ANTI-MONEY LAUNDERING
MODEL OPERATING MANUAL
For
BANKS AND OTHER COVERED INSTITUTIONS
GUIDELINES ON MEASURES AGAINST MONEY LAUNDERING

Introduction

The international drive against serious crimes, especially drug trafficking and terrorism, had led to an obligation on banks and other financial institutions to do whatever they can to avoid transactions which assist criminals in laundering the proceeds of their crime. Banks and Non-bank Financial Institutions under the supervising and regulation of the Bangko Sentral ng Pilipinas must support this drive and assist the authorities in identifying potential money laundering transactions. These guidelines are therefore, adopted to support governments, law enforcement agencies and international bodies such as the Financial Action Task Force in their efforts to combat the use of the financial system for the laundering of the proceeds of crime. While the country’s anti-money laundering law (R.A. No. 9160) was already enacted, the law on the secrecy of bank deposits remains stringent, however. Hence, in implementing procedures related to money laundering, care should be taken that laws are not violated. These guidelines are set to ensure compliance with the Anti-Money Laundering Law and its implementing rules and regulations, as well as other applicable regulations without violating other relevant laws and without losing bona-fide business/clients in the process. The guidelines are intended to help this process and to ensure high standards in the following areas:

- Establishing the identity of new individual customers.
- Identifying the true owners when opening new accounts for companies/corporations.
- Identifying the principal of an agent.
- Producing and retaining identification and transaction records.
- Reporting suspicious transactions to the competent authorities.
- Enhancing relationships with the authorities.
- Preventive procedures, training, pre-employment screening and internal controls.

It should be emphasized that the procedures being introduced in each of these areas are intended to be complementary to existing operating procedures and to the requirements of laws and regulations.

It should be noted that in some countries, for example U.S.A., Australia and Canada, the law requires procedures additional to those set out in these
guidelines. For example, in the U.S.A. certain transactions of $10K or more must be reported and recent legislation requires that, inter alia, a log must be kept of sales of instruments, such as money orders and travelers cheques, of $3K or more. Where the law is more stringent than these guidelines then obviously the law, must prevail.

The Guidelines consist of principles in bold type followed by explanatory notes. There are also twelve Appendices. These are:-

Appendix B - Guidance material on the nature of money laundering.
Appendix C - List of relevant international organizations.
Appendix D - List of examples of suspicious transactions.
Appendix E - Note on the scope of necessary training.
Appendix F - Glossary
Appendix G - Internal Form for reporting suspicious transactions
Appendix G-1 - Money Laundering Suspicion-Evaluation Record
Appendix H - Form for reporting suspicious transactions to the Anti-Money Laundering Council
Appendix I - R.A. No. 9160
Appendix J - BSP Circular No. 251 dated July 7, 2000
Appendix K - BSP Circular No. 253 dated July 31, 2000
Appendix L - BSP Circular No. 302 dated October 11, 2001
Appendix M - FATF Forty Recommendation

**Principles**

1. When establishing a business relationship or conducting a single transaction the identity of the customer must be established based on official or other reliable identifying documents.

2. Business units must not keep anonymous accounts or accounts in obviously fictitious names.

3. Where a customer is not clearly acting on his own behalf, reasonable measures should be taken to obtain information about the true identity of the principal.

4. Business units must keep records of customer identification for at least five years after the account is closed. These documents should be available to the competent authorities as allowed by law.

5. To enable compliance with requests for information from competent authorities business units must retain records of all transactions. As a minimum, account ledger entries and the records supporting them must be kept for five years.
6. Covered transactions, as defined under R.A. No. 9160, otherwise known as the Anti-Money Laundering Act of 2001 shall be reported to the Anti-Money Laundering Council (AMLC) within five (5) working days from the date of the transaction or from the date the concerned institution gained/acquired information/knowledge that the transaction is a covered transaction.

7. Business units should give special attention to business relations and transactions with persons, companies, and financial institutions from countries which do not apply sufficient controls against money laundering. For example those countries which are not members of the Financial Action Task Force (See Appendix A). Whenever these transactions have no apparent economic or visible lawful purpose or where the transaction is unusually large, their background and purpose should, as far as possible, be established, recorded in writing, and reported to the AMLC if said transaction (s) falls under the definition of a covered transaction.

8. Business units must not warn their customers when information relating to them is being reported to the competent authorities.

9. When a business unit reports its suspicions to the competent authorities it must comply with their instructions, as provided or allowed by law.

10. When a business unit develops strong suspicions about operations of a customer, this should be reported immediately to the Head of Investigations and to the Head of Compliance. A copy of the report should be given to the Head of Operations of the reporting unit.

11. The programme against money laundering based on these guidelines, should include:-

- the development of internal controls, policies and procedures;

- adequate screening procedures to ensure high standards when recruiting employees;

- an on-going employee training programme; and

- an internal control function to test the system.

