BANK OF PALESTINE LTD.

Anti-Money Laundering Manual

BANK OF PALESTINE LTD.
Anti-Money Laundering Manual

INDEX

BANK OF PALESTINE LTD.
ANTI-MONEY LAUNDERING MANUAL

1. Introduction

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities by using the financial system to make payments and transfer funds from one account to the other The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, have both enhanced the ease with which criminal money can be laundered and complicated the tracing process.

The bank, as provider of a wide range of money transmission and lending services, are vulnerable to being used in the layering and integration stages of money laundering as well as at the placement stage.

Criminals have responded to the measures taken by the financial sector over recent years by recognizing that cash payments made into financial sector businesses can often give rise to additional enquiries. Other means have therefore been sought to convert the illegally earned cash or to mix it with legitimate cash earnings before it enters the financial system. Thus making it harder to detect at the placement stage. In more sophisticated crimes. Where cash is not involved. BoP should consider the money laundering risks posed by its products and services offered. And devise appropriate procedures to address each of the relevant risks.

The purpose of this manual is to establish clear responsibilities and accountabilities to ensure that anti-money laundering policies, procedures, and controls are introduced and maintained by each branch within the bank. These policies and procedures should aim to deter criminals from using the Banks' facilities for money laundering. Thus ensuring that they comply with their obligations under the law.

1.1 Risks posed by various business segments of a bank:

Trade Finance
Some organizations, possibly under the disguise of front companies and nominees, create large scale but false international trading activities in order to move their illicit monies from one country to another. They create the illusion of international trade using false or inflated invoices to generate apparently legitimate international wire transfers. And use falsified or bogus letters of credit to confuse the trail further. Many of the front companies may even approach BoP for credit to fund the business activity.

Investment Banking:
The liquidity of many investment products particularly attracts sophisticated money launderers since it allows them to move their money quickly and easily, from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy. Investment businesses are also able to transfer monies across borders quickly and efficiently, complex and sophisticated investment products that are constantly being introduced.

Retail Banking:
Although it may not appear obvious that retail investment products might be used for money laundering purposes. Vigilance is necessary throughout the retail-banking network to ensure that personal banking products and services are not exploited.

Transactions through Intermediaries:
Intermediaries and product providers who deal directly with the public may be used at the initial placement stage of money laundering particularly if they receive cash Retail investment products. Are however, more likely to be used at the layering and integration stages. The liquidity of a branch trust may attract money launderers since it allows them to move their money, swiftly and without difficulty, from one product to another. Mixing lawful and illicit proceeds.

1.2 Impact on the financial system
The use of the financial system in the above manner is a matter of serious concern, not only for the law enforcement agencies, but also for the banks' managements, as public confidence in banks, and hence their stability, may be undermined through their association with criminals. In addition, banks may suffer direct losses from fraud, either through negligence in screening undesirable customers or where the integrity of their own officers has been undermined through their connection with criminals.

1.3 Control Mechanisms

The Basle Committee on Banking Regulations and Supervisory Practices has issued guidelines protecting banks from being used as a channel for money laundering. The Committee encourages all banks to establish effective policies and procedures. It encourages ethical standards of professional conduct amongst banks and financial institutions and ensures that co-operation with law enforcement agencies is achieved in stepping up vigilance and suppressing money laundering through the banking system.

1.4 Internal Reporting Procedures:

BoP is strongly committed to fully complying with the Basel Committee guidelines and all applicable regulations issued in the Palestinian Authority Territories.

The BoP operations cover the entire spectrum of banking activities. The requirements outlined in the manual are not intended to replace the regulations. These are merely intended to supplement existing regulations.

In general, all branches of the bank should ensure compliance with existing regulations. If there is any conflict between regulations and the requirements stipulated in the manual. The more conservative requirement should be followed. Where the manual makes reference to requirements, which are not addressed by PNA regulators. The manual's requirements should be adhered to. In case of any doubt on any procedure, the branch should obtain clarification from the Bank Compliance Officer (BCO).

The branch should update the BCO of the name, telephone number and e-mail address (if any)), of their respective Money Laundering Prevention Officers (MLPO).

