Wolfsberg Frequently Asked Questions ("FAQs") on Correspondent Banking

Preamble

The Wolfsberg Group[1] published its Anti-Money Laundering ("AML") Principles for Correspondent Banking in 2002 ("the Principles"[2]). The Principles constitute global guidance on the establishment and maintenance of Correspondent Banking relationships which if poorly controlled, can permit institutions with inadequate AML systems and controls direct access to international banking systems. The Wolfsberg Group believes that adherence to the Principles promotes effective risk management and enables institutions to exercise sound business judgement with respect to their Correspondent Banking Customers[3] (referred to in these FAQs as "the Correspondent"), and furthers the goal of Wolfsberg Group members to endeavour to prevent the use of their institutions for criminal purposes.

In the Principles, the Wolfsberg Group encouraged the development of an international registry for financial institutions. Upon registering, financial institutions would submit information useful for conducting due diligence as outlined in the Principles and financial institutions could use this information in support of their actions under the Principles. Such a registry has been developed by Bankers Almanac and is endorsed by the Wolfsberg Group. Further information on the international registry is contained in these FAQs.

To provide continuing guidance on money laundering controls in relation to correspondent banking, the Wolfsberg Group has prepared these FAQs, based on the Wolfsberg Group's views on current best practices and, in some aspects, on how we believe those practices should develop over time.

1. What is the nature and purpose of Correspondent Banking?

In dealing with Correspondents, a Bank (referred to in these FAQs as the "Institution") is effectively acting as its Correspondent's agent or conduit, executing and/or processing payments or other transactions for the Correspondent's customers. These customers may be individuals, legal entities or even other financial institutions. The beneficiaries of the transactions may be customers of the Institution or customers of other financial institutions. The Institution may have no direct relationship with the underlying parties to any transaction routed through it and, in such cases, may not be in a position to verify identity or to understand fully the nature of the specific transaction, particularly when processing electronic payments (wire transfers) or clearing cheques.

---

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

[2] See the Wolfsberg AML Principles for Correspondent Banking www.wolfsberg-principles.com/standards

[3] Correspondent Banking Customer is a Customer of an institution that is a financial services firm that uses the institution's Correspondent Banking services accounts to clear transactions for its own Customer base. The term includes (but is not limited to) Banks, Broker-Dealers, Mutual Funds, Unit Trusts, Investment Services Firms, Hedge Funds, Introducing Brokers, Money Services Businesses, Pension Funds, Credit Card Providers, Commercial Credit Companies, Household Finance Companies, Mortgage Banks, Building Societies, and Leasing Companies (see section 2 of the Principles).

The inter-relationships built up over decades between Institutions within Correspondent Banking networks have produced a highly efficient mechanism which is of fundamental importance to the global economy. This mechanism facilitates the movement of money from one person or entity to another, and from one country to another as well as currency conversion. In order for this international payment infrastructure to continue to function efficiently, whilst also effectively countering money laundering, each Correspondent must be responsible for performing due diligence on its own customers and monitoring its customers' transactions in accordance with applicable law and regulations and where appropriate, take into account all relevant international standards. Institutions should perform due diligence on their Correspondents (for details see the Principles). Institutions should take a risk based approach to due diligence, carrying out enhanced due diligence for Correspondents considered as higher risk (for details on enhanced due diligence see the answer to Question 6 below).

Customers of the Correspondent do not become customers of the Institution simply by virtue of a correspondent banking relationship. Rather, Correspondents, having the direct relationship with customers should perform such due diligence, because they are in the best position to know their customers, and should operate a proper internal control environment designed to mitigate potential money laundering risks.

In certain cases, including, for example, in the cases referred to in the answers to Questions 6 and 10 below, and without assuming any direct customer relationship, it may still be necessary for the Institution to request or receive information from its Correspondent regarding one or more of the Correspondent's customers, including other financial institutions that are its customers (although the transfer of information may be subject to laws or regulations that may prevent the Correspondent from divulging information to the Institution).

