PRINCIPLES ON CLIENT IDENTIFICATION AND BENEFICIAL OWNERSHIP FOR THE SECURITIES INDUSTRY

THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

MAY 2004

PRINCIPLES ON CLIENT IDENTIFICATION AND BENEFICIAL OWNERSHIP FOR THE SECURITIES INDUSTRY

I. INTRODUCTION

Client and beneficial owner identification and verification, know your client, as well as the keeping of the related data are considered the Client Due Diligence process (CDD process). The CDD process is a key component of securities regulatory requirements intended to achieve the principal objectives of securities regulation, the protection of investors; ensuring that markets are fair, efficient and transparent; and the prevention of the illegal use of the securities industry. These objectives must be taken into account to their broadest extent when implementing requirements relating to the CDD process. From the perspective of securities regulators, the CDD process must be carried out by authorized securities service providers[1] (ASSPs), to fulfill client and beneficial owner identification and verification, as well as know your client requirements.

In light of other international organizations' recent work, including the Financial Action Task Force (FATF), the International Organization of Securities Commissions (IOSCO) established a Task Force on Client Identification and Beneficial Ownership (the Task Force), in October 2002, to study existing securities regulatory regimes relating to the identification of clients and beneficial owners and to develop principles that address aspects of the CDD process. The CDD process is one of the long-standing pillars of securities regulation and industry practice.

The Task Force's survey of existing regimes of member jurisdictions found that, while there are different regulatory approaches to client and beneficial owner identification among IOSCO members due to differences in legal and regulatory frameworks, there are certain common features. These include requirements that compel ASSPs to: identify their clients and beneficial owners; obtain adequate information about their clients' circumstances and investment objectives; as well as maintain records of this data.

Although some of the main objectives of these principles are to prevent securities fraud and market abuse, the application of the CDD process in the securities industry also contributes to the pursuit of other policy goals related to the prevention of the illegal use of the securities industry such as money laundering and the financing of terrorism that are generally within the competence of other authorities.

An effective CDD process can help deter and detect violations of securities laws, codes, provisions and regulations, and reduce the risk of the illegal use of the securities industry; IOSCO members share these common objectives.

[1] ASSPs are regulated entities that perform securities transactions, e.g.: broker-dealers; mutual funds/collective investment schemes; futures firms; introducing brokers and certain investment advisors; securities firms; commodity pools; commodity pool operators; etc.

The principles described below should guide securities regulators and can also serve as an important parameter for ASSPs.

Each principle is accompanied by a general discussion explaining its importance and goals, followed by a series of recommended actions. These are broad descriptions of results and outcomes that government and non-government authorities, self-regulatory organizations (SROs), and ASSPs, should seek to achieve in the implementation of each principle.

Consequently, neither the principles nor the recommended actions describing how the principles are given effect, are designed themselves to serve as regulations, rules, specific codes of conduct or internal firm rules. Rather, the outcomes underlying the principles and measures should be considered in adopting regulations, rules or codes of conduct in ways that take into account how a particular market or legal system functions.

While these principles recognize that ASSPs may apply the CDD process to their clients and beneficial owners on a risk sensitive basis, the ASSPs should establish the bases for such risk determinations and should be able to justify their assessments to their regulator.

II. PRINCIPLES

CLIENT IDENTIFICATION AND VERIFICATION

Principle 1: Authorized Securities Service Providers, when establishing a business relationship with a client, should identify and verify the client's identity using reliable, independent source documents, data or other information.

Client identification and verification facilitates the prevention, detection and prosecution of the illegal use of the securities sector. Effective client identification and verification procedures are necessary to protect investors and to maintain the integrity of the markets.

ASSPs client identification and verification procedures should be documented and should provide a reasonable basis for the ASSP to believe that the true identity of each client will be adequately known.

ASSPs should have client acceptance policies. They must identify the clients before or when establishing a business relationship (this is when a client's account is opened or a client is granted authority to conduct transactions with respect to an account), and verify their identity as soon as possible, before or after the business relationship has been established, for purposes of assuming that the risks are effectively managed. In this regard, it is essential not to interrupt the normal conduct of business.

This flexibility must be exercised in a reasonable manner, given that verifications should occur as soon as is reasonably practicable after the client has been identified, in order to avoid illegal activities while verification is pending.

ASSP also should adopt risk management procedures to monitor accounts while client identity is being verified, taking into account the conditions under which a client may utilize the business relationship prior to verification of identity.

