOs are not necessarily based in Aruba, provided they are able to perform their tasks and responsibilities adequately at all times. In the case of a large institution, the MLCO function would be expected to be filled locally.

A service provider also must employ a person charged with overseeing the internal receipt and assessment of potential unusual transactions reports and the reporting of unusual transactions to the MOT (the MLRO). Regulated financial and trust service providers (service providers that fall within the scope of the AML/CFT Handbook) must appoint an MLRO based in Aruba. Obviously, other service providers also must make sure that the MLRO function is established in a way that ensures an adequate execution of its tasks and responsibilities.

Relevant information:
- *AML/CFT State Ordinance: article 47, paragraphs 1 and 2*
- *AML/CFT Handbook: Section 2.5*

39. Can the MLCO and MLRO functions be outsourced or must the persons fulfilling these functions be employed by the service provider?

The MLCO function can be outsourced, provided that the adequate execution of its tasks and responsibilities is ensured at all times (and in the case of regulated financial and trust service providers the outsourcing requirements of the AML/CFT Handbook are complied with). The MLRO must be a person employed by the service provider.

Relevant information:
- *AML/CFT State Ordinance: article 47, paragraphs 1 and 2*
- *AML/CFT Handbook: Sections 2.5 and 2.8*

40. When does the service provider have to inform the CBA and the MOT of the appointment of an MLCO and an MLRO?

A service provider must inform the CBA and the MOT within one month after the appointment of an MLCO and an MLRO.

Relevant information:
- *AML/CFT State Ordinance: article 47, paragraph 3*

41. Are there certain qualifications to be appointed as MLCO and MLRO?

The AML/CFT State Ordinance does not state required qualifications for an MLCO and an MLRO. However, the service provider must ensure that anyone appointed can adequately execute

the tasks and responsibilities of the MLCO and the MLRO at all times. This means that the MLCO and the MLRO must have sufficient knowledge, experience, skills, and resources, including sufficient time to perform their duties.

For regulated financial and trust service providers, the AML/CFT Handbook provides more detailed regulatory requirements regarding the MLCO and the MLRO.

Relevant information:
- *AML/CFT Handbook: Section 2.5*

42. May the MLCO and the MLRO be the same person?

The AML/CFT State Ordinance does not directly address this query. However, the service provider must assure that the tasks and responsibilities of the MLCO and the MLRO are executed adequately at all times. When considering whether it is appropriate to appoint the same person as MLCO and MLRO, a service provider must take into account:
- the respective demands of the two roles, including the size, nature, and risks of the business; and
- whether the individual will have sufficient time and resources to fulfill both functions.

Relevant information:
- *AML/CFT Handbook: Section 2.5*

43. What must I do if the position of MLCO or MLRO becomes vacant?

The service provider must ensure the adequate execution of the tasks and responsibilities of the MLCO and MLRO and the entrusting of the tasks and responsibilities of the MLCO and the MLRO to someone at all times. If the position of the MLCO or the MLRO is expected to fall vacant, the service provider must take immediate action to fill the vacancy. In the meantime, a member of the Management Board (or other appropriate member of senior management) could be appointed to the position for a very short period of time.

Relevant information:
- *AML/CFT Handbook: Section 2.5*

44. Can the MLCO and MLRO functions be fulfilled on a part-time basis?

The respective demands of the two functions will determine the answer to this question. The MLCO and the MLRO must have sufficient time and resources to adequately fulfill their respective functions and ensure the continuity of the reporting of unusual transactions at all times. What is sufficient in terms of time will depend on the size, nature, and risks of the business.

D. Reporting requirement

45. What are the criteria to determine whether a transaction is “unusual”?

The assessment of whether a transaction is considered an unusual transaction is based on the objective and subjective indicators issued by ministerial regulation.