1.4.1 Role of the Bank Compliance Officer

The broad role of the BCO is outlined as follows:

- Providing explanations/clarifications to branches on the procedures set out in this manual:
- Performing an overall assessment of the effectiveness of procedures and the adherence to the procedures by the branches:
- Reviewing all "suspicious" transactions reported to him/her in Suspicious Transactions Reports filed by various branches and updating senior management and the Bank Audit Committee of significant issues.
- He is the principal liaison officer between the bank and the Palestine Monetary Authority (PMA) and law enforcement agencies on all money laundering related issues.

1.4.2 Role of the Money Laundering Prevention Officer:

- Each branch should appoint a MLPO. This individual has to shoulder a very high degree of responsibility should therefore be at a sufficiently senior level in the management hierarchy. It is important that the position of the MLPO is such that management hierarchy. It is important that there is a clear reporting chain under which suspicious transactions will be reported to the MLPO without delay. (S) he should be the central point of contact with the BCO. Additionally.

1.4.3 Reporting Procedures

- Each Branch should follow the procedures for reviewing transactions, and produce Exception Reports suited to its business activities and based on the risks inherent in the transactions it enters into.

- Reviews should include a detailed examination of the transaction patterns and volumes through the customer' account(s) in the same name or accounts operated by related parties. Consideration should be given to the length of the business relationship, and reference should be made to identification records held. For example, all large cash deposits" should be scrutinized and explained. It is not sufficient to state that the funds were transferred from XYZ bank or that the customer inherited his/her wealth a detailed description of the source of the deposits and a written account of the customer's different sources of wealth and income is required. The definition of "Large cash deposits" may vary from one customer to another. However all branches must set a "large cash deposit" greater than US $ 10.000 equivalent. Should advise the BCO of the higher limit and the reasons for setting such a limit. Care should be taken not to restrict the review not only to cash activity or current and savings accounts. The coverage should include all transactions with customers including letters of credit and investment accounts.

- Review of Exception Reports and of customer accounts will be carried out within the Operations department. Any transactions that appear questionable should be brought to the attention of the branch manager in a memorandum. The branch manager should evaluate the questionable transactions. And if necessary should obtain written clarification from the Relationship Officer of the account (s) in question.

- The General Manager (GM) and the MLPO should be copied on the memorandum and a copy placed on the customer file for follow up. The MLPO should acknowledge receipt of the memorandum and simultaneously.

Provide a reminder of the obligation to do nothing that might prejudice enquiries. i.e. "tipping off". All internal enquires made in relation to the memorandum. And the rationale for disclosure / non-disclosure to the authorities should be documented. Care should be taken to guard against a report being submitted as a matter of routine to external regulatory authorities without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

- The Account Officer should send a written response to the HOO, and copied to the GM and to the MLPO. The response should explain the background and reasons for the unusual activity. The HOO should evaluate the response and record his recommendations in another memorandum addressed to the MLPO and copied the GM. The MLPO should evaluate all the information and determine whether the transaction(s) is/are reportable. Once the money laundering suspicions are confirmed, the MLPO should take appropriate steps to close the concerned customer's account unless the account is allowed to remain open with the express approval of the GM (see Verification Procedures).

- The guidelines regarding the suspicious or reportable transaction of The Palestine Monetary Authority (PMA) must be adhered to. Any transactions, which are considered, can be suspicious by the MLPO or which are reported to the PMA should be advised with all reverent details to the BCO at the Head Office using the Suspicious Transactions Report (Exhibit 3).
- If. As a result of an investigation into the Bank's activities by PMA, any suspicious activity is brought to the attention of the MLPO such transactions should be reported to the BCO in an official memorandum.
- On-going communication between the MLOP and the HOO is important. At the end of an investigation, the MLPO and the GM should advise all members of staff concerned of the outcome. It the particularly important that the HOO is Kept informed of all communication between the investigation officer and the MLPO at all stages of the investigation.
- Record keeping procedures are outlined in Section 5.

2. Stages in Money Laundering

There are three basic in the stages in the money laundering process. Each stage may comprise numerous transactions by launderers that could alert a financial institution to criminal activity:

2.1 Placement – the physical disposal of initial proceeds derived from an illegal activity. This gets "dirty" cash into the system.

Examples:

- Cash paid into banks (sometimes with staff complicity or mixed with the proceeds of legitimate business).
- Cash exported.
- Cash used to buy high value goods, property, investments or business assets.

