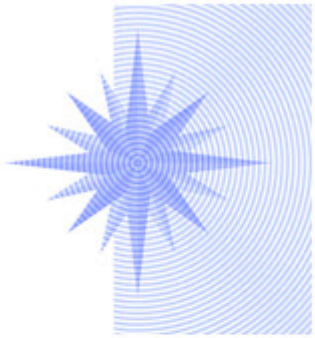
the Wolfsberg Group



Banco Santander
Bank of Tokyo Mitsubishi-UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
JP Morgan Chase
Societe Generale
UBS

Wolfsberg Statement on AML Screening, Monitoring and Searching (2009)

1. Introduction

The Wolfsberg Group[1] issued its initial paper examining how financial institutions could develop suitable screening, monitoring and searching processes and procedures in September 2003. Developments and operational experience, for example in the use and relative effectiveness of dedicated, automated transaction monitoring systems, together with the introduction of the Risk Based Approach (RBA) means that it is now appropriate to revise the statements made within that document. This paper therefore supersedes the 2003 paper providing more guidance on the design, implementation and on-going maintenance of transaction monitoring frameworks for real-time screening, transaction monitoring and retroactive searches. The Wolfsberg Group is committed to the development of appropriate standards and benchmarking for effective risk-based screening, monitoring and searching models.

2. Definitions

For the purpose of this document, the following definitions are applicable

- Real-time Payment Screening (Screening): The screening or filtering of relevant payments instructions prior to their execution in order to prevent making funds available in breach of sanctions, embargoes or other measures
- Transaction Monitoring (Monitoring): The automated or manual process of monitoring transactions after their execution in order to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, reporting to the authorities

[1] The Wolfsberg Group consists of the following leading international financial institutions: Banco Santander, Bank of Tokyo-Mitsubishi-UFJ Ltd, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale and UBS.

In addition, the following institutions also participated in the preparation of this paper: ABN Amro, American Express and Bank of Ireland.

- Client Screening: The screening of client names and associated details against lists provided by relevant competent authorities both at initial on-boarding and at other points during the client relationship
- Retroactive Searches (Searches): The identification of specific past transactions, as well as existing and closed accounts/relationships, in order to undertake due diligence and respond to external (*e.g*., regulatory) enquires

3. Role of Financial Institutions

Financial institutions should have appropriate processes in place that allow for the identification of unusual transactions, patterns and activity. Since these will not be suspicious in all cases, financial institutions should have the ability to analyze transactions, patterns and activity to determine if they are suspicious in nature (*e.g.,* indicative of potential money laundering.). This document does not consider how such unusual and potentially suspicious activity should be reviewed and investigated.

Suspicious transactions, patterns and activity must be reported to competent authorities in accordance with local laws, regulations or rules. Monitoring of account activity and transactions flowing through a financial institution is one means of ensuring this role is fulfilled.

Financial institutions should also have processes in place to screen payment instructions and client details against lists provided by relevant competent authorities. Financial institutions should also be able to respond expeditiously to any other ad-hoc search requests from such authorities.

4. Screening

Real-time payment screening is the screening or filtering of relevant payment instructions prior to execution. This activity, together with the screening of client details both at on-boarding and at other points during the client relationship, is typically used for complying with embargoes and sanctions and can be most effectively used for the identification of payments to or from persons or entities for which relevant competent authorities have provided notice to financial institutions.
While it is critical that screening is undertaken on a real-time basis in order to block affected payments before completion, it can adversely affect Straight Through Processing (STP) and therefore requires timely responses by relevant competent authorities to financial institution requests for clarification in order for payments to be completed within the time periods specified by the clearing and settlement systems.

In order to enhance the quality of real-time and other screening activity, the Wolfsberg Group believes that the following points are of the utmost importance:

- Real-time screening should only be required for screening and filtering related to embargoes or sanctions, and financial institutions should not be required to engage in real-time screening for names other than those specified by relevant competent authorities

- Institutions should screen during on-boarding and at appropriate points during the subsequent relationship (*e.g.,* upon receipt of a revised list provided by a relevant competent authority)
- Financial institutions should be able to rely on the quality and completeness of information provided by relevant competent authorities and other relevant parties such as data providers
- Intermediary banks can only screen information input by the originator of a payment or other instruction
- In order to minimize the production of a significant number of "false positives" (*i.e*., apparent matches that prove to have been incorrect on substantive review) and thereby to maximize operational effectiveness and efficiency, it is essential that lists provided by relevant competent authorities to financial institutions conducting real-time screening contain acceptable amounts and types of information (including, where available, full name, date of birth and other relevant unique identifiers); and
- Financial institutions acting in an intermediary capacity with respect to a payment or other transaction rely, to the extent permissible by law, on the active cooperation and efficiency of their counterparties to avoid delays in completing the transaction by resolving potential issues related to sanctions, embargoes or potential money laundering in a timely manner

5. Transaction Monitoring Frameworks

Transaction monitoring should be embedded in an institution's integrated anti-money laundering program and the appropriateness of an institutions transaction monitoring framework should be assessed using the principle that the framework should be aligned to, and focused on, the perceived risk relating to an institutions business model, the products and services it offers and the nature of its customer base.

Experience has shown that non risk-based regulatory standards for suspicious activity monitoring are not as effective in identifying potential money laundering and activity associated with potential terrorist financing.