**GUIDELINES**

1. The identity of a customer with whom a covered institution is entering into a business relationship or conducting a single transaction must be established from official or other reliable
**identifying documents.**

A business relationship is defined as an arrangement to carry out transactions on a frequent or regular basis. The Basle principles and local regulations require financial institutions to do all they can to determine the true identity of all customers using their services. Accordingly, business units should obtain evidence of identification from new customers. In particular, care should be taken to identify the ownership of all accounts, portfolios and funds and the identity of those using safe-custody facilities at the time when the relationship is established. Transactions should not be conducted with customers who fail to provide adequate evidence of their identity. This applies to single transactions relating to fund transfers, foreign exchange, money market or wholesale deposits, safe deposit boxes and large amounts of cash by non account holders as well as to longer banking and investment relationships.

Account opening procedures should normally include:-

- personal presence of the account holder.
- scrutiny of original identification documents.
- completion of a standard account opening form.
- verifications of any photographs.
- comparison of signatures with live signatures.

For banking business the standard account opening form should be completed personally by the prospective customer. Where the account holder cannot be personally present because he is abroad, or otherwise unavailable, the account should be treated with caution and steps taken in the longer term to correct the position. Meanwhile, any covered transaction should be reported to the competent authority. (See principle 6). Copies of documents should be retained in accordance with Principle 4.

The identifying documents should provide evidence of true name or names used, permanent address, date of birth and nationality. Identifying documents should preferably include at least one bearing a photograph and preferably be pre-signed. The identifying documents which are considered to be most reliable are official identity cards and passports. Identification documents that are easily obtained in any name e.g. medical cards, credit cards and student identification cards should not be accepted as sole means of identification. Where the authenticity of an identification document is in doubt, no transaction should be conducted unless the transaction is approved by a bank officer with authorities to do so. Normal banking and business prudence in conducting any transaction should prevail.
A good form of verification of identity is personal introduction by a known and respected customer, enquiries will need to be made to verify identity. The customer may also be asked to provide a reference from another financial institution and, if other identification enquiries are not satisfactory, it should be verified. For prospective customers who are normally resident in another country, and where satisfactory verification of identity cannot be obtained locally, identification procedures should proceed to verification by a branch or another financial institution. A branch or business unit, which instructs another business unit to conduct transactions on behalf of account holders, is responsible for ensuring that identification and "know your customer" procedures have been followed. This will apply particularly when the instruction emanates from an overseas branch.

The following minimum information/documents shall be obtained from individual customers:

(1) Name;
(2) Present address;
(3) Permanent address;
(4) Date and place of birth;
(5) Nationality;
(6) Nature of work and name of employer or nature of self-employment/business;
(7) Specimen signature; and
(8) Source of funds (s)

**Company Accounts**

Before establishing business relationships, covered institutions shall endeavor to ensure that the customer that is a corporate or juridical entity has not been or is not in the process of being, dissolved, wound up or voided, or that its business or operations has not been or is not in the process of being, closed, shut down, phased out, or terminated. Dealings with shell companies and corporations, which have no business substance in their own right but through which financial transactions may be conducted, should be undertaken with extreme caution. The following minimum information/documents shall be obtained from customers that are corporate or juridical entities:

(1) Articles of Incorporation/Partnership;
(2) By-laws;
(3) Official address or principal business address;
(4) List of directors/partners;
(5) List of principal stockholders owning at least two percent (2%) of the capital stock;
(6) Beneficial owners, if any; and
(7) Verification of the authority and identification of the person purporting to act on behalf of the client.

The nature of the company's business should be recorded. Where the person who opens the account is not the person who will be operating the account, the latter should be identified and checks conducted as for an individual account holder. Where there is any doubt, the certificate of registration should be verified.

Where the company is registered abroad, documents comparable to those above should be examined. Where the overseas company is not a known customer, all company documents should be verified. All signatories to the account must be properly identified.

**Treatment of Dormant Accounts**

Sometimes bank accounts which have been dormant for many years are activated for fraudulent or other criminal purposes. Where a dormant account becomes active it should be reviewed to ensure that the identification procedures have been followed and can still be relied upon. In case of doubt new account identification procedures should be instituted.

**Transactions Undertaken for Non-Account Holders**

Transactions undertaken for non-account holders demand special care and vigilance. Where the transaction involves significant amounts, the customer should be asked to produce positive evidence of identity including nationality, if the customer is not a Filipino. File copies of the identification documents should be retained. Identification documents should be treated as part of transaction records and should be retained and retrievable. Funds deposited by non-account holders into an existing account should be handled with particular care.

**Overseas Resident Corporate Investors**

For corporate customers the identity of directors and shareholders of the company should be sought. This should extend as far as practicable to identifying those ultimately interested in the ownership and control of the company. Evidence of the relationship between the individual introducing the company, the individual giving instructions on its behalf and that individual's authority to represent the company should be sought and retained. These principles are similar to those mentioned under paragraph headed "Company Accounts".
2. **Business units must not keep anonymous accounts or accounts in obviously fictitious names.**

Anonymous accounts and accounts under fictitious names should not be accepted. The Bangko Sentral prohibits the use of fictitious or anonymous accounts.