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

Examples:
- Money transaction abroad (often using shell companies or funds disguised as the proceeds of a legitimate business).
- Cash deposited in overseas banking systems.
- Resale of goods and assets>

2.3 Integration – the placing of laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

Examples:
- False loan repayments or forged invoices used as cover for laundered money.
- A complex web of transfers (domestic and international) makes tracing the original source of funds virtually impossible.
- Income from property or legitimate business assets.

These stages may occur as separate and distinct phases, or simultaneously, or more commonly, the may overlap. How the stages occur depends largely on the mechanisms available to the launderer.

2.4 Money Laundering Choke Points
There are certain steps in the money laundering process that the launderer finds difficult to avoid. It is during these stages, also know as "choke points", that money-laundering activity is more likely to be recognized. Efforts to combat money laundering will therefore focus on such stages, which are as follows:

- Entry of cash into financial system.
- Cross border flows of cash.
- Transfers of cash within and from the financial system.

3. BoP's Know Your Customer Policy

The need for a bank to "know your customers" is vital for the prevention of money laundering and underpins all other activities. If a customer has established an account under false identity, (s)he may be doing so for the purpose of defrauding the bank itself or merely to ensure the (s)he cannot be traced or linked to the proceeds of the crime that the bank is being used to launder. A false name address or date of birth will usually means that the bank / law enforcement agencies cannot trace the customer if (s)he is need for interview in connection with an investigation.

When a business relationship ID being established the nature of the business that the customer expects to conduct with the bank should be ascertained at the outset to know what might be expected as normal account activity. In order to be able to judge whether a transaction is or is not suspicious, the Bank should have a clear understanding of the legitimate business of their customers.

Understanding Customers use of BoP's products

It is not possible to be alert to a potential customer's misuse of BoP's products and services without knowing what the customer says (s)he wants do with the products or services. Of course, a customer who only wants a credit card, or a loan, a checking account and nothing more, will make either a very simple statement of purpose (such as "home improvement loan") or no statement at all (in the case of most credit cards). As a customer begins to use a more complicated mix of products. More sophisticated products, or products posing greater risk to BoP (credit risk, market risk or other risk), it becomes more important to understand the customer's explanation of how those products and services are intended to fit into the customer's business.

BoP believes that clear " Know Your Customer" (KYC) policies and procedures are the Bank's most effective weapon against being used as an intermediary in money laundering activities.

3.1 Objectives of BoP's KYC Policy

- Ensuring compliance with all laws and regulations and accepted banking practices;
- Minimizing the risk that BoP will be used for illicit activities of any kind;
- Protecting the reputation of BoP;
- Protecting our good customers and enhancing their relationship with us.

The following are key attributes of BoP 's KYC policy.

- Accurate identification of all new customers and current identification from all existing customers;
- Obtaining comprehensive knowledge of transactions carried out by it's customers so as to develop a "transaction profile" of each customer;

- Identification of unusual transactions or suspicious activity in a timely manner.

As a rule, an account should never be established until the identity of the potential customer is satisfactorily established. If a potential or even an existing customer refuses to produce the requested information. the relationship officer should not proceed with any business dealings with the client.

3.2 Scope of the KYC Policy.

This KYC policy applies to all branches within BoP, including, but not limited to these general categories of customer business relationships:

- Depository, including demand deposits, time deposits, savings, and money management accounts;
- Lending, including loans, letters of credit, acceptances, leases, overdrafts;
- Transaction processing, including safe deposit box and cash letter services;
- Custody, including retail safekeeping and securities safekeeping;
- Trading, including capital market products such as foreign exchange, derivatives, governments, municipals, corporate, repos, and other public and private securities;
- Fiduciary; including corporate trust and personal trust;
- Underwriting, including all underwriting and placement activities;
- Investment, including the sale and brokerage of deposit and non-deposit based investment and insurance products.

4. BoP 's Know Your Customer Procedures

4.1 Scope and Timing of Identity Verification

4.1.1 What is Identity?

An individual's identity comprises his/her name and all other names (official and alias names) used; address at which (s) he can be located and, date of birth.
Ideally, to identify someone, an official document bearing a photograph of the person should be obtained. However, photographic evidence of identity is only of value to identify customers who are seen face-to-face. The true identity of the customer must be known at the outset, and the information provided by the customer to confirm his/her identity must be "verified" to prove as far as possible that the facts supplied are correct.

