CENTRALE BANK VAN ARUBA

Circular of the Centrale Bank van Aruba to all money transfer companies

1. Introduction

This circular is intended for money transfer companies (MTCs). MTCs are regulated and supervised by the Centrale Bank van Aruba (CBA) pursuant to the State Ordinance on the Supervision of Money Transfer Companies (SOSMTC) and the State Ordinance on the prevention and combating of money laundering and terrorist financing (AML/CFT State Ordinance).[1]

2. Objective

The objective of this circular is to provide MTCs with practical guidance and tools on how to effectively conduct monitoring of customers and transactions and a basis from which MTCs can design, tailor and implement their own AML/CFT policies, procedures and measures. This circular presents ways of complying with the statutory requirements set out in the AML/CFT State Ordinance and the regulatory requirements of the 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) in the area of monitoring. This circular must always be read in conjunction with mentioned requirements.

The soundly reasoned implementation of the tools contained in this circular will provide a good indication that a MTC is in compliance with aforementioned statutory and regulatory requirements. A MTC may, however, adopt other appropriate measures to those set out in this circular, so long as it can demonstrate that such alternative measures also achieve compliance with the relevant statutory requirements of the AML/CFT State Ordinance and the regulatory requirements of the AML/CFT Handbook.

3. Importance of monitoring

MTC's provide an essential financial service. The risk entailed for a MTC is that it becomes inadvertently involved in money laundering (ML) and financing of terrorism (FT). In fact, the larger the number of transactions and the higher the number of different payors and beneficiaries, the higher the risk becomes.

Conducting on-going monitoring of transactions is a key factor in the process of detecting unusual or suspicious activity and reporting unusual transactions to the Reporting Center Unusual Transactions (*Meldpunt Ongebruikelijke Transacties (MOT)).* Not having implemented monitoring procedures could also result in a MTC being held liable under the Criminal Code of Aruba for negligent money laundering (*schuldwitwassen*)[2]. Moreover, as part of sound and controlled business operations, a MTC must, among others, have policies, procedures and measures to prevent any direct or indirect involvement in criminal

[1] Article 1 of the AML/CFT State Ordinance defines a financial service provider, among others, as anyone who on a commercial basis transfers or causes the transfer of monies or values.

[2] Article 430d of the Criminal Code of Aruba. In this context a MTC can be held liable for negligent money laundering where he should reasonably suspect that the money – indirectly or directly – is the proceed of crime, but nonetheless carries out the transaction for the customer.

offences or other violations of the law. Reference is made to article 6 of the SOSMTC and to the Guidelines on the conduct of business by and the administrative organization of MTC's.

4. Tools for effective monitoring

This circular brings the following three tools to your attention that are essential to ensure adequate monitoring of customers and transactions:

- Transaction analyses
- Enhanced data quality
- Adequate staff training

These tools will be further discussed below.

5. Transaction analyses

One of the basic pillars of a strong AML/CFT program is a strong, well-designed and effective transaction monitoring program. Its basic purpose is to identify and protect a MTC from conducting transactions that may facilitate ML/TF. In other words, it helps prevent that a MTC is misused for ML/TF purposes. Transaction monitoring also assists MTCs in cooperating and assisting law enforcement in its efforts to combat ML/TF.

Money launderers and terrorism financers will take all available actions to attempt to disguise their transactions by making them seem legitimate. This makes it more difficult for MTCs to be able to distinguish between good and bad clients and between acceptable and potentially illicit transactions.

Legal basis

An MTC must establish adequate transaction monitoring procedures and analyze the activity and transactions of its customers (i) to ensure that these transactions are consistent with the customer's risk profile and (ii) to allow for the identification of unusual (patterns of) activity or transactions and the reporting of unusual transactions to the MOT. Monitoring procedures must require more intensive scrutiny for higher risk customers.

Reference is made to article 3, paragraph 1, subsection d, article 6, paragraph 3, and articles 11 and 12 of the AML/CFT State Ordinance, as well as chapter 5 of the AML/CFT Handbook.

Guidance

The following two methods are essential for the performance of appropriate and effective transaction monitoring and analyses.

<u>Standard Analysis</u>

- Top lists:
  - Look for persons originating/receiving largest accumulated value of transaction.
  - Look for persons originating/receiving highest number of transactions.

  Note: Depending on the size and risk profile of your MTC, you must choose the frequency (e.g., on a weekly, monthly, quarterly and/or yearly basis) and the size of the top lists (e.g., for small institutions a top 10 usually suffices, for large institutions a top 20 or 25 may be more appropriate).