3. **Where a customer is not clearly acting on his own behalf business units must take reasonable measures to obtain information about the true identity of his principal.**

This type of account includes accounts opened by lawyers, accountants and financial institutions conducting affairs on behalf of their clients. It is an area of concern since money launderers will exploit the difficulty in establishing the identity of beneficiaries behind trusts and companies. The concern applies particularly to institutions, corporations, foundations and trusts that do not conduct any commercial or manufacturing business in the country where their registered office is located.

Verification of identity procedures, under principle 1, should be conducted in respect of all parties to the account. If satisfactory evidence of identity is not readily available the counterparty should be informed that the account cannot be operated without the provision of full evidence of identity of the parties.

When an account is opened for a trust, any written authority to open the account should be examined and the identity of the trustees should be verified.

Where a company is in liquidation or in receivership the identification procedures should be followed as far as possible and a copy of a letter of appointment, or similar document, should be seen and copied.

Similar checks should be conducted for non-incorporated bodies. Identity checks on partners who are authorized to operate a partnership account should be conducted as if they were individual customers.

4. **Business units must keep records of customer identification for at least five years after the account is closed.**

When an account is opened, photocopies should be made of the documents used to establish the identity of the account holder. These should be retained in the account file, together with other account opening forms.

At least, the record should include full name, address, date of birth, nationality, and occupation, or nature of business.
5. Business units must retain records of all transactions. As a minimum, account ledger entries and the records supporting them must be kept for five years.

All records relating to the account must be retained for five years. If the account or a covered transaction involving the account is under investigation, all relevant records shall be retained, even after five years, until after the investigation is completed. Retention may be by way of original documents, disc, photocopies or microfiche. It should be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved) to provide, if necessary, evidence for prosecution of relevant criminal behaviour. The records to be retained will, of course, depend on the nature of the transaction, as follows:-

(a) **Cash Deposits.**

   Generally, require:
   
   • paying-in slip or credit voucher showing account name, number and amount;
   
   • daily posting register showing account number and amount;
   
   • ledger entry.

(b) **Cash Transfers.**

   Generally, require:
   
   • debit voucher (cheque or authority to debit) showing name, account number and signature, or ATM transaction record showing account number, amount and time;
   
   • payment or posting register, showing cheque number, amount and account number;
   
   • ledger entry.

(c) **A foreign exchange transaction with account holder.**

   Requires the customer or account name, the amount, the currency purchased or sold and the exchange rate. When an account is being debited or credited, the normal debit/credit vouchers and entries apply. If a remittance is involved, copies of application to purchase/remit foreign exchange and record of remittances should be kept.
(d) **A foreign exchange transaction with a non-account holder.**

This requires names, addresses and signatures in addition to the currency and exchange rate. Identification of purchaser/remitter and application to purchase/remit foreign exchange with the record of remittance, if remittance is involved.

(e) **The sale of negotiable instrument for cash.**

The minimum requirement for non-account holders should be a purchase form or instruction on which the customer records his full name, address and amount.

Any contentious correspondence should be retained for a much longer time, until the issue is finally resolved.

6. **If the business units suspect that funds stem from relevant criminal activity they must promptly report their suspicions to their Head of Operations and to the Compliance Officer (with staff reporting to their branch manager or superior officer) and record the circumstances in writing.**

**Recognition of Suspicious Transactions**

As the type of transactions which may be used by a money launderer is almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for the type of account. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that the transaction, or series of transactions, is unusual. Accordingly procedures should be in place so that activity on account is monitored by staff who are familiar with those accounts. This day to day monitoring is made easier if the identification of suspicious transactions can be automated.

Examples of circumstances where funds might stem from drug-trafficking, terrorism and other serious crimes are shown in Appendix C.

What might appear to be suspicious or to constitute unusual activity on the account of a particular customer in the eyes of staff at one branch may be explicable by reference to the conduct of the same customer's account at another branch. Thus, it is important that suspicions reported by branches are reviewed centrally at the main office. Where transactions are conducted by a business unit (e.g. Treasury) not holding all the customer or account information, special vigilance is required. When a doubt arises about a specific transaction further
information about the customer should be sought from the branch holding the 
customer records.

When a suspicious transaction is rejected for commercial reasons, a record 
should be maintained.

Each branch should require each staff who deals directly with accounts and 
customers to report any suspicion to the branch manager (or to the staff's 
superior officer) using the form in Appendix G. The Branch Manager (or superior 
officer) should review/evaluate such suspicion of money laundering using the 
form in Appendix G-1. Where the Branch Manager (or the superior officer) is 
satisfied that the suspicion is reasonable he should report it immediately to the 
Head of Operations of the business unit and to the Compliance Officer by 
forwarding to them the completed report forms shown in Appendix G and G-1. It
is, of course, important that, as far as possible, normal business relations with 
account holders are maintained.

