THE JOINT FORUM

BASEL COMMITTEE ON BANKING SUPERVISION
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

June 2003

Initiatives by the BCBS, IAIS and IOSCO to combat money laundering and the financing of terrorism

This joint note from the Basel Committee on Banking Supervision (BCBS), International Association of Insurance Supervisors (IAIS) and International Organization of Securities Commissions (IOSCO) provides a record of the initiatives taken by each sector to combat money laundering and the financing of terrorism. It was first prepared for the March 2003 Joint Forum meeting in Hong Kong, and thereafter submitted for the information of the Coordination Group at its March 2003 meeting in Berlin. The note is intended to be descriptive rather than prescriptive, and does not attempt to be comprehensive in its coverage of anti-money laundering/combating the financing of terrorism (AML/CFT) issues.

To the extent that institutions in each sector are offering the same services, AML/CFT measures and standards need to be reasonably consistent, otherwise there would be a tendency for criminal funds to flow to those institutions in those sectors operating under less stringent standards. However, variations in patterns of relationships between institutions and customers in each sector require AML/CFT requirements to be tailored to the circumstances of the relationship. Hence, AML/CFT standards may reasonably differ in the detail and intensity of their application.

This note is divided into two parts. The first Part provides an overview of the common AML/CFT standards that apply to all three sectors and an assessment as to whether there are serious gaps or inconsistencies in approaches and recommendations. Part 2 consists of contributions by each of the three Secretariats. This is in three sections and covers, for each sector: the relationships between the institutions and their customers focussing on the products or services that are particularly vulnerable to money laundering; how each Committee has sought to address these vulnerabilities; and, finally, a description of ongoing and future work.

Part I: Overall assessment

The AML/CFT elements common to all three financial sectors are essentially prescribed by the FATF's 40 Recommendations and its subsequent eight special recommendations. The 40 Recommendations are currently under review and will lead to further changes in the standards prescribed. Just recently the FATF has worked with the IMF and World Bank to develop a "*Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards*" (the Methodology). The BCBS, IAIS and IOSCO were consulted at several stages in the development of this document, and especially on the content of three annexes applicable to each sector. This comprehensive Methodology is already being used as the basis for FATF and FATF-style mutual

evaluations, as well as by the IMF and World Bank in the Financial Sector Assessment Program (FSAP) and by the IMF in the Offshore Financial Centre Assessment Program.

The FATF standards and the Methodology encompass the following aspects of AML/CFT:

- customer identification;
- ongoing monitoring of accounts and transactions;
- record-keeping and reporting of suspicious transactions;
- internal controls and audit;
- integrity standards; and
- cooperation between supervisors and other competent authorities.

Given the broad scope of coverage of the FATF standards, it seems to the authors that there are no serious gaps or inconsistencies in the approaches to AML/CFT in the three sectors.

The Methodology further contains sector-specific criteria for banking, insurance and securities supervision of AML/CFT established by the BCBS, IAIS and IOSCO. The sector-specific criteria for bank supervision are the most detailed and extensive of the three sectors in recognition of the greater vulnerability of the banking sector. In the assessments conducted recently, national authorities have in fact scored quite poorly against the banking criteria. Nonetheless, the fact that the individual sector criteria are included within and examined under the Methodology means that the principles laid down are highlighted for national authorities and provide a benchmark for them to aim at.

From the specific perspective of the Joint Forum, questions arise concerning group-wide application of AML/CFT processes. Customer due diligence (CDD) by members of cross-sector financial groups creates unique issues not present where a financial institution operates in a single sector on a stand-alone basis. For example, each financial group needs to have internal control arrangements in place to be able to determine whether a customer of one member of the group is also a customer of another member of the group. This means that the financial group should have systems and processes in place to monitor the identity of customers of the entire group, and to be alert to customers that use their services in different sectors.