Relevant information:
- *AML/CFT State Ordinance: article 25*
- *Interim regulation indicators unusual transactions AML/CFT State Ordinance (Interimregeling indicatoren ongebruikelijke transacties LWTF) (AB 2012 no. 23)*
- *AML/CFT Handbook: Sections 6.2 and 6.3*

46. A service provider must report an already carried out or intended unusual transaction to the MOT without delay. However, the definition of "customer" in article 1 of the AML/CFT State Ordinance refers to, among others, a person who causes a transaction to be carried out. No reference is made to an "intended transaction".

It is correct that no reference is made to an "intended transaction" in the definition of a customer. However, taking into account the wording of article 26, paragraph 1 of the AML/CFT State Ordinance, it is evident that a "transaction" as defined in article 1 of the AML/CFT State Ordinance also includes "intended transaction".

Relevant information:
- *AML/CFT State Ordinance: article 26*

47. A service provider must not only report a completed unusual transaction to the MOT, but also an intended unusual transaction. What is meant by an intended transaction?

An intended transaction is one that a client intended to conduct and took some form of action to do so. An intended transaction is different from a general request for information, such as an enquiry as to the applicable fee for a certain transaction. An intended transaction includes in any case entering into discussions or negotiations to conduct the transaction or takes concrete measures. It does not matter who ceases the completion of the transaction and what the reason is. The intended transaction is reportable on the same grounds as when it would have been completed.

The following are examples of intended transactions:

- A service provider refuses to accept a deposit because the customer refuses to provide requested identification information.
- A service provider refuses to process a transaction for which the customer insists on using cash because its business practice is not to accept cash.
- A customer of a real estate agent starts to make an offer and provides a large deposit on the purchase of a house, which is not finalized.
- An individual asks an accountant to facilitate a financial transaction involving large amounts of cash. The accountant declines to conduct the transaction.
- A money transfer company refuses to process a request to transfer a large amount of funds because the amount is above the allowed maximum.

Obviously, an intention to conduct a transaction does not necessarily mean the transaction is unusual. Only intended transactions that are considered unusual transactions, based on an objective or subjective indicator, must be reported to the MOT.

Relevant information:
- *AML/CFT State Ordinance: article 26*

48. What is the difference between objective and subjective indicators?

The indicators are subdivided into objective and subjective indicators. The objective indicators describe specific situations in which transactions must always be reported. The subjective indicators oblige 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. The service provider should consider whether a particular transaction needs to be reported because it may be linked to money laundering or terrorist financing.

With respect to indicators that are related to a specific threshold, the service provider also should assess whether there is a connection among transactions. This assessment can be done on the basis of the type of transaction and the amounts involved. If a connection is shown to exist, then these transactions could be reported under the subjective indicator.

49. Within what timeframe must a carried out unusual transaction or an intended unusual transaction be reported to the MOT?

The report of unusual transactions must be filed by the service provider immediately after the service provider becomes aware of the unusual nature of the transaction.. This provision takes into account a situation where a service provider establishes the unusual nature of a transaction only after some time. It is possible that following a client's second or third transaction, the service provider concludes that the client's conduct may be connected with money laundering or terrorist financing. In such case, the previously conducted transaction(s) might be seen in a different light, the consequence of which is that these past transactions must be reported to the MOT immediately. It must be emphasized that this does not apply to transactions that must be reported on the basis of an objective indicator. These transactions must be reported without any delay, which means within 5 working days.

The above explanation does not mean that the service provider can delay the process of assessing possible unusual transactions. If the unusual nature of the transaction is not evident right away and a further assessment is necessary, the service provider must conduct such assessment with the utmost urgency and complete it as soon as reasonably practical.

Relevant information:
- *AML/CFT State Ordinance: article 26*
- *AML/CFT Handbook: Section 6.3*

50. What information has to be submitted when reporting a carried out unusual transaction or an intended unusual transaction to the MOT?