2. What are the money laundering risks in Correspondent Banking?

Correspondent banking is a high volume, time sensitive business involving substantial flows of money through a number of otherwise unconnected financial institutions (usually in different jurisdictions). In many cases, no single party involved has a complete overview of the whole transactional flow. An Institution processes transactions initiated by its Correspondent for parties that the Institution does not, in many cases, have a direct relationship with, that are not its customers and on which it therefore has not conducted due diligence. These characteristics can make Correspondent accounts vulnerable to potential abuse by money launderers and it may be difficult for the Institution to prevent and or detect illegal activity.

3. Taking a risk based approach, what criteria should be considered to identify Correspondents that are Higher Risk?

Each correspondent banking relationship should be reviewed on its own merits, and Institutions should generally be able to expect that countries implement the necessary money laundering laws and that Correspondents' are appropriately regulated and supervised (absent information to the contrary from credible sources).[4]

In reviewing the correspondent banking relationship, consideration should be given to factors which could pose higher money laundering risks, either individually, in combination, or more

[4] “Credible sources” refers to information that is produced by well known bodies that are generally regarded as reputable and that make such information publicly and widely available. Such sources may include, but are not limited to, supra-national or international bodies such as the Financial Action Task Force, World Bank, the International Monetary Fund, the organisation for Economic Co-operation and Development ("OECD") and the Egmont Group of Financial Intelligence Units, as well as relevant national government bodies and non-governmental organisations such as Transparency International.

usually when taken together. Such factors were identified in the Principles, where the focus was primarily on **Country Risk** and **Customer Risk.** These two criteria remain the drivers of money laundering risks for Institutions.

Country Risk:

Country risk should be assessed with respect to a Correspondent to determine if there is a potential for money laundering because of factors that relate to a particular country. Factors that would result in a determination that a country poses a higher money laundering risk include whether a country:

- is subject to sanctions, embargoes or similar measures issued by, for example, the United Nations or otherwise where national laws apply;
- has significant levels of corruption, other criminal activity or is politically unstable as identified by credible sources;
- lacks appropriate anti-money laundering laws and regulations, or the laws and regulations are inadequately implemented, as identified by credible sources.

Institutions should consider the domicile and residence of the Correspondent, as well as the country where the Correspondent's ultimate parent is headquartered (for details see Principle 9). In appropriate circumstances (for example when dealing with higher risk correspondents), country risk may also include an assessment of the major geographic markets covered by the Correspondent.

Customer Risk:

Customer risk factors relate either to the organisation and set-up of the Correspondent, or the nature and scope of its business activities. Factors to be considered which could pose a higher money laundering risk include whether a Correspondent is a/an

- Offshore Correspondent;[5]
- Correspondent that has a Material PEP Involvement;[6]
- Correspondent that is not state owned or publicly owned (or part of a group of companies that are state owned or publicly owned), although the nature and extent of state ownership, or the conditions under which the Correspondent is listed and trades on a Stock Market may also be considered relevant.
- Correspondent providing higher risk correspondent services to its own customers;[7]

[5] “Offshore Correspondent” is a financial institution that is restricted, pursuant to its license, from conducting financial activities with citizens of, or in the local currency of, the country that issued the license. In this respect, note that a financial institution which would be an offshore financial institution but which is also a Regulated Affiliate (defined in section 5 of the Principles) should not be treated as higher risk per se, unless required by local law. In such cases, the Wolfsberg Group believes that the Institution should consider the risk relevant to the offshore correspondent's ultimate parent in the same way as described above for country risk.

[6] "Material PEP Involvement" may occur in a Correspondent where a Politically Exposed Person enjoys significant control or is able to exert inappropriate influence on the activities of the Correspondent, either by reason of ownership, position or otherwise. Such a situation is unlikely to occur with a publicly owned Correspondent. For the definition of a PEP see Wolfsberg AML Principles on Private Banking: www.wolfsberg-principles.com/standards

[7] 'Higher risk correspondent services' include Downstream Correspondent Clearing (defined in section 6 of the Principles) or other correspondent clearing services to other financial institutions which, were they

- Central Bank or Supra-National Organisation transacting in products and services other than those that would be in keeping with that entity's primary activities;[8]

- Licensed and regulated non-bank financial institution such as a remittance or, exchange house, casas de cambio, bureaux de change and money transfer agents;

- Correspondent conducting higher risk transactions[9] via the Institution;

- Correspondent conducting significant 'Red Flag' transactions[10] via the Institution.

