CENTRALE BANK VAN ARUBA

Circular transaction monitoring for all trust service providers

1. Introduction

This circular is intended for trust service providers (TSPs). TSPs are regulated and supervised by the Centrale Bank van Aruba (CBA) pursuant to the State Ordinance on the Supervision of Trust Service Providers (SOSTSP) 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 TSPs with practical guidance and tools on how to effectively conduct transaction monitoring and a basis from which TSPs 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 TSP is in compliance with aforementioned statutory and regulatory requirements. A TSP 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

The risk entailed for a TSP is that it becomes inadvertently involved in money laundering (ML) and financing of terrorism (FT). If the TSP has no authorization to co-sign and approve transactions, the higher the risk becomes, considering that monitoring will only take place post event.

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 TSP 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 TSP must, among

[1] Article 1 of the AML/CFT State Ordinance defines a designated non-financial service provider, among others, as a trust service provider as meant in article 1 of the SOSTSP.

[2] Article 430d of the Criminal Code of Aruba. In this context a TSP 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.

others, have policies, procedures and measures to prevent any direct or indirect involvement in criminal offences or other violations of the law. Reference is made to article 6 of the SOSTSP.

4. Tools for effective monitoring

This circular brings the following tools to your attention that are essential to ensure adequate transaction monitoring:

- Transaction monitoring
- Adequate staff training

These tools will be further discussed below.

5. Transaction monitoring

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 enable the TSP to timely identify unusual transactions and protect a TSP from conducting transactions that may facilitate ML/TF. In other words, it helps prevent that a TSP is misused for ML/TF purposes. Transaction monitoring also assists TSPs 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 TSPs to be able to distinguish between good and bad clients and between acceptable and potentially illicit transactions.

Legal basis

The fundamental part of proper monitoring are adequate client acceptance and customer due diligence procedures and measures. It is crucial for TSPs to have a risk profile established for its clients.

A TSP must establish adequate transaction monitoring procedures and scrutinize the activity and transactions of its customers (i) to ensure that these transactions are consistent with the customer's risk profile and (ii) to identify unusual (patterns of) activity or transactions and, subsequently, report unusual transactions to the MOT. Monitoring procedures must require more intensive scrutiny for higher risk customers.

Reference is particularly 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 paragraph 3.2 and chapter 5 of the AML/CFT Handbook.

Guidance

It is essential that TSPs have accurate information on all bank accounts of their customers at all times, whether the TSP has signatory authorization on the bank account or not. In order to assess completeness and accuracy of bank account information of the customers it is crucial that TSPs obtain the financial statements and annual reports of each customer on a periodic basis (e.g. yearly). TSPs can arrange to periodically have contact with its customers, based on their risk profile, through meetings or teleconference in order to stay up-to-date with recent developments in the operations of said customers, their risk profile, and to stay abreast of any changes that may occur. In this regard, TSPs should have

procedures in place to ensure that all changes with regard to the customers bank accounts are timely communicated to the TSP.

A TSP should have procedures and measures in place to:

- establish whether or not a customer has a bank account; and
- ensure that it timely receives complete and accurate bank account information.

If a customer claims that it does not have a bank account, the TSP should assess whether this makes economic sense, or fits the business operation of the customer.

There are two scenarios possible with regard to transaction monitoring at TSPs:

- Real time monitoring (when facilitating a transaction).
- Post-event monitoring .

Real time monitoring

Considering the diverse businesses that customers are active in, a TSP's personnel should be very diligent in reviewing and authorizing transactions for each customer. The TSP should be able to:

- Determine whether the transaction fits the business activities of the customer. The goods and/or services related to the transaction as well as the counter party involved in the transaction should be looked into.
- Determine whether the counter party of a transaction is a person who is listed on an external/ internal monitoring list[3].
- Determine whether the amounts involved fits the transaction profile of the customer.
- Determine whether the frequency of the requests for facilitating transactions agrees with the business operations of the customer.
- Ensure it receives supporting documents for the transaction to be facilitated, such as payment invoices, purchase agreements, investment statements, bills of lading, et cetera. These documents must be relevant to the transaction and must be understandable (in a language that both the TSP as the supervisory authority can understand).

Post-event monitoring

Post-event monitoring may involve end of day, weekly or monthly reviews of bank statements received by the TSPs from their customers. This type of monitoring is of particular importance in the cases where a customer conducts its transactions without the involvement of the TSP.

For the review of the bank statements the TSP should be able to:

- Conduct a periodic check that all bank statements of each customer are received timely.
- Perform a detailed assessment of all transactions recorded on the bank statements, which may include:
  - requesting the customer to submit supporting documents for the transactions recorded on the bank statements, such as payment invoices, purchase agreements, investment statements, bills of lading, et cetera;

[3] Reference is also made to Sanction State Decree to Combat Terrorism and Terrorism Financing (AB 2010 no. 27) with regard to the external lists. A TSP may also have internal list of persons with whom it may not want to do business, based on information obtained from public sources, previous business experience or other information available.

- determine whether the transactions fit the business activities of the customer. The goods and/or services related to the transaction as well as the counter party involved in the transaction should be looked into;
- determining whether the counter party of a transaction is a person who is listed on an external/ internal monitoring list[4];
- determining whether the transaction amounts fit the profile of the customer;
- determining whether the frequency of the transactions agrees with the business operations of the customer.

Note 1: where real-time monitoring is possible, this should be performed as it can prevent an unlawful transaction from being conducted.
Note 2: supporting documents or other information received should be understandable (i.e. in a language understood by the TSP's personnel)

6. 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 TSP 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 TSP 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.

7. Conclusion

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

Note that the tools mentioned in this circular only apply to monitor money flow transactions. The TSP should however ensure that all types of transactions, e.g. also paper transactions such as loan agreements, are dully monitored.

[4] Reference is also made to Sanction State Decree to Combat Terrorism and Terrorism Financing (AB 2010 no. 27) with regard to the external lists. A TSP may also have internal list of persons with whom it may not want to do business, based on information obtained from public sources, previous business experience or other information available.