7. Business units should give special attention to business relations 
and transactions with persons, companies, and financial institutions 
from countries which do not apply sufficient controls against money 
laundering. Whenever these transactions have no apparent 
economic or visible lawful purpose, their background and purpose 
should, as far as possible, be established, recorded in writing, and 
be reported to the Branch Manager or to the staff's superior officer, 
who will report to the Head of Operations and to the Compliance 
Officer if, in his evaluation, the staff's suspicion is reasonably 
justified.

Where there is public information that particular countries or institutions have 
weak controls against money laundering then business units should regard 
themselves as being on notice to be cautious in handling transactions with them.

8. Business units must not warn their customers when information 
relating to them is being reported to the competent authorities.

Covered institutions should co-operate with authorities throughout the world in 
tackling money laundering. Therefore, customers should not be warned when a 
report on covered transactions is made to competent authorities. Moreover, in 
the event of the authorities regarding the account or transaction as bona-fide, 
relationship with the customer will not then have been damaged unnecessarily.

In some countries, for example the UK, it is a criminal offense to inform the 
customer, or any party, that a report has been made to the authorities.
9. When a business unit reports its suspicions it must comply with lawful instructions from the competent authorities.

Since the authority will often require time to investigate the reported suspicion, it should be expected to issue a lawful instruction on how the account should be handled. Usually, authorities will request that a normal account relationship should be maintained so that the customer does not become aware of official enquiries.

Where transactions have been reported the relevant records should be retained until the issue is finally concluded.

The competent authorities should be asked to provide feedback to the business unit about the result of investigations. This will facilitate a better understanding by employees of circumstances which might properly be considered suspicious.

10. When a business unit develops strong suspicions about operations of a customer, the circumstances should be reported through the usual process, to business Head of Operations and Compliance Officer and to higher officer or body, if applicable.

All suspicions about the operations of a customer, should be reported through the usual process, to the Head of Operations of the business unit and to the Compliance Officer and to higher officer or body, if applicable.

LAW AND REGULATIONS

Following are the applicable law and rules and regulations on Money Laundering:

a. R.A. 9160 - Appendix I
b. BSP Circular No. 251 dated July 7, 2000 - Appendix J
c. BSP No. 302 Dated October 11, 2001 - Appendix K

REPORTING PROCEDURE

1. All covered transactions should be reported by the staff to the Branch Manager or to the staff's superior officer using the form in Appendix G. Upon receipt of the report (Appendix G) the Branch Manager (or superior officer) will evaluate the report using Appendix G-1. If the Branch Manager (or the staff's superior officer) is of the opinion that there is/are reasonable basis for the suspicion, he/she should forward the report form G and G-1 to the Head of Operations of the business unit and to the Compliance Officer.
2. Upon receipt of a report on suspicion on Money Laundering (Appendix G and G-1), the Compliance Officer should convene a meeting of the Committee on Money Laundering composed of the (1) Compliance Officer, (2) The Head of Service Delivery - C&IB and Treasury, (3) The Head of Operations - Consumer Banking, to evaluate the report and determine if the suspicion is based on reasonable grounds.

3. If the Money Laundering Committee decides that there is reasonable basis for considering a covered transaction, or other illegal activity, a report will be made to the Anti-Money Laundering Council using a report form shown in Appendix H, to be signed by the Division Head of the function making the report. A copy of the report to the Central Bank should be given immediately to other members of the Management Committee (Mancom).

4. If applicable, covered transaction or other illegal activity should also be reported to the Regional Head of Investigations. The report may be in narrative form containing all information considered significant. The report should be made by the local Head of Investigation, if there is one, who should be given a copy of the report to the Anti-Money Laundering Council by the Committee on Money Laundering. If there is no local Head of Investigations, the report to the Regional Head of Investigations should be made by the Compliance Officer.

5. R.A. No. 9160 defined/specified covered transactions to be reported to the AMLC (Appendix I).
Appendix A

FINANCIAL ACTION TASK FORCE MEMBER COUNTRIES

Australia
Austria
Belgium
Canada
China
Denmark
European Commission
Finland
France
Germany
Greece
Gulf Co-operation Council
Hong Kong
Iceland
Ireland
Italy
Japan
Luxembourg
Netherlands
New Zealand
Norway
Portugal
Singapore
Spain
Sweden
Switzerland
Turkey
United Kingdom
United States
GUIDELINES ON MEASURES AGAINST MONEY LAUNDERING

The nature of Money Laundering

Money laundering may be briefly defined as the conversion or transfer of money to disguise its illicit origin. In many countries, it is already a criminal offense to be knowingly involved in money laundering and other countries have pending legislation. The involvement will include any intentional or negligent act by financial institutions and their employees that assist drug traffickers and other criminals to conceal or transfer the proceeds of their crimes or to build up funds with which to finance crime.