Additional Risks

An Institution may also take into account other higher risk services that it provides to the Correspondent which may also affect the overall risk profile of the Correspondent, for example trading in higher risk services.[11]

Institutions can use the above criteria (which do not purport to be exhaustive), to develop their own risk models for identifying higher risk correspondents and in doing so, apply appropriate due diligence, approval, monitoring and scrutiny. Institutions should document their own methods and controls.

4. Does exchanging a SWIFT key require due diligence?

Where payment related information is exchanged or intended to be exchanged, Institutions need to carry out a relevant level of due diligence. Where an exchange of non-payment related information is intended, customer due diligence should in principle be unnecessary. In the latter case however, the Institution exchanging the test key for information purposes only may be used in the same way as if the Correspondent has an account with the Institution. Presently it is not possible to distinguish test key requests for the exchange of non-payment related information from those exchanged to allow payment instructions, therefore Institutions should preferably carry out client due diligence in cases where the Institution performs payments for the Correspondent or if not, immediately thereafter.

5. Should relationships with Higher Risk Correspondents be avoided completely?

No. The Wolfsberg Group does not advocate a general avoidance policy with respect to relationships with higher Risk Correspondents, although there are some relationships that should clearly be avoided. These include relationships:

- with shell banks[12]. Institutions should also exercise care to ensure that they do not knowingly deal with financial institutions that themselves deal with shell banks;

---

to be customers of the Institution directly, would reasonably likely be regarded as higher risk customers (and transactions originating from or for the order of such a financial institution are conducted through the Correspondents account with the Institution) and/or Correspondents that provide Payable Through Accounts[7].

[8] An example of such a situation may be where the Central Bank is making and receiving payments for and on behalf of non-governmental third parties.

[9] An example of such higher risk transactions may be substantial pouch and bankers draft activity.

[10] "Red Flag" transactions are set out in Appendix 1.

[11] See Wolfsberg Guidance on a Risk Based Approach for Managing Money Laundering Risks.

[12] "Shell Banks" as defined in section 5 of the Principles.

- with unlicensed and/or unregulated non-bank financial institutions such as remittance or, exchange house, casas de cambio, bureaux de change and money transfer agents or entities or persons effectively operating as such;

- with any Correspondent where the results from conducting due diligence produce significant uncertainties that cannot be resolved, or;

- where the Correspondent's AML controls are considered inappropriate and/or insufficient and the Correspondent does not satisfy the Institution that necessary remedial action will be undertaken.

A policy of general avoidance of Correspondents demonstrating factors posing higher money laundering risks could have the unintended result of diminishing the overall effectiveness of the international payments system and consequently international trade without any resulting benefit. It also unfairly prejudices the legitimate commercial interests of Correspondents that are identified or perceived as posing higher risks and may have the unintended and unfortunate consequence of moving transactional activity underground and beyond effective scrutiny. The Wolfsberg Group believes that relationships to be avoided should be identified by regulators and financial institution supervisors, who conduct regular inspections and are best placed to identify such risks and to ensure appropriate remediation.

6. Where Higher Risk Correspondents are identified, what measures could be considered to be taken by an Institution?

In the Principles, the Wolfsberg Group advocated that Correspondents presenting greater risk should be subjected to a higher level of due diligence. The Principles outlined the type of risk indicators that an Institution should consider in initiating the relationship, and on a continuing basis, to ascertain what reasonable due diligence or enhanced due diligence and ongoing and enhanced scrutiny it will undertake. The Wolfsberg Group additionally recognises the value of the measures promulgated by the FATF in their revised 40 Recommendations (Recommendation 7) and the contributions made by other supranational bodies such as the Basel Committee on Banking Supervision and national regulatory authorities as well as other expert bodies.[13] The Wolfsberg Group believes that the following measures are the most important, and should be applied to all Correspondents posing higher money laundering risks to an Institution -

- **Conducting Due Diligence**. Gathering sufficient information about a Correspondent to understand the nature of the Correspondent's business and determining from public, readily available information, the reputation of the Correspondent and the quality of supervision. This should include, to the extent that such information is available, whether the Correspondent has been subject to a money laundering or terrorist financing investigation or regulatory action. Information collected should enable the Institution periodically to "screen" the Correspondent's identified owners[14] and Senior Management for negative media coverage/information relevant to the risks posed by the Correspondent, including any new or previously unknown links to PEPs, sanctioned persons or legal entities etc. using the Internet and/or other, more specialised, available resources where appropriate.