In the case of existing clients, ASSPs should apply the CDD process to them when there is a suspicion of illegal activity and/or when the ASSP has doubts about the veracity or adequacy of the previously obtained client identification data.

While ASSPs may identify and verify the identity of their clients on a risk sensitive basis, they should establish the criteria for such risk determinations and should be able to justify such criteria to their regulator.

Where the risk of illegal securities activity is lower, where information on the identity of the client is publicly available or where adequate checks and controls exist elsewhere in national systems, it is reasonable to permit ASSPs to apply simplified or reduced measures when identifying and verifying the identity of the client. Examples of clients where simplified or reduced client identification measures could be applied include:

- Financial institutions, that are subject to requirements consistent with these principles and are supervised for compliance with those requirements.
- Public companies that are subject to regulatory disclosure requirements.
- Government entities or enterprises.

Where the risk of misidentification or illegal securities activity is higher, an ASSP should apply more stringent client identification measures. Examples of higher risk categories of accounts could include, depending on the circumstances, the following:

- Accounts for politically exposed persons.
- Accounts for entities with complex corporate structures.
- Accounts for nationals from countries that are considered as non-cooperative or inadequately-regulated.
- Accounts for residents from countries that are considered as non-cooperative or inadequately-regulated.
- Accounts for ASSPs operating in countries considered as non-cooperative or inadequately-regulated.
- Accounts for unregistered or unregulated investment vehicles.
- Cross-border omnibus accounts for certain investment vehicles, including highly leveraged institutions (e.g. hedge funds).

ASSP, should determine which parties involved in a trust need to be identified and verified taking into account the features of its legal system, the type of service to be provided and the type of client. This should be done on a risk-based approach.

If a jurisdiction's legal system does not recognize the trust as a legal vehicle, the ASSPs should apply identification and verification procedures to the foreign parties to the trust (trustee, settlor and beneficiary), following a risk-based approach.

Recommended Actions:

- ASSPs should not keep anonymous accounts, or accounts held under fictitious names.

- ASSPs should have a written policy describing in general terms, the CDD process it follows. This policy should be approved by senior management.

- The measures that are to be taken by ASSPs should be consistent with any guidelines issued by the securities regulator, other competent authorities or SROs.

- When opening an account, a written contract should be executed before services are provided, if possible.

- Specific CDD procedures based on the type of client on a risk-based approach considering, for example: i) natural persons; ii) legal persons; iii) nationals; and iv) foreigners.

- Client identification and verification processes should be properly documented in each case.

- ASSPs may rely on documents as well as on non-documentary methods, or a combination of both, in order to identify clients and verify their identity.

  A. With respect to natural persons, reliable methods, could include, the following:

     - An unexpired government-issued identification evidencing nationality or residence and bearing a photograph or other similar safeguards, such as a driver's license or passport.
     - Independently verifying the client's identity through the comparison of information provided by the client with information from a consumer reporting agency, public database, or other source.
     - Checking references with other financial institutions.
     - Obtaining account statements.
     - Face to face meetings; interviews; statements; home visits; references from previous business relationships.

  B. With respect to non-natural persons, reliable methods could include the following:

     - Obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the client's name, the names of trustees, legal form, address, directors, and documents evidencing the power of a person to bind the legal person or arrangement.
     - Forming an understanding of the ownership and control structure.
     - Identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and management of the legal person or arrangement.

  All documents required should be reliable and should come from a source independent from the client.

OMNIBUS ACCOUNTS

Principle 1a: Authorized Securities Service Providers should have specific Client Due Diligence policies for omnibus accounts.

Omnibus accounts are accounts established by and in the name of financial institutions in order to engage in securities transactions on behalf of their clients. When establishing an omnibus account, an ASSPs should conduct identification and verification of their client -the other financial institution-, through procedures consistent with Principle 1.[2]

When the client establishing the omnibus account is a domestic financial institution, subject to a regulatory and oversight regime that is comparable to the regime applicable to the ASSP, the risk of illegal activity is lower. The application of simplified or reduced

[2] Because the other financial institution is the ASSP's client, the ASSP is not "relying" upon the other financial institution to conduct due diligence of the financial institution's clients as that term is used in Principle 5, below. Therefore, the ASSP will not be required to "drill down" through the financial institution to identify and verify all of the financial institution's clients.

identification and verification procedures in relation to such accounts may be appropriate. However, when the client establishing the omnibus account is a foreign financial institution, the risks associated with the account in some circumstances may be considered to be potentially higher, and enhanced procedures may be appropriate.