Any subsequent changes to the customer's name, address, or employment details of which the Bank becomes aware should be recorded as part of the KYC process.
Generally this is undertaken as part of good banking practice and due diligence (i.e. for the Bank's own protection against fraud and bad debts), but it also serves for money laundering prevention.

The primary duty to verify identity rests with the Account Opening Department. In some rare cases, the bank may have to approach another bank for identity verification.

4.1.2 Definitions / explanations of terms

The person or company whose identity must be verified (i.e. the prospective customer) is an "applicant for business".

An "applicant for business" may be seeking to establish a "business relationship" with the bank or may be an occasional customer undertaking a "one-off transaction". This can affect the identification requirements.

A "business relationship" is an arrangement between the bank and the "applicant for business" to facilitate the execution of transactions between the parties on a "frequent, habitual or regular" basis, and where the monetary value of dealings is not known or capable of being ascertained at the outset. The opening of any bank account should therefore be treated as forming a "business relationship".

A "one-off transaction" means any transaction carried out other than in the course of an established "business relationship". For example, a single foreign currency

transaction for a customer who does not have an account at the Bank constitutes a "one-off transaction".

4.1.3 Scope of Identity Verification

Identity must be verified in all cases where money laundering is known and suspected. (See specific details for different types of customers in later sections). It must also cover all types of the bank's business, including deposit taking, all types of lending and even issuing of credit and charge cards.

Exemptions
Identification procedures are **not required** in the following circumstances:

- It is single one-off transaction and the payment is less than (US $ 10,000).

Exception*: if at any time it is proven that a number of transactions are linked and the aggregate amount of these transactions amount to/exceeds (US $10,000), then identification procedures should be carried out. Transactions which are 3 months (or more) apart are not considered to be linked.*

- It is a Switch transaction, which originated in the branch and where all the proceeds are directly re-invested with BoP.

4.1.4 Timing of Identity Verification

What constitutes an acceptable time span for obtaining satisfactory evidence of identity must be determined in the light of all the circumstances including the nature of the business, the geographical location of the parties and the nature of evidence available before commitments are entered into or money changes hands.
Therefore, the Bank can start processing the business or application for account opening immediately, provided that it promptly takes appropriate steps to verify the customer's identity. As a rule the bank should not transfer or pay any money out to a third party until the identity requirements have been satisfied.

In preparing their procedures, the bank will need to establish clear and consistent policies to deal with situations where satisfactory evidence of identity cannot be obtained. Failure by an applicant to provide satisfactory evidence of identity without adequate explanation may in itself lead to a suspicion that the customer is engaged in money laundering.

When must identity be verified
Whenever a "business relationship" is to be established e.g. when a bank account is to be opened, or a significant "one-off transaction" or series of linked transactions to undertaken, the identity of the "applicant for business", i.e. the prospective customer, must be obtained and verified.

Once identification procedures have been satisfactorily completed, then the business relationship has been established. As long as records concerning that customer are maintained in line with Section 5, no further evidence of identity is required when transactions are subsequently undertaken for that customer as long as regular contact is maintained for at least (six) months preceding any new transaction.

When an existing customer closes one account and opens another, there is no need to re-verify identity, although good practice would be to obtain any missing or additional information and to re-confirm the details on the customer's file. This is particularly important if there has been no recent contact with the *customer e.g.* within the past twelve months. Details of the previous accounts and steps originally taken to verify identity or any introduction records should be transferred to the new account records and retained for the relevant period in accordance with the guidance set out in Section 5.

4.2 Verification Procedures

4.2.1 Guidelines for establishing satisfactory evidence of identity

- The overriding requirement for each of BoP 's branches is to be satisfied that it has established the true identity of the prospective customer as far as it is reasonably possible. The bank should establish to its satisfaction that it is dealing with a real person or organization (natural, corporate or legal), and verify the identity of those persons who have power to operate any account.

- If funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (i.e. the underlying beneficiary) should also be established and verified.

- Where face-to-face contact is normal procedure and it is expected that face-to-face contact will take place early in the business relationship, the prospective customer should be seen personally and photographic evidence of identity obtained.

- In respect of joint personal accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should be verified in accordance with the procedures set out in the paragraphs below.