[13] Expert bodies includes for this purpose are the New York Clearing House Members and the United Kingdom's Joint Money Laundering Steering Group on Money Laundering Prevention.
[14] With a shareholding of at least 10%.

- **Requesting and reviewing the Correspondent's KYC and AML practices**. Obtaining sufficient information regarding the Correspondent's AML programme to assess whether the Correspondent's AML related practices are adequate and appropriate. A useful tool in this regard is the Anti-Money Laundering Questionnaire which is referred to in the answers to Question 11 below and set out in full in Appendix 3. An Institution may also consider whether the Correspondent has verified the identity of, and performed on-going and appropriate due diligence on its customers' activity with the Correspondent through the Correspondent's account with the Institution and be satisfied that the Correspondent is able to provide relevant customer identification and due diligence information upon request to the Institution (This information may however be subject to laws and regulations to which the Correspondent is subject, and it may be that the Correspondent is prevented from divulging information regarding its customers). There may be cases, including where this is required by law, or part of its risk based approach, where an Institution might consider requesting information on the financial institutions to which the Correspondent itself provides correspondent banking services and/or on the customers having direct access to the Correspondent's account. This may be either on a generalised or specific basis to allow the Institution to make a further, reasonable assessment of their Correspondent and the business it undertakes. An Institution may also choose to obtain and review the appropriate KYC and AML Policies and Procedures to verify the information provided by the Correspondent.

- **Visiting or conducting physical meetings** with the Correspondent's identified owners and/or Senior Management.

- **The risk-based involvement of senior management[15] and an independent control unit**, perhaps compliance or a specialised money laundering unit both to approve new Correspondents and to review existing relationships periodically.

- The application of heightened scrutiny to the transactions conducted with the Correspondent (see answers to Questions 7, 8 and 9 below for details).

Whilst the Wolfsberg Group are aware of the recommendation "to document the respective responsibilities of each institution[16]," (understood to refer to the respective responsibilities towards each other with respect to money laundering prevention), such action cannot currently be described as common practice, and in any case such action would rarely be open to contracting parties bearing in mind the wider legal and regulatory environment to which financial institutions are subject. The Wolfsberg Group believes that in setting out both the Principles and these FAQs, the roles and responsibilities of financial institutions conducting correspondent activity can be more fully understood and more widely accepted.

7. What role does transaction monitoring play in managing money laundering risks in Correspondent banking?

Section 12 of the Principles states that financial institutions should implement policies and procedures to facilitate the identification of unusual or suspicious activity and reporting, as required by applicable law. Furthermore, in its Statement on Monitoring Screening and Searching[17], the Wolfsberg Group advocated that financial institutions should have appropriate processes in place that allow unusual activity and unusual patterns of activity or

[15] "Senior Management" is described in the Principles at section 5.
[16] As per Recommendation 7 FATF Revised 40 Recommendations.
[17] Copy available at www.wolfsberg-principles.com/standards

transactions to be identified. Since unusual transactions or patterns of activity are not 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 a means of ensuring that this role is fulfilled.

In Correspondent Banking businesses however, the volume and speed of transactions and their commonality, combined with the lack of specific or complete information regarding the Correspondent's customer and the beneficiary of the transaction, makes monitoring of transactions by the Institution more difficult than for other business involving direct dealings with customers. Nevertheless, Institutions do still commonly monitor their Correspondents' transactions, by employing rules or threshold based "triggers," designed to identify unusual and potentially suspicious transactions based on published typologies. Such "triggers" then identify transactions that can be more closely examined. More recent transaction monitoring systems have been designed to identify unusual Correspondent activity or unusual activity vis-à-vis a Correspondent's prior activity over a given period. There have also been systems designed to assess one Correspondent's activity against a so-called "peer" or "peers" (i.e. a cluster of Correspondent banks with similar profiles and transaction patterns). However, perhaps due to the limited numbers of relationships involved, there has not yet been sufficient information to provide statistical samples on the efficiency of this type of monitoring.