Recommended Actions:

- ASSPs should apply enhanced CDD process in relation to omnibus accounts maintained for foreign financial institutions. These enhanced procedures include the following:

  - Gathering sufficient information regarding the other financial institution to understand its business and to determine from publicly available information its professional reputation.

  - Assessing the adequacy of the financial institution's CDD process.

  - Determining whether the financial institution has a physical presence in the jurisdiction in which it is incorporated, with the understanding that the ASSP should not establish or maintain an omnibus account for a financial institution that neither has a physical presence in that jurisdiction nor is affiliated with a regulated financial group that has such a presence.

  - Assessing the regulatory and oversight regime of the country in which the other financial institution is located to determine whether the client is subject to sufficient CDD standards.

  - Obtaining approval of senior management before establishing new omnibus account relationships.

  - Documenting the respective responsibilities of each institution.

BENEFICIAL OWNER IDENTIFICATION

> ***Principle 2: Authorized Securities Service Providers should obtain sufficient information, in order to identify persons who beneficially own or control securities accounts.***

Whenever it is apparent that securities acquired or maintained through an account are beneficially owned by a party other than the client,[3] that party should be identified using client identification and verification procedures established in accordance with the criteria

[3] The beneficial owner is defined as the natural person or persons who ultimately own, control [or influence] a client and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement (see definition FATF Forty Recommendations – 20 June 2003).

set out in Principle 1 and 1a, following a risk-based approach, so the ASSP has reasonable grounds to believe that the true identity of the beneficial owner is known.

When establishing a business relationship, all clients should be required to specify whether they are acting for their own account or for the account of another party or parties (beneficial owners and representatives). ASSPs should take reasonable measures to identify and verify the beneficial owner(s) of client accounts, including reasonable measures to understand the ownership and control structure of clients that are non-natural persons.

Recommended Actions

- ASSPs should take steps to identify the beneficial owner of legal vehicles under a risk-based approach. Legal vehicles include:
  - Corporate structures.
  - Partnerships.
  - Companies that issue shares in bearer form.
  - Unregistered or unregulated investment vehicles.
  - Highly leveraged institutions.
  - Joint ventures.
  - Mandates.
  - Trusts.

- ASSPs should identify and verify the beneficial owner(s) of legal vehicles.

- The client should certify to the ASSP, the existence and identity of those persons who exercise ultimate effective control over a legal person or arrangement (e.g., shareholders; company management; control group; etc.)

- Upfront disclosure by the client to the ASSPs.

- ASSPs should obtain copies of the legal documents (if applicable), that evidence the existence and good standing of the legal vehicle.

- Where the client or the owner of the controlling interest is a listed company or a regulated or registered investment vehicle, such as a collective investment scheme, mutual fund or commodity pool, that is subject to adequate regulatory disclosure requirements, it is not necessary to seek to identify and verify the identity of any shareholder, participant or unit holder of that entity.

KNOW YOUR CLIENT (KYC)

> ***Principle 3: Authorized Securities Service Providers should obtain from each client information about the client circumstances and investment objectives relevant to the services to be provided and should conduct ongoing due diligence regarding the client's accounts.***

ASSPs should obtain information about their clients' circumstances, including financial background and business objectives in order to develop the client's profile which will serve as the basis to establish the KYC. This information is expected to be provided by the client in order to start building its records, which will serve to determine the client's risk profile. Additionally, with such information, the ASSP can ensure both that the client has received adequate risk disclosure, and that the ASSP has a sufficient basis for meaningful due diligence of the business relationship.

ASSPs should also conduct the KYC process from the moment a business relationship is established and on an ongoing basis thereafter. ASSPs should scrutinize transactions undertaken throughout the course of those relationships to ensure that the transactions being conducted are consistent with the institution's knowledge of its clients, the client's business and risk profile, taking into account, where necessary, the client's source of funds. Where the activities of an ASSP include providing investment advice, it is of particular importance that this advice takes into consideration a proper understanding of the needs and circumstances of the client.

Recommended Actions:

- ASSPs should implement the KYC procedure on each of its clients to ensure that transactions performed are consistent with the ASSPs' knowledge of the client, the client's business and risk profile, including, and where necessary, the source of funds.