- The verification procedures necessary to establish the identity of the prospective customer should basically be the same whatever type of account or service is required (e.g. current, deposit, lending accounts). The name of the authorized staff member undertaking the account opening procedure should be noted on the customer's file.

- In cases where a branch confirms a letter of credit on behalf of another bank, the customer for BoP 's purpose will be the opening bank on whose behalf BoP confirms the credit. BoP is not obliged to obtain details of the actual applicant of the letter of credit.

- The best identification documents or "Primary Evidence" such as a certified true copy of a passport should be obtained directly from the prospective customer. However, it must be appreciated that no single form of identification can be fully guaranteed as genuine or representing correct identity and that the identification process will generally need to be cumulative.

  The MLPO of each branch is responsible for laying down the criteria for classifying documents as Primary Evidence (e.g. copy of Passport and/or ID) and Secondary Evidence (e.g. copy of Utility Bill). As a rule, a customer should be asked to submit at least 2 forms of Primary Evidence.

  The evidence of identity required should be obtained from documents issued by reputable sources. File copies of the supporting evidence should be retained. Alternatively, the reference numbers and other relevant details should be recorded to enable the documents to be re-obtained.

- Every month, a designated officer from the Operations Department should conduct a review of all new customer files to ensure that the bank has obtained all the documentation as required by the procedures of the branch. In addition, all files where documentation has been found lacking as a result of previous reviews should also be reviewed to ensure that proper follow-up has been initiated and the files updated. In those branches where there are more than 100 new accounts opened during the month, the review could be done on a sample basis. The sample size in any case should not be less than 20% of the accounts opened during the month.

- If the bank has inadvertently not obtained the required documentation for any customer, this fact should be recorded in a "Pending Documentation Register" (Exhibit 1) maintained by the designated officer.

  After completing the review, the designated officer should document his findings in a memorandum addressed to the relevant Account Officer requesting immediate action to obtain the necessary documents. The HOO should also review and initial the Register. When all the required documentation has been satisfactorily received, the record can be deleted from the Register after obtaining prior approval from the HOO.

  If documentation is pending for more than six months, such cases should be reported to the MLPO on a monthly basis. At the end of each year, accounts for

which identity verification documents are pending for more than 6 months, or accounts for which other documents are pending for over one year, should be reviewed by the MLPO. The Account Officers should be advised of such accounts. As a rule, such accounts should be closed. However, in exceptional cases, an Account Officer may wish to give his (her) customers additional time to submit the necessary documents in which case the account may be allowed to remain open with the express approval of the General Manager. All such accounts should be closely monitored so that the required documentation can be obtained when the customer next visits the bank. If the Account Officers are unable to obtain the required documentation within the extended time period, the MLPO should authorize the closure of such accounts.

- Records of the supporting evidence and the methods used to verify identity must be retained for ten years after the account is closed or the business relationship ended, in line with the guidance given in Section 5 on Record Keeping.

4.2.2 Reliance on other (regulated) institutions to verify identity

Verifying identity is often time consuming and expensive and can cause inconvenience for prospective customers. It is therefore important that as far as possible the bank standardizes and simplifies its procedures and avoids duplicating the identification requirements where it is reasonable and practicable to do so.

Although the responsibility to obtain satisfactory evidence of identity cannot be avoided by the bank that is opening the account for a customer, there are occasions when it is reasonable to rely on another regulated person or institution to undertake the procedures or to confirm identity as given below.

Branch introductions

Where a customer is introduced by one branch of the BoP to another, providing the identity of the customer has been verified by the introducing branch in line with the BoP's anti-money laundering procedures, it is not necessary for identity to be re-verified or for the records to be duplicated. The account file should contain authenticated documentation confirming that the introducing branch has complied with the identity verification requirements.

In exceptional circumstances, the bank may need to approach another bank, on a non-competitive basis, specifically for the purpose of verifying identity. In these exceptional circumstances, the Applicant Introduction Certificate (Exhibit 2) should be used for making the enquiry. The request should be signed by the MLPO. To enable branches to comply with the legislative requirements, it is important that response are received to enable the bank to verify identity positively without undue delay.

As such requests are normal procedure, an enquiry form to confirm identity for money laundering purposes could frequently be misinterpreted by the receiving

bank. It is important that the distinction is recognized by the bank's staff and by the receiving institution.