8. How should an Institution design and maintain an effective and efficient transaction monitoring system?

It is the view of the Wolfsberg Group that the Institution's monitoring activity can be helpful (although probably more so if the beneficiary of a transaction is a customer and less so if there is no direct relationship). However, the Institution's monitoring should not be considered a replacement for the Correspondent monitoring its own customers' transactions and to investigate unusual or suspicious activity that it identifies.

The Wolfsberg Group believes that Institutions should increasingly use their monitoring capabilities to identify potentially suspicious transactional Correspondent activity and to investigate further where concerns arise over such transactions. The Wolfsberg Group advocates taking a risk based approach, allowing Institutions themselves to determine the extent to which their monitoring resources should be employed, in particular, having regard to the nature and extent of their relationships and business with Correspondents.

The Wolfsberg Group cautions that, even in cases where potentially suspicious transaction types and patterns are identified, care must still be exercised. None of these transactions types or patterns (with the exception of transactions involving shell banks) should automatically be considered suspicious without further investigation. Where such transaction types or patterns are identified, there may often be acceptable explanations for such activity.

Employing single, simple triggers, to identify large transactions for example, or transactions coming from particular countries, particularly where the Correspondent is based, are generally ineffective and conversion rates[18] are extremely low. A more effective way to improve conversion rates seems to be for Institutions to focus on identifying significant and relevant unusual activity and by identifying specific transaction types and patterns, where these can either be isolated or combined, as shown in Appendix 1. By focussing on improving conversion rates, Institutions will improve the effectiveness and efficiency of their monitoring

[18] Conversion rates can generally be used to assess the effectiveness and efficiency of a transaction monitoring system by, for example, dividing the number of alerts generated by established rules; e.g. thresholds, triggers etc. by the number of suspicious activity reports filed. The greater the percentage, the greater the conversion rate, and the greater the likely effectiveness and efficiency of the system.

programmes and at the same time, should improve the quality of reporting to government authorities.

To this end, the Wolfsberg Group has summarised certain types and patterns of transactions ("Red Flag Transactions" in Appendix 1), conducted over correspondent accounts that have been identified in publicly available sources as being illustrative of potentially suspicious activities. In respect of these activities, the Wolfsberg Group has suggested possible monitoring responses that could be investigated further, with the assistance of law enforcement and government agencies in their efforts to combat money laundering by, *inter alia*, further developing effective and efficient transaction monitoring programmes.

9. What additional transaction monitoring should be conducted for Higher Risk Correspondents?

For the reasons described above, it is critical that the Correspondent performs effective transaction monitoring, and reasonable for the Institution to expect that this will be done. The Wolfsberg Group believes that the Institution should structure its own transaction monitoring systems so that relationships with Higher Risk Correspondents are subject to monitoring where:

- rules and threshold are more narrowly drawn to facilitate closer scrutiny; and
- the level of deviation permitted in respect of unusual activity prior to alerts being generated (if such tools are employed) is reduced, compared to those permitted for non-higher risk Correspondents.

The primary responsibility for due diligence, customer acceptance and ongoing monitoring of correspondent banking relationships must lie with a clearly identified individual relationship manager, business unit or department. The Wolfsberg Group advocates that a body within the institution which is independent from those responsible for the relationship with the Correspondent, should be involved in defining (including amending) the parameters and for reviewing the effectiveness of that monitoring.

A regular review of the overall transactional activity with higher risk Correspondents may be appropriate.

An Institution may decide to place limits or restrictions on transaction types and/or amounts and or volumes and or involvement in transactions with particular countries for a limited or an indefinite period, perhaps to correspond with any expected activity.