However, this principle of group-wide risk management does not imply that CDD requirements must be exactly the same across the banking, securities and insurance sectors. Differences in the nature of institutions' activities and operations in the various sectors may justify variations in the CDD requirements imposed on each sector. What is important from a level playing field perspective is that the same activities be regulated the same, whether an institution is licensed to operate in one sector or another.[1]

While variations in the patterns of relationships between institutions and customers in each sector may require customer identification requirements to be tailored to the circumstances of the relationship, there are sound reasons for broad consistency, not least level playing

[1] This approach to competition issues between sectors is reflected in the EU's regulation of financial services, as the requirements applicable to investment firms regarding their investment services activities are also imposed on banks regarding their investment services activities. However, requirements applicable to deposit taking and lending imposed on banks are not imposed on investment firms, which by definition do not take deposits or make loans. Additionally, while, at one point, the EU considered incorporating insurance into the harmonised regime applicable to banks and investment firms, variations in the activities of insurance companies ultimately led the EU to develop an independent regulatory regime for insurance companies.

field considerations. Many financial groups now engage in banking, securities and insurance businesses, and it is important there is consistent application of CDD on a consolidated basis. Customers of one arm of a financial group will likely be conducting business with other members of the group and it makes no sense from a risk management perspective to apply different CDD standards to the same persons or entities for the same activities. Moreover, a customer relationship issue that arises in one part of a financial group would affect the reputation risk of the whole group.

Another question relevant to the Joint Forum arises in relation to the cross-selling of products within mixed financial groups. The issue is whether simplified CDD would be acceptable in cases where one member of a group is approached by a customer from a different arm of the group. Prima facie, it would seem reasonable to rely on the CDD conducted by the affiliate. However, this does raise questions of completeness of due diligence and access to the information that may be housed in another arm of the group, if the customer identification and acceptance procedures for one arm are different from those for another arm. A similar issue arises if a customer wishes to perform a similar activity in a different country where the CDD standards might be more strict.

The revised 40 FATF Recommendations will provide an opportunity for the standard-setting organisations to review their standards and guidance taking account of each others' work in this respect with the aim of preventing as far as possible inconsistencies between their standards and guidance where this is unwarranted from a risk-based approach.

Part 2: Sector contributions

This Part contains the contributions from the three Secretariats.

1. Nature of customer relationships and specific vulnerabilities of each sector

Banking

By its nature, because of its ability to move funds rapidly, the banking system is especially vulnerable to money laundering. Customers of the bank include the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners) and the beneficiaries of transactions conducted by professional intermediaries. The account holder can be a customer that does not present himself or herself for interview at the bank (i.e. a non-face-to-face customer) or one introduced to the bank by a third-party. It may also be a legal entity (e.g. corporate, trust) interposed between the ultimate beneficial owners and the bank, or a professional intermediary (e.g. mutual fund, lawyer) depositing funds that it manages for its clients.

Specific activities for which the risk of money laundering is relatively higher are:

- Customers who use fronts (e.g. trust, corporates, professional intermediaries) to open an account so as to hide their true identities.
- Private banking operations, which by nature involve a large measure of confidentiality.
- Customers who are politically exposed persons (PEPs) may significantly raise the potential for reputation risk.
- Introduced business, where a bank may place undue reliance on the due diligence conducted by an introducer.

- Correspondent banking business, especially where banks do not fully understand the nature of the respondent banks' business, or if the respondents are shell banks or located in a jurisdiction which has poor know-your-customer standards.

Insurance

The IAIS is fully aware that the insurance industry is at risk of being misused by criminals for fraudulent activities, and has agreed that work in this area should be amongst the Association's priorities. The financial resources of insurance companies will in particular attract fraudsters. However, the nature of the insurance business means that other financial institutions are more vulnerable to money laundering.

In insurance several parties could be involved in transactions that may raise the possibility for money laundering: the insurer, the policyholder, the insured person and the beneficiary. The contracting parties are generally free - within the boundaries of law – to determine the conditions of the insurance contract e.g. with respect to the duration, benefits, early surrender and designation of beneficiaries.

The insurance industry has several ways to market its products. Some companies (direct writers) sell insurance directly to the customer and have their own call centres or agents. Some companies use intermediaries. These intermediaries could work exclusively for the company in question or work independently, i.e., selling products for more than one company. Sometimes insurance companies use other companies in the same group to market its products, e.g. sales over the counter of bank branches.

In insurance, risk assessment and premium-setting are essential elements within the underwriting process. To assess risk, information on the background of the client is collected, investigated and filed, especially in the case of insurance of large risks. Various 'trigger events' occur after the contract date and indicate where due diligence is also applicable. These trigger events include claims notification and surrender requests. Well understood, self-interest leads insurance companies to be careful in their payment of claims which are normally only paid after thoroughly checking the circumstances of the loss and the identity of the claimant.

Examples of the type of contracts that are particularly attractive as a vehicle for laundering money are single premium investment policies, i.e.

