Bangko Sentral ng Pilipinas

MAYNILA, PILIPINAS

MEMORANDUM

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION & EXAMINATION SECTOR

October 1, 2002

MEMORANDUM TO: **ALL BANKS & NON-BANK FINANCIAL INTERMEDIARIES PERFORMING QUASI-BANKING FUNCTIONS (NBQBs)**

For the guidance of all concerned, attached is a paper on Customer Due Diligence For Banks issued by the Basel Committee on Banking Supervision which paper highlights the Know-Your-Customer (KYC) standards to be observed in the design of KYC programs best suited for your purposes.

The essential elements should start from risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. Nonetheless, it is important that the requirements do not become so restrictive that they deny access to banking services, especially for people who are financially or socially disadvantaged.

In our review of your KYC programs, the guidelines herein indicated should be adopted and shall be used as basis of our assessment of your anti-money laundering programs. It is understood that transactions of your Trust departments shall be subject to the same or similar KYC standards.

ALBERTO V. REYES
Deputy Governor

Attch.: a/s

CUSTOMER DUE DILIGENCE FOR BANKS AND NON-BANK FINANCIAL INTERMEDIARIES PERFORMING QUASI-BANKING FUNCTIONS (NBQBS)

1. Customer acceptance policy

Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are unacceptable to bank management. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for high risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance, where as quite extensive due diligence may be deemed essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with high risk customers, such as potentates (see below), should be taken exclusively at senior management level.

2. Customer identification

Customer identification is an essential element of KYC standards. A customer is defined as any person or entity that keeps an account with a bank and any person or entity on whose behalf an account is maintained, as well as the beneficiaries of transactions conducted by professional financial intermediaries. Specifically, a customer should include an account-holder and the beneficial owner of an account. A customer should also include the beneficiary of a trust, an investment fund, a pension fund or a company whose assets are managed by an asset manager, or the grantor of a trust.

Banks should establish a systematic procedure for verifying the identity of new customers and should never enter a business relationship until the identity of a new customer is satisfactorily established. Banks should "document and enforce policies for identification of customers and those acting on their behalf".[1] The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

---

[1] Core Principles Methodology, Essential Criterion 2.

The customer identification process applies naturally at the outset of the relationship, but there is also a need to apply KYC standards to existing customer accounts. Where such standards have been introduced only recently and do not as yet apply fully to existing customers, a risk assessment exercise can be undertaken and priority given to obtaining necessary information, where it is deficient, in respect of the higher risk cases. An appropriate time to review the information available on existing customers is when a transaction of significance takes place, or when there is a material change in the way that the account is operated. However, if a bank is aware that it lacks sufficient information about an existing high-risk customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. In addition, the supervisor needs to set an appropriate target date for completion of a KYC review and regularisation of all existing accounts. In any event, a bank should undertake regular reviews of its customer base to establish that it has up-to-date information and a proper understanding of its account holders' identity and of their business.

Banks that offer private banking services are particularly exposed to reputational risk. Private banking by nature involves a large measure of confidentiality. Private banking accounts can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. In no circumstances should private banking operations function autonomously, or as a "bank within a bank"[2], and no part of the bank should ever escape the required procedures. This means that all new clients and new accounts should be approved by at least one person other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

2.1 General identification requirements

Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. National supervisors are encourage to provide guidance to assist banks in their designing their own identification procedures. Examples of the type of information that would be appropriate are set out in Annex 1.

[2] Some banks insulate their private banking functions or create Chinese walls as a means of providing additional protection for customer confidentiality.

Banks should apply their full KYC procedures to applicants that plan to transfer an opening balance from another financial institution, bearing in mind that the previous account manager may have asked for the account to be removed because of a concern about dubious activities.

Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or "bearer" status or who gives a fictitious name. Nor should confidential numbered[3] accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies (IBCs), may make proper identification of customers or beneficial owners difficult. A bank should take all steps necessary to satisfy itself that it knows the true identity of the ultimate owner of all such entities.

2.2 Specific identification issues

There are a number of more detailed issues relating to customer identification which need to be addressed. Particular comments are invited on the issues mentioned in this section. Several of these are currently under consideration by the FATF as part of a general review of its forty recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, nominee and fiduciary accounts or client accounts opened by professional intermediaries

Trust, nominee and fiduciary accounts can be used to avoid customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that

[3] In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

the true relationship is understood. Banks should establish whether the customer is acting on behalf of another person as trustee, nominee or professional intermediary (e.g. a lawyer or an accountant). If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place.

Banks may hold "pooled" accounts (e.g. client accounts managed by law firms) or accounts opened on behalf of pooled entities, such as mutual funds and money managers. In such cases, banks have to decide, given the circumstances, whether the customer is the intermediary, or whether it would be more appropriate to look through the intermediary to the ultimate beneficial owners. In each case, the identity of the customer that is subject to due diligence should be clearly established. The beneficial owners should be verified where possible. Where not, the banks should perform due diligence on the intermediary and establish to its complete satisfaction that the intermediary has a sound due diligence process for each of its clients.

Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all companies needs to be obtained.

The above procedures may prove difficult for banks in some countries to follow. In the case of professional intermediaries such as lawyers, there might exist professional codes of conduct preventing the dissemination of information concerning their clients. The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients. The Working Group has therefore not taken a definitive position on this issue.

2.2.2 Introduced business

The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility

of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

The FATF is currently engaged in a review of the appropriateness of eligible introducers, i.e. whether they should be confined to reputable banks only or should extend to other regulated institutions, whether a bank should establish a contractual relationship with its introducers and whether it is appropriate to rely on a third party introducer at all. The Working Group is still developing its thinking on this topic.

2.2.3 Potentate risk

Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such persons are commonly referred to as "potentates". There is always a possibility that they may abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

Accepting and managing funds from corrupt potentates will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes. Indeed, some countries have recently amended or are in the process of amending their laws and regulations to criminalise active corruption of foreign civil servants and public officers in accordance with the relevant international convention.[4] In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations

[4] See OECD Convention on combating Bribery of Foreign Public Officials in International Business Transactions, adopted by Negotiating Conference on 21 November 1997.

apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for banks considering a relationship with a potentate to identify that person as well as people and companies that are clearly related to the potentates.

2.2.4 Non-face-to-face customers

Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent advent of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of non-face-to-face customers is being discussed by FATF, and is also the subject of a draft EC Directive, and the topic therefore remains subject to review by the Working Group.

A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The anonymous and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.[5]

[5] The Electronic Banking Group of the Basel Committee is currently developing guiding principles for the prudent risk management of electronic banking activities and will specifically outline appropriate supervisory expectations regarding the approaches banks should take in identifying, assessing, managing and controlling the risks associated with electronic banking. These principles will also include guidance on how to authenticate and identify customers in an electronic banking context.

3. On-going monitoring of high risk accounts

On-going monitoring of accounts and transactions is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The on-going monitoring process includes the following:

- Banks should develop "clear standards on what records must be kept on customer identification and individual transactions and the retention period".[6] As the starting point and natural follow-up of the identification process, banks should obtain and keep up to date customer identification papers and retain them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

- Senior management of a bank in charge of private banking business should know the personal circumstances of the bank's large/important customers and be alert to sources of third party information. Every bank should draw its own distinction between large/important customers and others, and set threshold indicators for them accordingly, taking into account the country of origin and other risk factors. Significant transactions by high-risk customers should be approved by a senior manager.

- Banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to be possibility that the customer is conducting undesirable activities. They may include transactions that do not make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal

[6] Core Principles Methodology, Essential Criterion 2

and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. A list of suspicious activities drawn up by supervisors can be very helpful to banks.

- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with potentates and high profile individuals or with persons and companies that are clearly related to or associated with them.[7]

4. Risk management

Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Banks should appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local supervisory practice. Banks should have clear written procedures, communicated to all personnel, for staff to report suspicious transactions to a specified senior manager. That manager must then assess whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and supervisory authorities.

All banks must have an ongoing employee-training programme so that bank staff is adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the customer identity for new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff is reminded of their responsibilities and is kept informed of new developments. It is crucial that all relevant staff fully understand the

[7] It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations etc. It should however be noted that potentates (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, masking the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.

need for and implement KYC policies consistently. A culture within banks that promotes such understanding is the key to successful implementation.

Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures. Management should ensure that audit functions are staffed adequately with individuals who are well-versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

***

Annex 1

General identification requirements

This annex presents a suggested list of identification requirements for personal customers and corporates. National supervisors are encouraged to provide guidance to assist banks in designing their own identification procedures.

Personal customers

For personal customers, banks need to obtain the following information:

name and/or names used,

permanent residential address,

date and place of birth,

name of employer or nature of self-employment/business

specimen signature, and

source of funds.

Additional information would relate to nationality or country of origin, public or high profile position, etc. Banks should verify the information against original documents of identity issued by an official authority (examples including identity cards and passports). Such documents should be those that are most difficult to obtain illicitly. In countries where new customers do not possess the prime identity documents, eg, identity cards, passports or driving licences, some flexibility may be required. However, particular care should be taken in accepting documents that are easily forged or which can be easily obtained in false identities. Where there is face to face contact, the appearance should be verified against an official document bearing a photograph. Any subsequent changes to the above information should also be recorded and verified.

Corporate and other business customers

For corporate and other business customers, banks should obtain evidence of their legal status, such as an incorporation document, partnership agreement, association documents or a business licence. For large corporate accounts, a financial statement of the business or a description of the customer's principal line of business should also be obtained. In addition, if significant changes to the company structure or ownership occur subsequently, further checks should be made. In all cases, banks need to verify that the corporation or business entity exists and engages in its stated business. The original documents or certified copies of certificates should be produced for verification.