10. What should an Institution do if it identifies unusual correspondent account activity with no apparent explanation?

The extent and quality of information an Institution has on a transaction initiated by Correspondent may be limited due to the indirect nature of the relationship between the Institution to the originator and/or beneficiary. Nevertheless, questionable activity should be investigated in a timely fashion, in accordance with an Institution's Policies and Procedures, and conclusions drawn on the basis of the information available. In certain circumstances, Institutions may feel it could be helpful either to request additional information from the Correspondent, or to request the Correspondent to perform its own investigation into the relevant transaction(s), which may include requesting or receiving information on a customer of the Correspondent. However, an Institution should be aware of laws and regulations to which the Correspondent is subject, and it may be that the Correspondent is prevented from divulging information regarding its customers. In these circumstances an Institution may consider whether it can gain comfort from the Correspondent's reassurance that it has

reviewed the customer's transaction in accordance with the latter's profile and that it is consistent with that profile.

11. What is the Wolfsberg International Registry? What information can be found in the Wolfsberg International Registry? What is the Anti-Money Laundering Questionnaire?

In the Principles, the Wolfsberg Group encouraged the development of an international registry for financial institutions. Upon registering, financial institutions would submit information useful for conducting due diligence as outlined in the Principles. Financial institutions would use this information in due diligence. The Bankers' Almanac recently initiated a new product, the Bankers' Almanac "Due Diligence Module", developed as part of BANKERSalmanac.com. The "Due Diligence Module", which has been endorsed by the Wolfsberg Group, is a repository for the collection and storage of relevant due diligence information and documentation. By submitting due diligence information to the "Due Diligence Module" of Bankers Almanac, the Wolfsberg Group believes that financial institutions will eliminate some, and eventually, most of the need to reproduce, and repeatedly supply, due diligence information. Instead, financial institutions can direct inquiries to the "Due Diligence Module", where the most up to date due diligence information will always be stored. The Wolfsberg Group encourages all financial institutions to review the Due Diligence Module and contact Bankers Almanac to submit, at no cost, due diligence information regarding their institutions.

In conjunction with the Wolfsberg Group, Bankers Almanac has developed a list of required documents, reflecting recognised best practices with respect to necessary information to complete appropriate due diligence on financial institutions. A copy of the list of required documents is set out in Appendix 2**.** The Due Diligence Module can be viewed at: www.bankersalmanac.com/addcon/home/duedm.htm.

The Registry will include information on each financial institution's license (and the licenses of their subsidiaries) and copies of corporate governance documents, such as, company by-laws, Memorandum, Articles or Certificate of Incorporation, or Memorandum, Articles or Certificate of Association. In addition, there will be biographies of board members and senior management of the financial institution, annual reports (including the annual reports of subsidiaries), and a completed, standard form Anti-Money Laundering Questionnaire.

To provide due diligence information and documentation, or to obtain further information, Bankers Almanac can be contacted at: The Bankers' Almanac, Windsor Court, East Grinstead, RH19 1XA, United Kingdom, facsimile: +44 (0) 1342 335940, or email at: duediligence@bankersalmanac.com.

The Anti-Money Laundering Questionnaire has been designed to provide an overview of a financial institution's anti-money laundering policies and practices. There are no correct or incorrect responses. The Questionnaire requires an explanation when a "No" response is chosen (this does not imply that a "No" response is incorrect) and allows for an explanation when a "Yes" response is chosen. A copy of the Questionnaire is set out in Appendix 3.

Appendix 1 - "Red Flag" Transactions and Possible Monitoring Responses

1. Red Flag Transactions - Publicly Identified Potentially Suspicious Transactions

The monitoring of transactions and/or dealing with the outcome of the results of such monitoring may be difficult for the Institution particularly where entities such as shell banks are involved. The following examples are illustrative of possible suspicious transactional correspondent activity and are derived from publicly available sources.[19] They are illustrative of wire transfers in particularly large amounts and/or in particularly large volumes/frequencies and/or in "bursts" of activity occurring within a short period of time ("Red Flag Transactions"):

- transactions involving high risk countries vulnerable to money laundering (if and to the extent this can be identified);
- transactions with those Correspondent relationships already identified as higher risk Correspondents;
- large (value or volume) transaction activity involving monetary instruments; (e.g. travellers cheques, money orders, bank drafts) - especially involving instruments that are sequentially numbered;
- transactional activity that appears unusual in the context of the relationship with a Correspondent;
- transactions involving shell banks;
- transactions involving shell corporations;
- transaction activity frequently involving amounts that are just less than any locally mandated transaction reporting requirements, or transactions or enquiries that appear to test or identify an Institution's own internal monitoring thresholds or controls.