- unit-linked single premium contacts
- purchase of annuities;
- lump sum top-ups to an existing life insurance contract;
- lump sum contributions to personal pension contracts.

Securities

The customer of an investment service provider can be a person or entity that opens a securities account on its own behalf or on whose behalf a securities account has been opened. A customer can open an account with an investment service provider in person or via remote means (e.g., internet), and the opening of such account would generally establish a direct relationship between the investment service provider and the customer. It is possible for a direct relationship to be established between an investment service provider and a customer where a third party introduces the customer to the investment service provider. There also exist indirect relationships in the securities industry, such as where an investment services provider maintains an account for another provider (i.e., omnibus account).

Investment services providers generally do not maintain cash deposit accounts for their customers. Rather, they require their customers to remit funds to them either by check or by wire transfer to the deposit account of the investment firm at a bank. [2] Consequently, the securities industry is less at risk than the banking sector regarding the placement of laundered funds directly into the securities industry. However, the securities industry is potentially vulnerable to the layering of laundered funds subsequent to the placement phase.

Specific activities which the securities sector is potentially vulnerable to the risk of money laundering include:

- The activities of employees that unwittingly are requested to take actions which further a customer's money laundering scheme and the activities of rogue employees who undertake activities (in violation of the firm's internal controls and policies) such as the establishment of bank and securities accounts in multiple jurisdictions on behalf of the customer and the transfer of funds and securities between such accounts in furtherance of a customer's money laundering scheme. While the risk of rogue employees is not unique to the securities sector, the types of activities these employees engage in may differ from those in the banking and insurance sectors.
- Acceptance of orders and related funds from intermediaries or banks operating from jurisdictions that do not have an effective AML/CFT system in place to prevent the introduction of laundered funds into the firms and banks operating in those jurisdictions or in which the securities regulator and/or banking supervisor will not share information regarding customer positions or funds held by or through firms operating in that jurisdiction with non-domestic regulators.
- Wash sales or other fictitious trading schemes to transfer money or value through the clearing and settlement infrastructure. Reciprocal trades in offsetting positions can generate profits in the account of one party and losses in the account of the other party. In this type of scheme, the money launderers intentionally generate trading losses in a securities account into which criminal proceeds have been deposited and generate reciprocal trading profits in a seemingly unrelated securities account that cannot be easily identified or associated with the money laundering scheme. When the trades are liquidated, the profits are paid in the ordinary course through the clearance and settlement system from the account/party suffering the loss to the account/party earning the profit. Value can also be transferred between parties through the sale of shares in small, illiquid issues at artificially arranged prices, without regard to fair market value. Such schemes may or may not also involve an intent to generate additional profits from a manipulation of the value of the shares. Such schemes often constitute a violation of the securities laws as well as a money laundering offence.

[2] If a jurisdiction permits universal banking, however, and a bank is authorised to provide investment services as well as undertake deposit taking and lending activities, the universal bank, in its capacity as a bank, can maintain cash deposit accounts for its investment service customers. A universal bank is subject to the AML/CFT system applicable to banks generally in its jurisdiction regarding its deposit taking activity on behalf of its investment services customers.

2. Guidance provided to address vulnerabilities

Banking

The BCBS, in its *Customer due diligence for banks* (CDD) paper in October 2001 issued prudential guidance for CDD which are applicable to AML/CFT. This paper sets out standards and provides guidance for the development of appropriate practices by banks in this area. Adequate due diligence on new and existing customers is a key element. Banks must develop policies and procedures in key areas such as customer acceptance, customer identification, ongoing monitoring of high-risk accounts and risk management. The essential elements for these are presented in this paper, together with recommendations for more rigorous standards of due diligence for higher-risk areas. Specific examples are:

- Banks should take decisions to enter into business relationships with higher risk customers at the senior management level.
- Banks should identify the beneficial owners of all accounts. Guidance is provided on the persons to be identified where the customer is a non-natural person, such as a trust, corporate, or professional intermediary. If a bank is unable to identify the beneficial owner to its satisfaction, it should refuse the business.
- Banks should apply enhance due diligence for private banking operations. There should be policies and procedures for handling banking relationships with PEPs.
- Banks should use the conditions below when determining whether it can rely on introducers. These conditions also apply to a number of other areas, e.g. to assess whether reliance can be placed on the due diligence performed by professional intermediaries and to respondent banks in a correspondent banking relationship:
  - The introducer complies with the minimum CDD standards required of banks;
  - The CDD procedures of the introducer are as rigorous as those which the bank would have conducted itself for the customer;
  - The bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
  - The bank must reach agreement with the introducer that it will be permitted the right to verify the due diligence undertaken by the introducer; and
  - All relevant identification data and other documentation pertaining to the customer's identity are immediately submitted by the introducer to the bank
- For correspondent banking, banks should fully understand the nature of the respondent bank's management and business; should refuse to enter into or continue a correspondent banking relationships with foreign shell banks; and should pay particular attention when continuing correspondent banking relationships with respondent banks located in jurisdiction with poor know-your-customer standards.