The following information must be included in an unusual transaction report:
a. the identity of the client;
b. the nature and number of the identity document of the client;
c. the nature, time, and place of the transaction;

d. the amount and designated use and origin of the money, securities, precious metals, or other values involved in a transaction;
e. the circumstances based on which the transaction is considered unusual;
f. a description of the object in question for a transaction that involves a high value object,, and
g. the indicator or indicators pursuant to which the transaction has been designated as unusual.

The "designated use and origin of the money, securities, precious metals, or other values involved in a transaction" also means that detailed originator and beneficiary information must be included in the report.

Abovementioned information should be submitted in the reporting forms, as issued by the MOT.

Relevant information:
- *AML/CFT State Ordinance: article 26*

51. Can a service provider decide not to report an unusual transaction to the MOT assuming that the previous or next service provider in the chain has submitted or will report to the MOT?

Each service provider must comply with the reporting requirements for unusual transactions and, thus, must report all unusual transactions on the basis of objective or subjective indicators. All service providers in the same chain of the unusual transaction must report to the MOT.

Relevant information:
- *AML/CFT State Ordinance: article 26*

52. Can I inform a customer that I will make or have made an unusual transaction report to the MOT?

No. Disclosing any information to a customer regarding an unusual transaction report that will be made or has been made is prohibited.

Relevant information:
- *AML/CFT State Ordinance: article 31 (and the relevant explanatory notes to the AML/CFT State Ordinance)*
- *AML/CFT Handbook: Section 6.4*

E. Enforcement

53. What are the sanctions in case of violation of the provisions laid down in the AML/CFT State Ordinance?

In the case of non-compliance with the AML/CFT State Ordinance (including the regulatory requirements of the AML/CFT Handbook, which are directives issues pursuant to article 48, paragraph 1 of the AML/CFT State Ordinance), the CBA can:

(i) issue a direction (*aanwijzing*) to follow a certain line of conduct so that the service provider complies with the provisions of the AML/CFT State Ordinance within the timeframe determined by the CBA;
(ii) impose a penalty charge order (*last onder dwangsom*);
(iii) impose an administrative fine (*bestuurlijke boete*).

In addition, non-compliance also can be sanctioned by criminal prosecution. Therefore, the CBA can also report a case to the Public Prosecutor's Offic**e**, when there are grounds for doing so.

Relevant information:
- *AML/CFT State Ordinance: articles 48, paragraph 3, 37, paragraphs 1 and 2, 56*
- *AML/CFT Handbook: Section 1.3*
- *Enforcement policy supervision Centrale Bank of Aruba (Handhavingsbeleid toezicht Centrale Bank van Aruba) (this policy document is available on the website of the CBA).*

54. Can individual directors be subjected to sanctions or only the legal entity?

A direction (*aanwijzing*) can be issued to a service provider, being a legal entity or a natural person.

A penalty charge order (*last onder dwangsom*) or an administrative fine (*bestuurlijke boete*) can be imposed on the infringer. In most cases, the infringer will be the service provider itself (being a legal entity or a natural person) because most of the relevant provisions of the AML/CFT State Ordinance and the AML/CFT Handbook address service providers. However, 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 the violation occurred. In other words, the CBA has the possibility of imposing a penalty charge order or an administrative fine on individuals who can be held responsible for violating the AML/CFT law/regulations. A person will be considered an individual de facto in charge if, although so authorized and reasonably so required, he/she fails to take measures to prevent the prohibited conduct and consciously accepts the considerable risk that may arise from this conduct. The moment the individual de facto in charge becomes aware of the unlawful conduct is relevant. If he/she then fails to intervene, this person could be criminally liable. Depending on the circumstances of the case, such individuals include the service providers' management board members, supervisory board members, heads of department, and so forth.

Relevant information:
- *AML/CFT State Ordinance: article 37, paragraph 3*
- *Criminal Code: article 53, paragraphs 2 and 3*
- *AML/CFT Handbook: Section 1.3*
- *Enforcement policy supervision Centrale Bank of Aruba (Handhavingsbeleid toezicht Centrale Bank van Aruba) (this policy document is available on the website of the CBA).*