2. Possible Monitoring Responses by Institutions

The Wolfsberg Group is committed to co-operating with, and assisting, law enforcement and government agencies in their efforts to combat money laundering by, *inter alia*, developing and operating effective and efficient transaction monitoring programmes. The Wolfsberg Group has identified the following possible monitoring responses that could be further investigated by Institutions, in seeking to address some of the "Red Flag" Transactions highlighted above:

- identifying Correspondents whose accounts are operating significantly outside the parameters that would otherwise be expected, based either on the information

[19] These sources include, *inter alia,* the FATF Report on Money Laundering typologies 2001- 2002 - Correspondent Banking**;** FINCEN SAR Activity Review Trends Tips & Issues (August 2004) - Indicators of possible Misuse of Shell Corporations and Shell Banks; Guidelines for Counter-Money Laundering Policies and Procedures in Correspondent Banking - The New York Clearing House Association LLC - Section 4.1 Examples of Possible Suspicious Correspondent Account Activity; Swiss Federal Banking Commission Money Laundering Ordinance 2002 - Schedule: Indicators of Money Laundering; Basel Committee on Banking Supervision, Customer Due Diligence for Banks - October 2001.

received during due diligence, or from previous behaviour regarding expected activity and/or monitoring for significant divergences from this expected activity, whether in respect of volumes, values and/or frequency of transactions are concerned. For higher risk Correspondents, consider reducing the level of acceptable divergence before identification of the relationship occurs;

- identifying Correspondent transactions which have passed through several different jurisdictions or financial institutions prior to or following the Institution's involvement, without any apparent purpose other than to disguise the nature, source, ownership or control of the funds. Particular concerns may arise where the prior or subsequent transactions involve high risk countries (particularly NCCT), vulnerable to money laundering and therefore transactions connected to such countries should be monitored;

- identifying wire transactions with the following attributes or combined attributes, for example large, even-currency amounts and/or repetitive wire transfers from a particular originator to a particular beneficiary, and/or individual wire transactions conducted within a short period of time (such as on a daily basis, twice daily or every other day);

- identifying the deposit, or withdrawal, of monetary instruments with the following attributes or combined attributes; for example, if sequentially numbered, and/or in large amounts, or just below a locally mandated transaction reporting threshold, and/or in a short space of time (e.g. on the same day);

- identifying transactions where activity appears to be structured either to avoid an Institution's monitoring systems and/or to be just below a locally mandated transaction reporting threshold or trigger;

- identifying suspected shell banks by reliance on lists provided from reliable and credible sources;[20]

- identifying suspicious shell corporations that do not provide adequate information about ownership by reliance on lists provided from reliable and credible sources..[21]

[20] To our knowledge no public lists are available identifying Shell Banks. The Wolfsberg Group would welcome any attempt by public authorities to make publicly available lists of Shell Banks remaining in operation. The Wolfsberg Group is not convinced that it is otherwise possible to identify Shell Banks simply from their transactional activity via an Institution, unless the Shell Bank is a Customer of the Institution, in which case the Institution should in any event close the relationship.

[21] Again, to our knowledge no such public lists are available, although it appears that many governmental authorities may have information/lists of corporations that may be used as "fronts" for individuals/organisations of concern. The Wolfsberg Group would welcome any attempt by public authorities to make publicly available lists of such corporations. The Wolfsberg Group is not convinced that it is otherwise possible to identify suspicious shell corporations simply from their transactional activity via an Institution unless the shell corporation is a Customer of the Institution.