In addition to customer identification, the CDD paper provides recommendations for:

- The ongoing monitoring of accounts;
- Appropriate compliance and internal audit functions within the bank;
- Application of an accepted minimum standard of KYC policies and procedures on a global basis;
- Supervisory obligations and powers in the implementation of KYC in a cross-border context.

Recommendations in the CDD paper have been incorporated into the Methodology, which has become the uniform basis for assessing the implementation of AML/CFT measures in all countries. A main feature in the sector-specific criteria for banks is the level of detail on customer identification, drawn from the CDD paper. They have since been amplified in a special paper on account opening and customer identification procedures that was issued in February 2003 (see section 3) in order to provide banks with detailed guidance on the nature of information that it may be reasonable to request from new customers.

Among the more complex issues addressed by the CDD paper is the identification of beneficial owners where the customer is a non-natural person and the criteria for determining when a bank can rely on introducers/intermediaries. Customers who are non-natural persons and the reliance on intermediaries are not unique to the banking business.

Insurance

The IAIS is committed to preventing the misuse of insurance companies for money laundering purposes by giving guidance to insurance supervisory authorities as well as, as appropriate, to the insurance industry and by strengthening cooperation between its members as well as with the industry.

At present the above-mentioned guidance is given through the Anti-Money Laundering Guidance Notes for Insurance Supervisors & Insurance Entities (January 2002). The "Guidance Notes" address the use of insurance entities to launder the proceeds of crime and stress the importance of "knowing your customer" principles, and the need for co-operation with law enforcement authorities in this area.

Insurance entities that are through the nature of their business vulnerable to ML should be constantly vigilant in deterring criminals from making use of them for the purpose of money laundering. The duty of vigilance is to avoid assisting the process of laundering and to react to possible attempts of insurance entities being used for that purpose. The duty of vigilance consists mainly of the following elements:

(a) Underwriting checks;

(b) Verification of identity;

(c) Recognition and reporting of suspicious customers/transactions;

(d) Keeping of records;

(e) Training.

All insurance entities that are through the nature of their business vulnerable to ML should have an effective anti-money laundering programme in place which enables them:

- in the case of insurers, to foster close working relationships between underwriters and claims investigators;
- to determine (or receive confirmation of) the true identity of prospective policyholders and where the applicant for an insurance policy is acting on behalf of another person, to take steps to verify the identity of the underlying principal. In this respect an insurance entity should not enter into a business relationship or carry out a significant one-off transaction if it is unable to identify and verify the identity;
- to recognise and report suspicious transactions to the law enforcement authority and insurance supervisor;
- to keep records for (a prescribed) period of time;

- to train staff *(key staff should have a higher degree of training);*
- to liaise closely with the law enforcement authority and insurance supervisor on matters concerning *vigilance policy* and systems;
- to ensure that internal audit and compliance departments regularly monitor the implementation and operation of vigilance systems;
- to assure ongoing compliance with all relevant laws and regulations;
- to designate an officer who is responsible for day-to-day compliance with current regulations. Large entities may have a separate money laundering reporting officer;
- to establish high ethical standards in all business and require compliance with laws and regulations governing financial transactions; and
- to ensure cooperation with law enforcement authorities, within the confines of applicable law.

- The IAIS invites representatives from the industry, law enforcement and FIUs to make case studies and typologies on money laundering available to raise awareness and to enable the insurance companies and supervisors to implement effective AML controls.

The IAIS' "Guidance Notes" have been incorporated into the FATF's "Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards".

Securities

Because of the multiplicity of arrangements for the trading and settlement of securities and the patterns of relationships incident to the provision of investment services, across markets and product types domestically, and across jurisdictions, IOSCO has not sought to develop a single AML/CFT system that could be made applicable to the securities sector internationally. Rather, IOSCO has adopted a high level principle that regulators should require market intermediaries to have in place policies and procedures designed to minimise the risk of the use of an intermediary's business as a vehicle for money laundering,[3] Thus, IOSCO has left it to its individual members to develop the specific requirements relating to an effective AML/CFT regime within their respective jurisdictions.