- Aggregate amounts:
  - Look for originators/beneficiaries who try to avoid the Afl. 2,500 threshold that requires a source of funds to be filled out or whose transactions exceed the daily maximum of Afl. 5,000 per individual transaction[3], by e.g sending amounts just below the threshold(s) at different branches and/or on consecutive days or days that closely follow each other.
    - Sort by originator and date.
    - Sort by beneficiary and date.

  Note: When performing this analysis, make sure to include transactions to/from all branches.

- High risk countries and persons:
  - Look for transactions to/from countries that appear on the FATF lists[4].
  - Look for transactions to/from PEPs.
  - Look for transactions by persons who are listed on external/internal monitoring lists[5] (e.g., UN so-called freezing lists, internal list of authority requests, internal list of persons previously reported to the MOT).

- Unusual transactions:
  When conducting the different analyses listed above also pay attention to the following:
  - Purpose of transaction (is the nature of the transaction consistent with the customer's profile?).
  - Unusual (high) amount in a certain period (which has no apparent economic or visible lawful purpose).
  - Unusual destination (having no apparent economic or visible lawful purpose).
  - Variations in the name of the originator/beneficiary (number of first names and last names can differ per identification document. Therefore, the input in the system must be correct and consistent for effective transaction analyses).

<u>Network Analysis</u>

This type of analysis is to identify individuals who are possibly working together to avoid that the origin and destination of funds are traceable.

- Look for commonalities:
  - Originators/ beneficiaries with same last name/ address/ telephone number.
  - Different originators/ beneficiaries with same particular purpose of transaction (e.g., car parts, repayment of loan, etc., which can trigger further research into groupstructure – see next bullet).
  - Same group of persons originating/receiving transactions from different group(s) of persons. These transactions can be originated from/received in different countries.

The CBA requires that a MTC records its transaction analyses and is able to supply this documentation to the CBA if requested to do so.

---

[3] Reference is made to the CBA's Operational and Sector Specific Guidelines for MTCs, point 8, and the Guidelines on the Conduct of Business by and the Administrative Organization of MTCs, article 9, par. 1, sub a.

[4] Reference is made to the FATF statements circulated by the CBA (www.cbaruba.org). The updated FATF list also can be found on the website of the FATF (www.fatf-gafi.org).

[5] Reference is also made to the Sanction State Decree to Combat Terrorism and Terrorism Financing (AB 2010 no. 27).

6. Data adequacy

Deficiencies or inconsistencies in customer identification information can have large impacts on the effectiveness and reliability of the information gathered during transaction analyses. To be able to analyze transactions effectively, a MTC must ensure that customer identification information that is entered in its system(s) is accurate, complete and consistent. Furthermore, a MTC must ensure that it collects sufficient information about the origin and destination of the money. A tool in this case is the Source of Funds Declaration form which is required to be filled out by the customer for transactions exceeding Afl. 2,500 or its equivalent in foreign currency.[6] If a MTC has doubts about the reliability of the information, it must take suitable measures. For example, instructing cashiers to inquire about the origin and destination of the money the next time the customer visits the MTC.

MTCs must ensure that the data collected pursuant to the customer due diligence (CDD) process are kept relevant and up-to-date. MTCs must also record and retain all CDD information in an accessible way for a period of at least ten years after carrying out the transaction in question. The keeping of records must take place in such a manner that separate transactions can be reconstructed at all times and be submitted to the competent authorities on first demand.

Reference is made to articles 7 and 33 of the AML/CFT State Ordinance and chapter 8 of the AML/CFT Handbook.

7. Adequate staff training

One of the most important controls for the prevention and detection of ML/TF is to have employees who are able to identify unusual activity, which may involve ML/TF. It is, therefore, essential that a MTC has clear and well-articulated policies, procedures and measures for ensuring that its employees are adequately trained, at appropriate frequencies, in applying CDD, and the identification and reporting of unusual transactions and record keeping. This is essential to ensure that employees have and maintain a high level of awareness of the new developments and risks connected with ML/TF. To this end, a MTC must also establish and maintain procedures that monitor and test the effectiveness of the employees' awareness of AML/CFT issues and the training provided to employees.

Reference is made to article 46 of the AML/CFT State Ordinance and chapter 7 of the AML/CFT Handbook.

8. Conclusion

Effective monitoring is key in preventing a MTC from becoming inadvertently involved in ML or TF. By deploying the aforementioned tools, a MTC can mitigate the risks of being misused by criminals for ML/TF purposes.

[6] Refer to point 8 of the CBA's Operational and Sector Specific Guidelines for MTCs and appendix 3 of the AML/CFT Handbook.