Appendix 2 - Bankers' Almanac Due Diligence Module

Required Documents and Information from Financial Institutions:

1. Response to Anti-Money Laundering Questionnaire
2. Dated copy of Corporate Anti-Money Laundering Policies and/or Procedures
3. USA Patriot Act Certification – for institutions required to provide Certifications
4. Biographies of Board Members and Senior Management
5. List of owners (as well as other identifying information, such as address, etc.) who directly or indirectly own, control or have the power to vote 10 percent or more of any class of voting securities for any company that is not publicly traded. For companies that are publicly traded identify the exchange on which the company is traded
6. Latest Annual Report, including Annual Reports of subsidiaries.
7. Copy of license and licenses of subsidiaries (with English translation if original license is in language other than English)
8. Copies of corporate governance documents, such as:
    - Company by-laws
    - Memorandum, Articles or Certificate of Incorporation
    - Memorandum, Articles or Certificate of Association
9. Extract from commercial register

Appendix 3 - Bankers' Almanac AML Questionnaire

I. General AML Policies, Practices and Procedures:		
Does the AML compliance program require approval of the FI's Board or a senior committee thereof?	Y ❑	N ❑
Does the FI have a legal and regulatory compliance program that includes a designated Compliance officer that is responsible for co-ordinating and overseeing the AML program on a day-to-day basis, which has been approved by senior management of the FI?	Y ❑	N ❑
Has the FI developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions that has been approved by senior management?	Y ❑	N ❑
In addition to inspections by the government supervisors/regulators, does the FI Customer have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?	Y ❑	N ❑
Does the FI have a policy prohibiting accounts/relationships with shell banks (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)?	Y ❑	N ❑
Does the FI have policies covering relationships with politically exposed persons consistent with industry best practices?	Y ❑	N ❑
Does the FI have appropriate record retention procedures pursuant to applicable law?	Y ❑	N ❑
Does the FI require that its AML policies and practices be applied to all branches and subsidiaries of the FI both in the home country and in locations outside of the home country?	Y ❑	N ❑
II. Risk Assessment		
Does the FI have a risk focused assessment of its customer base and transactions of its customers?	Y ❑	N ❑
Does the FI determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the FI has reason to believe pose a heightened risk of illicit activities at or through the FI?	Y ❑	N ❑
III. Know Your Customer, Due Diligence and Enhanced Due Diligence		
Has the FI implemented systems for the identification of its customers, including customer information in the case of recorded transactions, account opening, etc. (for example; name, nationality, street address, telephone number, occupation, age/date of birth, number and type of valid official identification, as well as the name of the country/state that issued it)?	Y ❑	N ❑
Does the FI have a requirement to collect information regarding its customers' business activities?	Y ❑	N ❑
Does the FI collect information and assess its FI customers' AML policies or practices?	Y ❑	N ❑
Does the FI have procedures to establish a record for each customer noting their respective identification documents and Know Your Customer Information collected at account opening?	Y ❑	N ❑
Does the FI take steps to understand the normal and expected transactions of its customers based on its risk assessment of its customers?	Y ❑	N ❑
IV. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds		
Does the FI have policies or practices for the identification and reporting of transactions that are required to be reported to the authorities?	Y ❑	N ❑
Does the FI have procedures to identify transactions structured to avoid large cash reporting requirements?	Y ❑	N ❑
Does the FI screen transactions for customers or transactions the FI deems to be of significantly high risk (which may include persons, entities or countries that are contained on lists issued by government/international bodies) that special attention to such customers or transactions is necessary prior to completing any such transactions?	Y ❑	N ❑
Does the FI have policies to reasonably ensure that they will not conduct transactions with or on behalf of shell banks through any of its accounts or products? (A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.)	Y ❑	N ❑
Does the FI have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?	Y ❑	N ❑
V. Transaction Monitoring		
Does the FI have a monitoring program for suspicious or unusual activity that covers funds transfers and monetary instruments (such as travellers checks, money orders, etc.)?	Y ❑	N ❑
VI. AML Training		
Does the FI provide AML training to relevant employees that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?	Y ❑	N ❑
Does the FI retain records of its training sessions including attendance records and relevant training materials used?	Y ❑	N ❑
Does the FI have policies to communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?	Y ❑	N ❑
Does the FI employ agents to carry out some of the functions of the FI and if so does the FI provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the FI's products and services and internal policies to prevent money laundering?	Y ❑	N ❑