- ASSPs providing investment advice should ensure that the advice is suitable based on a proper understanding of the needs and circumstances for the client. Information that ASSPs could obtain includes: personal references; types of transactions anticipated; source of the funds; current estimated annual income and net worth; previous investment experience; investment objectives; previous experience with other ASSPs; etc.

- ASSPs should establish clear written policies to determine clients and activities are to be considered as low or high risk.

- Among the risk factors that an ASSP may consider are the following:
  - Non-face-to-face clients.
  - Politically exposed persons (PEPs).
  - Corporate vehicles.
  - Origin of resources.
  - Type of activities undertaken by the client.
  - Public reputation.
  - Country of residence of the client.

- In order to fulfill the KYC assessment, ASSPs should comply with the following: i) obtain relevant information of the client in order to be able to establish its profile; ii) classify the client and its expected transactions as low or high risk; iii) analyze and verify the transactions undertaken by the client and if they are considered as low or high risk; iv) analyze if the client's transactions are in accordance with their profile.

RECORD KEEPING

Principle 4: Authorized Securities Service Providers should keep records on the Client Due Diligence process for at least five years after the business relationship is ended.

Keeping appropriate records is fundamental. Records must have sufficient content, context and structure to provide evidence of the clients' and beneficial owners' identities and the pattern of the client's business activities, including all transaction records.

Records should remain available, for at least five years after the business relationship has been terminated, in good condition and in useable form. They should be preserved and protected from accidental or intended damage or destruction and unauthorized access.

Recommended Actions:

- ASSPs should establish clear written policies and procedures to ensure the integrity, security, availability, reliability, confidentiality and thoroughness of all CDD data, as well as appropriate recovery and backup procedures.

- ASSPs should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for investigations and the prosecution of criminal, civil and administrative proceedings.

- ASSPs should ensure that third parties have special consideration for record keeping related to trusts. ASSPs' senior management should approve record keeping policies that allow for an efficient retrieval of CDD data of the clients of trusts, when relying on third parties.

THIRD PARTY RELIANCE

Principle 5: Authorized Securities Service Providers may use reliable third parties to meet their Client Due Diligence obligations, provided that the requirements under these principles are met.

Reliable third parties can comprise a wide array of regulated financial entities. In this case, the ultimate responsibility/liability regarding the CDD data remains with the ASSP.[4]

[4] The CDD obligations do not include the requirement in some jurisdictions that an ASSP perform an assessment as to the suitability of investment advice the ASSP provides to its clients based on its clients' circumstances an investment objectives. For those jurisdictions, the duty to ensure the suitability of investment advice is not necessarily included in the concept of "Third Party Reliance."

ASSPs should have timely access to the CDD data maintained by third parties, whether the third parties are foreign or domestic.

Recommended Actions:

- ASSPs should determine whether it is reasonable to rely on a third party.
- ASSPs should determine whether it is reasonable to rely on a third party to apply a CDD process and the ASSP and the third party should establish their respective responsibilities in writing. For these purposes, clear policies should be established in order to determine an acceptable level of reliability on that third party.
- ASSPs should take adequate steps to satisfy themselves that CDD data will be made available from the third party upon request without delay.
- ASSPs should satisfy themselves on reasonable grounds, that the third party is regulated and supervised for, and has sufficient and adequate mechanisms in place to comply with CDD requirements consistent with these principles.
- ASSPs should not rely on third parties based in jurisdictions considered as high risk, non-cooperative or inadequately-regulated with respect to CDD.
- ASSPs' senior management should specially review arrangements by which the ASSP may gain effective access to CDD data maintained by the third party.
- An outsourcing or agency relationship is not included in the concept of "Third Party Reliance." If an ASSP outsources part of its CDD process to an independent service provider, the ASSP remains solely responsible for assuring compliance with CDD requirements and must monitor the operation of the outsourced CDD process, assess its effectiveness and ensure that its regulator are able to obtain all information and records relating to the outsourced CDD process.

UNSUCCESSFUL CDD PROCESS

> ***Principle 6: Authorized Securities Service Providers should establish clear written policies to determine what actions are to be taken in the event the Client Due Diligence process cannot be successfully completed or when illegal activities are suspected.***

ASSPs should establish clear written policies regarding how they will proceed regarding clients and/or transactions in which the CDD process cannot be properly completed within the time frame established or it is suspected that an illegal use of the markets may occur (or has occurred).[5] These policies should include the filling of reports in accordance with the existing regulation in each jurisdiction.

