# Monitoring Screening and Searching

# Wolfsberg Statement

## 1 Preamble

The Wolfsberg Group of financial institutions (the "Wolfsberg Group")[1] has previously produced: Global Anti-Money Laundering Guidelines for Private Banking; The Wolfsberg Statement on The Suppression of the Financing of Terrorism; and The Wolfsberg Anti-Money Laundering Principles for Correspondent Banking. All of these have stated the need for appropriate monitoring of transactions and customers to identify potentially unusual or suspicious activity and transactions, and for reporting such to competent authorities. The Guidelines, Statement and Principles, however, have not addressed issues related to the development of risk-based processes for monitoring, screening and searching of transactions and customers. Therefore, the Wolfsberg Group is making this statement to identify issues that should be addressed in order that financial institutions are able to develop suitable monitoring, screening and searching processes.

The Wolfsberg Group acknowledges that the risk profile may be different for a financial institution as a whole and for its individual units depending on the business conducted in a particular unit (e.g. Retail, Private Banking, Correspondent Banking, Broker Dealer). It must be recognised, however, that any process for monitoring, screening or searching is limited to detecting those clients and transactions that have identifiable characteristics that are distinguishable from apparently legitimate behaviour. Because money launderers and terrorists will take all available actions to attempt to disguise their transactions and accounts by providing them with an air of legitimacy, it becomes difficult, if not sometimes impossible, to make any distinctions between good and bad clients and acceptable and potentially illicit transactions. We are, however, committed to implementing processes and methods and making use of information technology systems where appropriate, so that we, to the best of our ability, have in place efficient and effective processes and systems to identify potential suspicious activity.

## 2 Definitions

- **Real-time Screening (Screening):** Defined as the screening or filtering of payment instructions (i.e. wire or funds transfers) prior to their execution in order to prevent making funds available in breach of sanctions, embargoes and other measures.
- **Retroactive Searches (Searches):** Defined as the identification of specific past transactions, as well as existing and closed accounts.

[1] The Wolfsberg Group consists of the following leading international financial institutions: ABN AMRO Bank N.V., Banco Santander Central Hispano S.A., Bank of Tokyo-Mitsubishi Ltd., Barclays Bank, Citigroup, Credit Suisse Group, Deutsche Bank AG, Goldman Sachs, HSBC, J. P. Morgan Chase, Société Générale, UBS AG.

- **Transaction Monitoring (Monitoring)**: Defined as the process of monitoring transactions after their execution in order to identify unusual transactions, including monitoring single transactions, as well as transaction flows.

# 3 Role of Financial Institutions

Financial institutions must have appropriate processes in place that allow for the identification of unusual activity and unusual patterns of activity or transactions. Since unusual transactions, patterns or activity need not be suspicious in all cases, financial institutions must have the ability to analyse and determine if the activity, patterns or transactions are suspicious in nature with regard to, among other things, potential money laundering. Suspicious activity, patterns and transactions 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 that this role is fulfilled. Financial institutions should have processes in place to screen payment instructions against the lists provided by competent governmental authorities to identify amongst others, potential terrorists or terrorist financing. Financial institutions should respond expeditiously to search requests from competent governmental authorities.

# 4 Risk-Based Approach

Traditionally, laws, regulations and rules with regard to monitoring, screening and searching issued by some governmental authorities have not embraced a risk-based approach. Instead governmental directives have focused on collecting data from financial institutions by establishing thresholds, such as large cash transaction reports, or by providing specific information on which financial institutions must react, such as embargoes or sanctions. Implicit in these collection and reporting obligations is that activity or transactions that are being reported may be suspicious or illegal. However, because, for example, not all large transactions are suspicious, monitoring should not be limited to focusing on thresholds, but rather should be aimed at recognising unusual activity in comparison to known and expected activities.

Similar to the risk-based approach for conducting due diligence at account opening, monitoring, and some screening and searching processes should also be risk-based. A risk-based approach for monitoring and relevant screening and searching should be closely linked to the risk-based approach used at account opening and such an approach should consider both elements that increase as well as reduce risk. Where financial institutions know their clients better, including understanding their intended activity at the institution, the greater is the ability to identify gaps between current activity and past and expected activities, which in turn provides financial institutions with critical information to assist in determining whether unusual or suspicious activity exists.

Financial institutions should consider the use of information technology systems in the context of the risk associated with the business units, e.g. size, nature of business conducted and overall monitoring process.

Therefore, a risk-based approach may require a differentiated level of implementation of real-time screening, retroactive searches and transaction monitoring systems.