It is estimated that 80% of world drug trafficking revenue (about US$500 billion per year) is subsequently laundered. Money obtained from drug trafficking usually starts in the form of a large volume of cash in mixed denomination notes. This volume is often larger than the volume of the drugs themselves. The trafficker needs cash with as little risk as possible and it is easier if the cash is in a hard currency. Clearly, the stage of depositing cash in a financial institution is the critical one for the money launderer. Deposits may often be made in the name of a company whose beneficial owners do not have to be disclosed in its country of incorporation or elsewhere. Deposits are also made into accounts in the name of trustees where the beneficiaries are kept secret. Sometimes, these deposits are made by the legal profession where the rules of legal confidentiality may be exploited. Deposits of cash are sometimes achieved by using false identities. Criminals also utilize informal banking systems such as "Hawalla bankers" who conduct an international exchange of gold bullion, gold jewelry or currency. Such cash deposits would tend to go to jurisdictions where the banking system is insufficiently regulated and where "letter box" companies are permitted. These jurisdictions include small countries who derive a source of revenue from the sale of banking licenses or who create tax havens. As a result, the proceeds of criminal acts will often be transferred to a financial institution in an insufficiently regulated" off-shore" jurisdiction and then transferred back to a well regulated regime in the form of a loan or an investment in property.

Stages in Money Laundering

There are three stages of money laundering during which there may be numerous transactions made by launderers that could alert a financial institution to criminal activity:
(a) Placement - the physical disposal of cash proceeds derived from illegal activity.

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

(c) Integration - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

**Abuse of the Investment Industry in the Money Laundering Process**

Because investment business is not generally cash based, it is probably less at risk from the initial placement of criminally derived funds than mainstream banking. Most payments are made by way of cheque from another financial institution and it can therefore be assumed that the first stage of money laundering has already been achieved. Nevertheless, the purchase of investments for cash is not unknown and therefore the risk of investment business being used at the placement stage cannot be ignored.

However, investment business is arguably more at risk from the second stage of money laundering i.e. the layering process. Unlike laundering via the mainstream banking networks, investment business allows the launderer to change the form of funds, not just from cash in hand to cash on deposit but from money in whatever from to an entirely different asset or range of assets as many times as required. Investments that are cash equivalent i.e. bearer bonds and similar investments in which ownership can be evidenced without reference to registration of identity may be particularly attractive as vehicle for laundering money.

Investment transactions incorporate an added attraction to the launderer in that the alternative asset is normally highly liquid. The ability to liquidate investment portfolios containing both lawful and illicit proceeds, whilst concealing the criminal source of the latter, combined with the huge variety of investments available, and the ease of transfer between them, offers the sophisticated criminal launderer an ideal route to effective integration into the legitimate economy.
Money Laundering Schemes Uncovered

Drug investigations are sometimes initiated by an alert teller who observes unusual activity related to cash deposits. The following recent UK cases are illustrations.

A teller had observed that a non-customer occasionally remitted money to Peru for collection by his brother. Subsequently, the man opened an account and regularly deposited approximately GBP5,000 in cash which he claimed derived from his business as a fruit importer. The bank reported the circumstances to the authorities and the police conducted an investigation which led to the discovery of a cocaine refining laboratory in England. Approximately 30 Kgs of cocaine was seized, other bank accounts were discovered and GBP1.5M was confiscated.

A man opened an account with a UK bank and deposited GBP50K in cash, subsequently requesting that it be transferred to a company account held at the bank’s Guernsey subsidiary. The bank was suspicious and made discreet enquiries of the customer who claimed that the money was the proceeds of the sale of a boat. Following a request for a money to be transferred to a different company account in Guernsey, the bank reported the proposed transaction to the authorities who discovered connections with drug trafficking in Spain. Two men were subsequently arrested and respectively received 14 years and 61/2 years imprisonment. Nearly GBP400K was seized.

A teller noticed that a Dutch non-customer had visited the branch on several occasions exchanging in all GBP14K of cash into Dutch currency. This was regarded as suspicious because it was known that the man had an account at another branch nearby. The circumstances were reported to the authorities and the man was subsequently arrested for importing cannabis.

A joint account through which, for several years, only small transactions were conducted received several cash deposits amounting to GBP52K. The deposits were unexplained and inconsistent with the humble character of the account holders. The circumstances were reported to the police and investigations revealed a conspiracy to supply heroine and cocaine.

Money launderers also set up or buy corporations in off-shore jurisdictions using nominee directors who open local bank accounts. The corporation will then make deposits of cash to finance loans to other ostensibly unconnected companies in larger states.
Another well used technique of money laundering is to under value or over value goods imported or exported so as to illicitly transfer value to hard currency countries. This may be achieved by false invoicing.

The most common form of money laundering that insurance companies, brokers, and independent financial advisers will encounter takes the form of a proposal to enter into a single premium contract. Examples of the type of contract that are particularly attractive as a vehicle for laundering money are:

- investment bonds;
- purchased annuities;
- lump sum top-ups to an existing life insurance contract; and lump sum contributions to personal pensions contracts.

As in the example below, these contracts in themselves may be merely one part of a sophisticated web of complex transactions which will often have their origins elsewhere in the financial services sector.