4.2.3 Account Opening Procedures

Individuals

All individuals must be positively identified by independently verifying the data given be below. (This requirement is not applicable for staff accounts).

- Name
- Address
- National ID or other identifying number.
- Date of birth.

The true name of names used should be verified by reference to a document obtained from a reputable source, which bears a photograph (passport and/or national ID). In addition to the name, it is important that the current permanent address should be verified, as it is an integral part of identity. Satisfactory evidence can be obtained by undertaking a combination of the following checks:

- Making a PMA's credit reference search;
- Requesting sight of a recent utility bill, bank statement (to guard against forged of counterfeit documents, care should be taken to check that the documents offered are originals);
- Checking a local telephone directory.

An introduction from a respected customer personally known to the Management, or from an Officer/ Authorized signatory of the Bank, may assist the verification procedure but must not replace the need for address verification procedures set out in paragraph above. Details of who initiated and authorized the introduction should be recorded on the customer's file. However, personal introductions without full verification should not request other staff to breach account opening procedures as a favor to the applicant.

Particular car should be taken in accepting documents that are easily forged of which can be easily obtained by falsifying identity. Due to the fact that documents providing photographic evidence of identity need to be compared with the applicant's appearance customers should be asked to bring these identity documents personally to the bank.

Exceptional Approvals

Where independent identity verification is not possible, for example for very young or elderly persons, accounts may be opened by exceptional approvals. In such cases, approval should be obtained from the GM of the bank.

In the case of non-resident individuals, passports and national ID cards should be used for identity verification. In the case of minors, parents can provide identification.

Business Accounts

Particular care should be taken to verify the legal existence of applicant (i.e. the company) any to ensure that any person purporting to act on behalf of the applicant is fully authorized. The principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

If a commercial relationship is envisaged, a personal visit must be made be the account officer to confirm the existence of corporation and the nature of the business. A corporate resolution must be available showing the authority of designated signatories and a copy of the resolution and the signatories identification documentation should be maintained of file.

Corporate Customers

Due to the difficulties of identifying beneficial ownership, corporate accounts are most likely to be used as vehicles of money laundering, particularly when fronted by a legitimate trading company. The customer may be a quoted company or a subsidiary of such a company or even a private company whose directors are known to the bank.

The following documents should be obtained in the case of a company:

- Original or certified copy of the Certificate of Incorporation or the Certificate to Trade;
- Certified true copy of relevant resolution of the Board of Directors;
- The Memorandum and Articles of Association;
- Results of credit checks from the PMA.

Exchange Houses

Although the Exchange Houses are regulated by the PMA, in the case of companies engaged in money exchange or money transmittal, the Bank should take extra care in screening accounts relation to such companies. In addition to the customary account opening documentation, the valid license form the PMA are required, and evaluation report must be completed and updated annually.

Non Registered Companies

The Bank should identify the persons who ultimately own and control the company and should obtain documents listed above for corporate customers. If the company is already in existence, the signatures on the mandate should be confirmed.

Money Brokers
Money Brokers regulated by PMA, usually bring the transacting parties together in the wholesale deposit business. BoP should not rely on brokers for undertaking detailed verification procedures of the counter parties introduced by the broker.

Clubs and Societies
The identity of at least two partners should be verified Additionally, a mandate should be obtained from the board of directors of the club or the societies authorizing the account opening and conferring authority on the account operators. The identity of all signatories should be verified. A license from Ministry of Interior to approve opening such an account is required.

Powers of Attorney
The authority to deal with assets under a Power of Attorney constitutes a business relationship and therefore, where appropriate, the bank should check the identity of any holders of powers of attorney or third party mandates. Records of all transactions undertaken in accordance with the Power of Attorney should be kept in accordance with Section 5.

Trust Accounts
When a transaction is being done on behalf of a third party, the identity of the original party should be identified.

Ultimate responsibility for verification procedures at the time of Account Opening.

In cases where junior assistants perform the initial account functions, the process will be considered complete only when the Account Officer has signed the Account Opening form. Therefore, the ultimate responsibility to ensure that verification procedure are complied with and documented is that of the Account Officer.