## 4.1 Real-time Screening

Real-time transaction screening is the screening or filtering of payment instructions (i.e. wire or funds transfers) prior to their execution. Real-time screening is typically used for enforcing embargoes and sanctions. Real-time screening can be most effectively used for the identification of payments to or from persons or entities for which governmental authorities have provided notice to financial institutions. While it is crucial that screening is undertaken on a real-time basis in order to block affected payments before completion, it can adversely affect Straight Through Processing and, therefore, requires timely action on the part of governmental authorities in order to allow appropriate payments to be completed within the time periods specified by the clearing and settlement systems.

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

- real-time screening should only be required to be used for screening or 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 governmental authorities;
- real-time screening technology should be driven by responses that only require a true or false answer to matches with the applicable lists provided by governmental authorities;
- financial institutions should be able to rely on the quality and completeness of the names provided by governmental authorities; and
- criteria should be established as to acceptable amounts and types of information that must be provided to financial institutions to conduct real-time screening to include such things as, full name, date of birth and other relevant unique identifiers which should mitigate the significant number of "false positives" (i.e. apparent matches that prove incorrect on substantive review).

## 4.2 Retroactive Searches

Retroactive searches may be the result of ongoing risk-based due diligence or enhanced due diligence pursuant to policies and procedures implemented by financial institutions. Retroactive searches may also be the result of requests by governmental authorities or the issuance of judicial processes, such as subpoenas or search warrants, that require financial institutions to search for specific data.

The Wolfsberg Group believes that retroactive searches provide a valuable tool for locating and identifying transactions and accounts of interest. However, there is not uniformity among financial institutions and governmental authorities as to how retroactive searches should be conducted and what records at an

institution should be the subject of such searches. The lack of uniformity and clarity can (and often does) lead to time consuming manual searches.

When financial institutions engage in retroactive searches as the result of their own processes, care should be taken to ensure that such searches are risk-based. Financial institutions should identify those data sources that will allow for the most effective and efficient searches to identify the appropriate data based on the risks associated with the customer or transactions.

As a means of developing uniformity that will provide necessary assistance to financial institutions and ultimately produce retroactive searches of significant utility to law enforcement activities, the Wolfsberg Group recommends that governmental authorities, in consultation with financial institutions, identify specific types of data that it would be of value to maintain electronically (e.g. client identifying information, beneficial owner information, transaction information) and financial institutions should seek to create such information in an electronic format that would then support effective and efficient retroactive searches.

## 4.3 Transaction Monitoring

The majority of ongoing monitoring for unusual and potentially suspicious activity is accomplished by transaction monitoring. Risk-based transaction monitoring for potential money laundering requires the development of risk models that identify the potential risks to money laundering and provide a means of ranking the risks in order to compare the risks to completed transactions. An appropriate transaction monitoring process will compare the transaction information against the identified risks, such as geographic location of transaction, the type of products and services being offered and the type of client engaging in the transaction with the different typologies for money laundering and other ilicit activites to determine if a transaction is unusual or suspicious.

This approach requires that a model exist that supports the identification of transactions that deviate from a standard model or benchmark and allows a risk-based review and analysis. Transaction monitoring based on such a concept provides financial institutions with the necessary coverage for review of transactions that are not subject to real-time screening or retroactive searches. The Wolfsberg Group intends to continue to develop guidance for

- a process that permits reasonable reviewing of transactions;
    - identifying reasonable, risk-based scores / alerts;
    - ensuring comparability between financial institutions as to the robustness of the model;
    - establishing industry standards for understanding levels or degrees of "unusualness" or suspicion; and
    - ability to replace or enhance current process of monitoring solely for transactions exceeding specific thresholds.

# 5 Standards for Risk-Based Transaction Monitoring

An effective risk-based transaction monitoring process should:

- compare the client's account/transaction history to the client's specific profile information and a relevant peer group and/or compare the clients account/transaction history against established money laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies
- establish a process to compare customer or transaction specific data against risk scoring models;
- be capable of recognizing patterns and of "learning" which transactions are normal for a client rather than designating certain transactions as unusual (for example, not all large transaction are unusual and may easily be explained);
- issue alerts if unusual transactions are identified;
- track those alerts in order to ensure that they are appropriately managed within the 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; and
- provide appropriate aggregated information and statistics.

# 6 Conclusion

Risk-based transaction monitoring, real-time screening and retroactive searches must be embedded in an integrated anti-money laundering program. Past experience indicates that those current governmental standards for monitoring for suspicious activity, which have tended not to be risk-based, are not effective enough for identifying potential money laundering activity. The Wolfsberg Group believes that a risk-based approach will enhance the effectiveness of monitoring unusual or potentially suspicious activity, to the extent such activity is distinguishable from legitimate activity. It is for this reason that the Wolfsberg Group supports the introduction of risk-based monitoring models that set forth uniform standards or baselines while being sufficiently flexible to meet the needs of individual financial institutions. The Wolfsberg Group is committed to the development of appropriate standards and benchmarks towards establishing effective risk-based monitoring, screening and searching models.