Recently in the UK, money laundering involving insurance business was uncovered where cash derived from drug trafficking was deposited in several bank accounts and then transferred to an offshore account. The trafficker entered into a GBP50,000 life insurance contract, having been introduced by a broking firm. Payments was made by two separate transfers from the offshore account. It was supported that the funds used for payment were the proceeds of overseas investments. At the time of the trafficker's arrest, the insurer had received instructions for the early surrender of the contract.

Group employees will thus need to give special attention to deposits of cash or other unusual transactions which might fit into one of the techniques outlined above.
Appendix C

GUIDELINES ON MEASURES AGAINST MONEY LAUNDERING

These guidelines take into account the findings of a number of public bodies who have considered money laundering. These are the following:

(a) **The 1988 United Nations Vienna Convention Against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances** which, inter alia, proposed improvements in laws and administrative procedures relating to financial institutions. It created an obligation to criminalise money laundering and set forth the principle that banking secrecy should not interfere with criminal investigations.

(b) **The Basle Committee on Banking Regulations and Supervisory Practices** which in December 1988 set out principles to avoid the financial system becoming a conduit for criminal funds. It stated that banks should:

   i. make reasonable efforts to determine the customer's true identity and bona fides;

   ii. ensure that business is conducted in conformity with high ethical standards and, that service is not provided where there is good reason to suppose that transactions are associated with laundering activities;

   iii. co-operate fully with national law enforcement agencies including where there are reasonable grounds for suspecting money laundering taking appropriate measures which are consistent with the law; and

   iv. adopt policies consistent with the Statement's principles and implement procedures for customer identification and retention of internal records of transactions.

(c) **The Financial Action Task Force on Money Laundering** set up following the G7 Paris Summit in July 1989. It has made 40 detailed recommendations for further action by countries, competent authorities and financial institutions. There are now 26 countries in the Task Force.

(d) **The UK Joint Money Laundering Working Group**, set up by the Bank of England with the BBA, the building societies, the police and H.M. Customs and Excise. The Group was established as a result of the Home Affairs
Committee report on Drug Trafficking and Related Serious Crime and the G7 Task Force. Its terms of reference include “To agree recommendations on money laundering to be put to HMG”. It produced, in December 1990, Money Laundering Guidance Notes for Banks and Building Societies and in 1991 similar separate guidance notes for insurance and investment business. The guidance notes have since been revised to reflect the EC Directive on Money Laundering and have been issued in 3 separate editions namely:

i. Guidance Notes for Mainstream Banking, Lending and Deposit Taking Activities;

ii. Guidance Notes for Wholesale, Institutional and Private Client Investment Business; and

iii. Guidance Notes for Insurance and Retail Investment Products.

They require U.K. registered financial institutions to issue a clear statement of policies relating to money laundering and to alert their overseas branches and subsidiaries to those policies.

(e) EC Directive on Prevention of the use of the Financial System for the Purpose of Money Laundering

The EC Directive on Money Laundering which is applicable to a broad range of financial sector activity recognizes the risk to the stability of, and confidence in, the financial system if money launderers take advantage of the freedom to supply financial services which a single integrated market will afford. It directs member states to combat money laundering and, in particular, the laundering of proceeds derived from drug trafficking.

Financial institutions are required to identify customers by means of suitable evidence and keep records of the evidence in addition to records of individual transactions. Member States are also required to introduce a mandatory suspicions-based reporting regime and all credit and financial institutions are required to train staff and establish proper internal procedures to deal with money laundering.
GUIDELINES ON MEASURES AGAINST MONEY LAUNDERING

Examples of Suspicious Transactions

A suspicious transaction can be described as any activity which is out of character with the usual running of an account which could relate to the laundering of proceeds of a serious crime such as the following.

Cash Transactions

Large cash deposits made by an individual or company whose ostensible business activities should not normally generate substantial amounts of cash.

The frequent deposit of cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.

Frequent exchange of cash into other currencies.

Substantial increases in cash deposits by an account holder without apparent cause, especially if such deposits are soon transferred out of the account and/or to a destination not normally associated with that customer.

The deposit of cash by means of numerous credits slips so that the total of each deposit is unremarkable but the total of all the credits is large.

Customers who open numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

Company accounts whose transactions, both deposits and withdrawals, are dominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.)

The Use of Accounts

Any individual or company whose accounts shows virtually no normal personal banking or business related activities but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business.
Customers who wish to maintain a number of trustee or clients' accounts which do not appear consistent with type of business, and transactions which involve nominee names.

Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the bank to verify.

Matching of Payments out with credits paid in by cash on the same or previous day.

Paying in large third party cheques endorsed in favour of the customer.

Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

Increased use of deposit facilities. The deposit and withdrawal of sealed packets.

Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts especially if the deposits are promptly transferred between other client company and trust accounts.

Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

Customers who appear to have accounts with several other financial institutions within the same locality, especially when there is a regular consolidation process from such accounts prior to a request for onward transmission of the funds elsewhere.