5. Record Keeping

All branches should retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering, as these are essential components of the audit trail. If investigations into a money laundering case cannot link criminal funds passing through the financial system with the original criminal money, then confiscation of the criminal funds cannot be made. Often the only valid role a financial institution can play in a money laundering investigation is through the provision of records, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trail.

The records prepared and maintained by the bank on its customer relationships and transactions should be such that:

- Requirements of BoP procedures and any external regulations/ legislation are fully met;
- Competent third parties will be able to assess the Bank's observance of anti-money laundering policies and procedures;
- Any transactions effected via the bank can be reconstructed; and
- The bank can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to the disclosure of information.

The single most important feature of the Basel Regulations in this area is that they require relevant records to be retained for at least five years from the winding up of the relationship with a customer.

5.1 Identity Records

Documents verifying "Evidence of Identity" must be kept for a minimum period of ten years after the relationship with the customer has ended. The records retained must indicate the nature of the evidence of identity obtained. A copy of the evidence or any information as would enable a copy to be obtained must be kept on file. The date when the relationship with the customer has ended is the date of:

- The carrying out of a one-off transaction or the last in the series of transactions; or
- The ending of the business relationship, i.e. the closing of the account(s); or
- The commencement of proceedings to recover debts payable on insolvency whichever earlier.

5.2 Transaction Records

Transaction records must be retained for a period of at least ten years following the date on which the relevant transaction or series of transaction is completed. The precise nature of the records required is not specified. But the objective is to ensure, in so far as is practicable, that in any subsequent investigation the concerned branch can provide the authorities with its section of the audit trail.

Transaction logs must contain the following data (also see 5.6 below):

- Date of the transaction, customer's name and account number
- Type of transaction (include serial number if it involves monetary instrument)
- Amount of the transaction
- Identity of the bank personnel who conducted the transaction (or System ID)
- Identity of the officer who approved the transaction, and the payee.

5.3 Format of Records

Retention may be by way of: original documents; computerized; or, electronic form, including Optical Disk. However, the record retention requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Document held centrally must be capable of distinguishing between the transaction relating to different customers and of identifying where the transaction took place and in what form.

5.4 Retrieval of Relevant Records

The overriding objective is for the bank is to be able to retrieve relevant information without undue delay. An investigating officer will usually require that the information requested should be available within a specified number of days (usually not longer than a week).

When setting document retention policy, the bank must weigh the statutory requirements and the needs of the investigation authorities against normal commercial considerations. When original vouchers are used for account entry, and are not returned to the customer or his agent, it is of assistance to law enforcement agencies if these original documents are kept form at least one year to assist forensic analysis. This can also provide evidence to a branch when conduction its own internal investigations.

5.5 Bank's Record Retention Policy

Where documents verifying the identity of a customer are held in one branch of the BoP, they do not need to be held in duplicate form in another. However, they must wherever possible be freely available on request within the bank, or otherwise be available to the investigation agencies under legal procedures and mutual assistance treaties. Access to bank records must not be impeded by confidentiality or data protection restrictions.

5.6 Funds Transfer Record Keeping

Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the original ordering customer of the ultimate beneficiary is not clearly shown in an electronic payment message instruction.

When sending SWIFT MT 103 message, the fields for ordering and beneficiary customers should be completed with respective names and addresses. In case this is no done. Full records of the ordering customer must be kept by the originating department. This is no mandatory if both parties are banks.

The following procedures relate to the originating or transmitter's financial institution the intermediary financing institution and the beneficiary's financial institution.

Required records may be kept on paper, microfilm, or electronic systems and must be retained for ten years. The originator, intermediary and the beneficiary must keep a record of the following:

- Name and address of the originator;
- Amount and execution date of the payment order;
- Payment instructions;
- The identity of the beneficiary's bank;
- The beneficiary's name and address and account number;
- Any other specific identification of the beneficiary.

If the originator is not an established customer who is already obtaining financial services from the institution then additional records should be kept. Information to be included by the transmitter's financial institution include:

- Name and address of the transmitter; and the amount of the transmittal order:
- Name of the recipient's financial institution;
- Name and address or specific identifier of the transmitter's financial institution;
- Name, address, account number and specific identifier of the recipient.

If a branch receives instructions from another financial institution for forwarding, the following records should be maintained:

- Name, address and account number of the transmitter;
- Amount and execution date of the transmittal order,
- Identity of the recipient's financial institution;
- Name, address, account number and specific identifier of the recipient;
- Name and address or specific identifier of the transmitter's financial institution.