[5] As examples of failures in the CDD process, we can mention the following: i) the client refuses to provide information and/or means of proof for his identification; ii) the information provided is false or inconsistent;

Recommended Actions

- If an ASSP does not accept a new account and/or to establish a business relationship due to CDD failures, it could consider making a report to the competent authorities, specifying the attempt and denial of the service to that person.

- ASSPs should, when appropriate, apply expedited mechanisms when the CDD process cannot be performed or when illegal activities are suspected, such as: i) halting transactions; ii) closing of the account; iii) reporting to the competent authorities; iv) freezing of assets and accounts upon the authorities request; etc.

ROLE OF THE REGULATOR

> ***Principle 7: The regulator should have adequate powers in order to establish the preconditions needed to implement these principles. It should also have adequate powers to monitor and ensure compliance by Authorized Securities Service Providers with Client Due Diligence obligations and to require information identifying persons who beneficially own or control securities accounts.***

The regulator should have adequate powers and the authority to adopt regulations to impose CDD requirements reflecting these principles. No domestic secrecy laws, regulations, codes or provisions should prevent or restrict the collection of the information and records by the regulator.

The regulator should have adequate powers to monitor and ensure compliance by ASSPs with the CDD process. Additionally, the regulator should have authority to conduct inspections and be empowered to obtain, and if necessary to compel production of any information from ASSPs, that is relevant to monitoring such compliance. Additionally, the regulator should have authority to impose adequate administrative sanctions on ASSPs for failure to comply with such requirements. Adequate training for both, the regulator and the ASSP, is essential for these purposes.

The regulator should have the power to require information identifying persons who beneficially own or control accounts. The regulator should have the power to obtain identification records and CDD information on a timely basis.

Recommended Actions:

- Regulators should ensure the existence of adequate provisions, regulations, codes or guidelines on Client Due Diligence process.

---

iii) the clients try to hide the nature of its businesses and transactions; iv) the third party does not comply with certain requirements; etc.

- If the regulator does not bear the primary responsibility for enforcing the CDD process, an SRO or another competent authority should ensure the existence of these processes among their members and its corresponding implementation, in accordance with the applicable provisions, rules and/or codes of conduct. The regulator in such jurisdictions where SROs or another competent authority exist should have regulatory oversight over such matters.

- ASSPs should be responsible and subject to liability for inadequate implementation processes.

- Regular training should be provided for employees of both, regulator and the ASSPs, to enhance their capabilities relating to CDD process.

COOPERATION

> ***Principle 8: The regulator should seek cooperation with other jurisdictions by sharing client due diligence information directly with other foreign regulators or indirectly through other authorities.***

The regulator should assess the legislative framework in its own jurisdiction to determine whether it has the necessary authority to cooperate and share information with other foreign regulators and to the extent necessary, should work with the appropriate domestic authorities to identify and remove any impediment to such cooperation.[6]

IOSCO members, should take steps to adhere to the IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (May 2002) (IOSCO MMOU) and should cooperate with their foreign counterparts to the full extent contemplated by the IOSCO MMOU.

Regulators also are encouraged to enter into Memoranda of Understanding with other regulators or other formal or informal information sharing arrangements, as needed, with those authorities that are not IOSCO members or IOSCO MMOU signatories, in order to ensure that the exchange of information and international cooperation would be successfully implemented.

The regulator should seek to have the powers to request from other domestic authorities and government agencies in its jurisdiction any information and documentation necessary to respond to requests from its foreign counterparts.

Recommended Actions:

- Regulators should have powers to obtain and to share CDD information with its foreign counterparts, when the information be legally requested.

[6] A Resolution on Principles for Record Keeping, Collection of Information, Enforcement Powers and Mutual Cooperation to Improve the Enforcement of Securities and Futures Laws Passed by the Presidents' Committee (November 1997).

- Regulators should seek to establish or implement mechanisms for the exchange of CDD information.

- Regulators should seek to ensure that no domestic secrecy laws, regulations or provisions prevent the collection or provision of client identification information.[7]

- Regulators should establish controls and safeguards to ensure that client due diligence information received from foreign regulators is used only in an authorized manner, consistent with requirements concerning privacy and data protection.

[7] Report on the Self-Evaluations Conducted by IOSCO Members pursuant to the 1994 IOSCO Resolution on "Commitment to Basic IOSCO Principles of High Regulatory Standards and Mutual Cooperation and Assistance."