Customers who pay or deposit cash to cover requests for bankers drafts, money transfer or other negotiable and readily marketable money instruments.

Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

Customers who make regular and large payments that cannot clearly be identified as bona fide transactions to, or who receive regular and large payments from countries which are associated with terrorist activity or with the production, processing or marketing narcotics.
Money Laundering Using Investment Related Transactions

Sales and Dealing Staff

New Business

Although longstanding customers may be laundering money through an investment business, it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies or even companies organized as a front. Investment may be direct with an investment business or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

- A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.

- A client with no discernible reason for using the firm's service of your business e.g. clients with distant addresses who could find the same service nearer their home base;

- Clients whose requirements are not in the normal pattern of the firms’ business which could be more easily serviced elsewhere.

- An investor introduced by an overseas bank, affiliate or other investor both of which are based in countries where production of drugs or drug trafficking may be prevalent.

- Any transaction in which the counterparty to the transaction is unknown.

- A Corporate/Trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise there are a number of legitimate reasons for dealing via intermediaries on a "numbered account" basis; however this is also a useful tactic which may be used by the money launderer to delay, obscure or avoid detection.
Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiries.

Dealing Patterns & Abnormal Transactions

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Longstanding and apparently legitimate customer accounts may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

Dealing Patterns

• A large number of investment transactions across a number of jurisdictions.

• Transactions not in keeping with the investor’s normal activity, the financial markets in which the investor is active and the business which the investor operates.

• Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client’s request.

• Bearer securities held outside a recognized custodial system.

Abnormal Transactions

• A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.

• Any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.

• Transfer of investments to apparently unrelated third parties.

• Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.
• Other transactions linked to the transaction in question which could be designed to disguise money and divert it into other forms or other destinations or beneficiaries.

**Settlements**

**Payments**

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of methods. Cash settlement through a financial adviser may not in itself be suspicious; however large or unusual settlements of securities, deals in cash and settlements in cash to a large securities house will usually provide cause to further inquiry. Examples of unusual payment settlement may be as follows:

• A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction.

• Large transaction settlement by cash.

Payment by way of third party cheque or money transfer where there is a variation between the account holder, the signatory and the prospective investor, must give rise to additional enquiries.

**Delivery**

Bearer securities, held outside a recognized custodial system, are extremely portable and anonymous instruments which may serve the purpose of the money launderer well. Their presentation in settlement or as collateral should therefore always prompt further enquiry as should the following:

• Settlement to be made by way of bearer securities from outside a recognized clearing system.

• Allotment letters for new issues in the name of persons other than the client.

**Disposition**

• Payment to a third party without any apparent connection with the investor.

• Settlement either by registration or delivery of securities to be made to an unverified third party.

• Abnormal settlement instructions including payment to apparently unconnected parties.
**Money Laundering Involving off-Shore Activity**

Customer introduced by an overseas branch, affiliate or other bank based in countries where drug trafficking is rife.

Use of letters of credit or other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

Regular large wire transfer transactions to tax haven countries.

Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

Frequent requests for travellers cheques or foreign currency drafts to be issued.

**Money Laundering Involving Lending**

Request to borrow against assets held by the bank or a third party, where the origin of the assets is not known or is inconsistent with the customer's trading.

Request by a customer to provide or arrange finance where the source of the customer's financial contribution to the deal is unclear, particularly where property is involved.
Appendix E

GUIDELINES ON MEASURES AGAINST MONEY LAUNDERING

Scope of Training

The effectiveness of procedures must depend on the extent to which staff appreciate the serious nature of the background issues and their own personal obligations under any legislation. They must be encouraged to provide prompt advise of covered transactions. It is, therefore, important that appropriate training measures are provided.

The following training should be undertaken:

(a) New Employees

Training to provide a general appreciation of the background to money laundering, and the subsequent need for reporting of any covered transaction to the appropriate designated point. This should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on monitoring accounts, on the reporting of the suspicions, of legal requirements to report, and of the importance of these issues.

(b) Front Line Staff

Training members of staff who are dealing directly with the public and who are the first point of contract with potential money-launderers. They should be made aware of the reporting system. Training should be provided on the factors that may give rise to suspicion and on the procedures to be adopted when a covered transaction is suspected.

Staff should be made aware of the vigilance required in dealing with non-regular customers particularly where large cash transactions are involved.

(c) Account Opening/New Client Personnel

Employees who deal with account opening, or accepts new clients, should receive the training given to cashiers. In addition, the need to verify the identity of the customer must be understood, and training should be given in account opening and customer/client identity verification procedures. Such employees should be aware that the offer of suspicious funds or the request to undertake a covered transaction should be reported to the
relevant authorities whether or not the funds are accepted or the
transactions proceed.

(d) Investment Business Processing Staff

Those members of staff who process the settlement of investment must
receive appropriate training in the processing and verification procedures.
The identity of the investor and matching against cheque received in
settlement is, for instance a key process. Such staff should be made
aware that the offer of suspicious funds accompanying a request to
undertake investment business may need to be reported to the proper
parties whether or not the funds are accepted or the transaction proceeds.