The Wolfsberg Group believes that a risk-based approach enhances the effectiveness of monitoring for unusual and potentially suspicious activity, to the extent that such activity is distinguishable from legitimate activity. It is for this reason that the Wolfsberg Group supports the introduction of risk-based monitoring models and frameworks that are sufficiently flexible to meet the needs and nature of individual financial institutions.

- <u>Institutions Assessment of Risk</u>

The type of monitoring framework implemented will depend on a financial institution's risk assessment and so will vary between institutions and even between business units within a financial services group. Based on this risk assessment, the development of an appropriate monitoring framework will depend both on the products and services being supported, the size and nature of the institutions operations and, where appropriate, the adoption of a risk-based approach. The results of this assessment will determine whether an institution opts for a single approach to monitoring or deploys a combination of monitoring activities.

- A risk-based approach

Risk profiles will vary between financial institutions and also between business units within an institution depending on the products and service offered by each (*e.g.*, retail, private banking, correspondent banking, broker-dealer etc.). The framework used to monitor transactions should reflect this risk assessment with greater attention focused on those business areas and types of activity considered to represent the highest risk.

- Framework Components

The most appropriate and effective overall monitoring framework may contain one or more of the following elements

- A dedicated automated transaction monitoring system
- System-generated exception reports
- Manual "line of business" incident reports
- Scheduled periodic reviews/sampling
- Event-driven reviews (e.g., following issuance of new typologies)

In all cases the objective is to try and focus monitoring resource on the most unusual and potentially suspicious transactions and patterns of activity whilst reducing, as far as possible, the "false/positive" rate.

Financial institutions should ensure that the existence of a transaction monitoring framework does not result in a reduction of staff vigilance. Experience and analysis has shown that suspicious activity is frequently identified in circumstances that either do not lend themselves to automated surveillance or cannot be replicated within transaction monitoring frameworks. This means that a continuing emphasis on staff training and awareness is required, particularly focused on customer facing staff.

5.1 Dedicated Automated Transaction Monitoring Systems

If the risk analysis indicates that the use of a dedicated automated system is likely to be effective as part of an institutions risk-based transaction monitoring framework, some or all of the following functional capabilities may be determined to be appropriate including the ability to:

- Compare a clients or accounts transaction activity during the reporting period against relevant transaction history over a time period that the institution considers to be reasonable and appropriate;
- Compare customer or transaction-specific data against risk scoring models;
- Issue alerts if unusual and potentially suspicious transactions are identified;
- Track those alerts in order to ensure that they are appropriately managed within the financial institution and that suspicious activity is reported to the authorities as required;
- Maintain an audit trail for inspection by the institution's audit function and by bank supervisors

- Provide appropriate aggregated information and statistics

Operational experience with automated transaction monitoring systems has demonstrated that their effectiveness is significantly affected by the availability of intelligence and typology information that can be used to devise and calibrate the rule set.

5.2 Other Transaction Monitoring Frameworks

The size of a financial institution or the nature of the products and services it offers may make it inappropriate to implement a dedicated automated transaction monitoring system either across the entire operation or within particular business units. It is therefore reasonable that there will be situations where a financial institutions risk assessment will indicate that the most appropriate, effective and efficient framework may consist of a set of system-generated exception reports or other approaches (*i.e*., sampling).

Where exception reports and periodic sampling are considered to be the most appropriate option for an institution, it may choose to adapt or enhance controls or reports already in place for other purposes or may introduce new ones. In business situations with highly structured products (*e.g.,* structured finance, corporate finance loans), a combination of spreadsheet reporting and analysis supported by sample-based reviews may be determined to be the optimum solution.

These monitoring controls and their associated exception thresholds should be subjected to regular review and the underlying assessment and assumptions documented.

5.3 Maintaining & Reviewing the Monitoring Framework

As with all risk-based processes, a financial institution may wish to consider undertaking periodic reviews to ensure that both the thresholds being used to calibrate rules and alerts, as well as the nature of the overall framework, remain appropriate given the risk environment.

A financial institution may decide that a formal review process at regular intervals is required or may use trigger events (*e.g*., the issuance of a report on new money laundering typologies) to prompt a review and re-assessment in addition or as an alternative to a formal review program.

When considering whether or not the risk environment has changed, financial institutions may wish to consider some or all of the following sources of information

- Findings published by the FATF and other competent authorities;
- Law enforcement guidance and publications;
- Information from regulators and government Financial Intelligence Units (FIU's);
- Media monitoring;
- Operational experience of the financial institution's own monitoring activity.

In all cases such reviews should be documented and details of changes to rule/alert thresholds retained. Such reviews and adjustments are essential to focus resources toward those transactions and patterns of activity that are considered by the financial institution to represent

the greatest risk, as well as ensuring that the level of resource required to support such activity remains appropriate and proportionate.

As in all aspects of the management of money laundering risks, there is a continued need for private and public sector organizations to work in partnership to ensure that relevant information is made available as quickly as possible to the appropriate authorities and that feedback is provided by them as soon as possible.

6. Searching

Financial institutions may perform retroactive searches during ongoing risk-based due diligence, or as an element of enhanced due diligence pursuant to its policies and procedures. Retroactive searches may also be the result of requests by governmental authorities or the issuance of judicial processes (*e.g*., subpoenas or search warrants), that require financial institutions to search for specific data. To ensure consistent results, and where possible and appropriate, a financial institution should apply uniform processes and procedures for entering search criteria.

When a financial institution engages in retroactive searches as a result of its own policies and procedures, care should be taken to ensure that such searches are risk-based and that they are performed against those data sources that will allow for the most effective and efficient identification of relevant data based on the risks associated with the customer or transactions.