However, numerous IOSCO reports and resolutions bear on the implementation of an AML/CFT scheme by national securities regulators. The IOSCO Technical Committee issued an initial "Report on Money Laundering" in 1992[4] which, among other things, discusses the significance of the original FATF 40 Recommendations to the securities industry. Moreover, while not specifically directed at the prevention of money laundering, many of the regulatory mechanisms and procedures that have been instituted in the securities industry to accomplish the objectives of securities regulation can be and are, in practice, used to aid in investigations of money laundering. A number of IOSCO reports and resolutions bear on issues relating to the beneficial ownership of positions and customer identification, particularly the Resolution on Principles for Record-keeping, Collection of Information,

[3] IOSCO Objectives and Principles of Securities Regulation (Updated February 2002).

[4] IOSCO Public Document No. 26, at http://www.iosco.org/iosco.html.

Enforcement Powers and Mutual Cooperation to Improve the Enforcement of Securities and Futures Laws (November 1997).[5]

Because of the approach outlined above, the AML/CFT regimes adopted nationally by IOSCO's members or voluntarily adopted by investment services providers in particular jurisdictions are not entirely uniform. At the same time, certain characteristics are common. An AML/CFT regime of an investment services provider generally consists of CDD requirements and other internal controls and procedures. CDD generally is conducted by the investment service provider who has the direct relationship with the customer. Investment services providers also generally adopt other internal controls to address the risks that their business will be used as a vehicle for money laundering. Appropriate internal controls include the adoption of a written internal policy regarding the prevention of the use of the firm for money laundering, the establishment of management controls to prevent the involvement of the firm in money laundering schemes, and due diligence programs and contractual methods for the firm to be able to obtain the kinds of client identification information that it and its regulatory authority may require.

3. Ongoing and future work

Banking

The BCBS has been promulgating the standards in the CDD paper to supervisors worldwide and to the banking industry. In February 2003, the Committee released a *General guide to good practice on account opening and customer identification*. This document is aimed at assisting banks to develop an effective customer identification programme. The focus is documentation requirements and information items that should be gathered and verified for different types of bank customers, who may be natural persons or institutional customers.

The BCBS continues its work on developing further guidance on AML/CFT. Presently it is developing guidance on consolidated know-your-customer risk management for a banking group. A consolidated approach allows for consistency in the identification and monitoring of customer accounts across business lines and geographical locations throughout the group. This note should be completed in the third quarter of 2003.

Insurance

The IAIS has designated AML/CFT as an important issue in the supervision of insurance companies. For this purpose

- The IAIS has sought closer relations with the FATF by applying for observer status in the FATF, submitted comments on the Consultation Paper regarding the review of the FATF Recommendations and attended meetings of the FATF working group on the review of the Recommendations. By participating in the review, the IAIS wants to ensure that FATF Recommendations accurately reflect the unique nature of the insurance business.
- IAIS representatives attended meetings to discuss the AML/CFT Methodology.
- The IAIS is drafting Insurance Core Principles on AML/CFT as part of the ICP revision.

[5] Available at http://www.iosco.org/resolutions/index.html.

After completion of the new FATF Recommendations the IAIS intends to review its “Anti-Money Laundering Guidance Notes for Insurance Supervisors & Insurance Entities”.

Securities

In May 2002, IOSCO adopted a Multilateral Memorandum of Understanding concerning Consultation, Cooperation and the Exchange of Information that will facilitate exchanges of information relating to cross-border securities violations. This multilateral MOU builds on the many previously existing IOSCO Resolutions and Principles to establish an international benchmark for cooperation and information sharing. This MOU will enable signatories to cooperate rapidly and effectively in the fight against cross-border financial fraud. The process adopted for the implementation of the MOU provides incentives for members to raise their respective national standards regarding information sharing.

In 2002, IOSCO established a Task Force on Client Identification and Beneficial Ownership in order survey the regulatory framework of members with a view to assessing the level of related vulnerabilities of securities markets to money laundering activities and to providing as much regulatory guidance as possible. The Task Force will take into account the revisions of the FATF 40 + 8 Recommendations. IOSCO is actively monitoring the ongoing work of the FATF.