(e) Sales/Advisory Staff

Members of staff who are dealing directly with the public (whether as
members of staff or financial advisers) are the first point of contact with
potential money-launderers and their efforts are therefore vital to the
organization’s strategy in the fight against money laundering. They must
be made aware of their responsibilities and should be made aware of the
organization’s reporting system for such transactions. Training should be
provided on factors that may give rise to suspicions and on the procedures
to be adopted when a transaction is deemed to be suspicious.

(f) Supervisors and Managers

A high level of instruction covering all aspects of money laundering
procedures should be provided to supervisors and managers. This should
include internal reporting procedures, requirements for verification and
retention of records.

(g) On-going Training

It will also be necessary to make arrangements for refresher training at
regular intervals.
## Appendix F

### GUIDELINES ON MEASURES AGAINST MONEY LAUNDERING

#### Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money laundering</td>
<td>The conversion or transfer of property for the purpose of disguising its illicit origin.</td>
</tr>
<tr>
<td>Suspicion of money laundering</td>
<td>Impression given by a set of circumstances that customer activity is possibly connected with money laundering.</td>
</tr>
<tr>
<td>Relevant criminal activity</td>
<td>Refers to any acts or omission or series or combination thereof involving or having relation to the following:</td>
</tr>
<tr>
<td></td>
<td>a. Kidnapping for ransom under Article 267 of Act No. 3815, the Revised Penal Code, as amended;</td>
</tr>
<tr>
<td></td>
<td>b. Robbery and extortion under Articles 294,295,296,299,300,301 and 302 of the same Code;</td>
</tr>
<tr>
<td></td>
<td>c. Qualified theft under Article 310 of the same Code;</td>
</tr>
<tr>
<td></td>
<td>d. Swindling under Article 315 of the same Code;</td>
</tr>
<tr>
<td></td>
<td>e. Piracy on the high seas under the same Code and Presidential Decree (P.D.) No. 532;</td>
</tr>
<tr>
<td></td>
<td>f. Destructive arson and murder as defined under the same Code and hijacking and other violations under Republic Act (R.A.) No. 6235,</td>
</tr>
<tr>
<td></td>
<td>including those perpetrated by terrorists against non-combatant persons and similar targets;</td>
</tr>
<tr>
<td></td>
<td>g. Jueteng and Masiao punished as illegal gambling under P.D. No. 1602;</td>
</tr>
<tr>
<td></td>
<td>h. Smuggling under R.A Nos. 455 and 1937;</td>
</tr>
</tbody>
</table>
i. Section 3, paragraphs B,C,E,G,H and I of R.A. No. 3019, the Anti-Graph and Corrupt Practices Act, as amended;

j. Section 3,4,5,6,7,8 and 9 of Article Two of R.A. No. 6425, the Dangerous Drugs Act of 1972 as amended;

k. Plunder under R.A. No. 7080, as amended;

l. Violations under R.A. No. 8792, the Electronic Commerce Act of 2000;

m. Fraudulent practices and other violations under R.A. No. 8799, the Securities Regulation Code of 2000;

and

n. Felonies of offenses of a similar nature that are punishable under the penal laws of other countries.

Competent authority

Designated officer, Local, Regional or Group Head of Investigations, the Compliance Officer, Bangko Sentral ng Pilipinas, The Anti-Money Laundering Council.
Appendix G

Name of Institution

REPORTING STAFF:
Name………………………………………
Tel…………………………………………..
Branch/Dept .................................
Position ........................................

CUSTOMER/CLIENT:
Name  Occupation/Employer or Business
Address  Account No.
Contact/Tel  Type of Account
Passport No  Account Balance
Other ID  As at date

INFORMATION/SUSPICION
Information/Transaction:
  Date of Transaction:
  Nature of Transaction:

Reason for suspicion

REPORTING STAFF’S SIGNATURE…………………………….. Date………………..
( You should not advise the customer/client or anyone else of your suspicion and report.)

Notes: Attach copies of the following documents:
  • account opening Form
  • Customer’s identification documents or certificates of incorporation/registration
  • Documents supporting suspicion
Appendix G-1

(Name of Institution)
MONEY LAUNDERING SUSPICION
EVALUATION RECORD

Date
Customer/Client

Evaluated by
Branch/Dept

ENQUIRIES UNDERTAKEN

DOCUMENTS RESEARCHED/ATTACHED

DETERMINATION/DECISION

__________________________
SIGNATURE
### Appendix H

<table>
<thead>
<tr>
<th>(NAME OF INSTITUTION)</th>
</tr>
</thead>
<tbody>
<tr>
<td>REPORT ON SUSPICIOUS TRANSACTIONS</td>
</tr>
<tr>
<td>Name of Office/Address</td>
</tr>
<tr>
<td>Nature and Brief Description of the Transaction</td>
</tr>
<tr>
<td>Other Relevant Information</td>
</tr>
</tbody>
</table>

Signature of Authorized Officer
Over Printed Name