The originator's bank must be able to retrieve the required information by reference to the originator's name or, if the originator is an established customer, by reference to the number of the account used for fund transfers.

6. Recognition and Reporting of Suspicious Transactions

6.1 Recognition of Suspicious Transactions

As the types of transaction that may be used by "A Money Launderer" are almost unlimited. It is difficult to define a suspicious transaction. Suspicion is personal and subjective, and falls far short of proof based on firm evidence. However, it is more than the absence of certainty that someone is innocent. Nevertheless, a person would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime.

Where there is a business relationship, a suspicious transaction will often be one that is inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is to know enough about the customer and the customer's business to recognize that a transaction, or series of transaction, is unusual.

Questions that the bank might consider when determining whether an established customer's transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?

Where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

6.2 Examples of Suspicious Transactions

Example of what might constitute suspicious transactions, are given in appendix 1. These are not intended to be exhaustive and provide examples only of the most basic ways by which money may be laundered.

6.3 Reporting of Suspicious Transactions

All branches have a clear obligation to ensure that reporting of suspicious transaction is done in accordance with the Internal Reporting Procedures set out in Section 1.4.3 of the manual. It is essential that:

- Each employee knows to which person he or she should report suspicions and;
- There is a clear reporting chain under which those suspicions will be passed without delay to the MLPO.

Once an employee has reported his/her suspicion to the MLPO (s) he has fully satisfied the legal obligation.

7. Staff Training

7.1 The Need for Staff Awareness

Staff must be aware of their obligations, and must be informed that they can be held personally liable for failing to report information in accordance with internal procedures. Staff should be encouraged to co-operate fully and to provide a prompt report of any suspicious transactions.

All relevant staff should be educated in the importance of the " know Your Customer" requirements for money laundering prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer, but also, where a business relationship is being established the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date.
Moreover, the staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

7.2 Staff Training Procedures

The bank should provide training to its employees on the following:

- The bank's procedures on money laundering.
- The legal requirements concerning the obligations of the bank and its employee.
- The techniques of recognition of suspicious transactions.

Although Directors and Senior Management may not be involved in the day-to-day procedures, it is important that they understand the legal obligations placed on them, their staff and the bank itself.

The timing and content of training for various sectors of staff will need to be adapted to by the Bank Compliance Officer. BoP Training Center should play a prominent role in planning the training schedules of the staff at each branch.

7.3 Supervisors and managers

A higher level of instruction covering all aspects of anti-money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include:

- The offences and penalties arising from the non-reporting and for assisting money launderers;
- Procedures relating to the service of production and restraint orders;
- Internal reporting procedures;
- The requirements for verification of identity; and
- The requirements for retention of records.

7.4 Money laundering Prevention Officers

In-depth training concerning all aspects of the PMA instructions and internal policies will be required for the MLPOs at all branches. In addition, each MLPO will require extensive initial and on-going instruction on the validation and reporting of suspicious transaction, on the feedback arrangements, and on new trends and patterns of criminal activity.

7.5 Methods of providing training

There is no standard preferred way to conduct staff training for money laundering purposes. The training should be tailored to meet the needs of the bank, depending on the available time and resources. Assistance can be obtained from firms of accountants and specialized training agencies. The Bank Compliance Officer at each branch will be responsible for devising the training methodologies.

Appendix 1

Examples of suspicious transaction

Customer Service Department / Tellers

- Customer is reluctant to provide proper identification or other information or provides information that seems sketchy or false.
- Customer has more than one account in more than one name without a clear and logical reason.
- Customer attempts to make several large cash deposits over a short period of time to one or more accounts.
- Customer requests the exchange of large amounts of currency from small to large denomination bills.
- Customer makes frequent purchases of monetary instruments for cash.
- Customer makes constant deposits of funds and immediately wires the money out, Note: This is common in the course of business of a foreign exchange company.
- Customers who receive wire transfers and immediately purchase monetary instruments in favor of another party.
- Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.
- Customers who frequently exchange cash into other currencies.
- Customers whose deposits contain counterfeit notes or forged instruments.
- Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
- Large cash deposits using ATM facilities thereby avoiding direct contact with the bank staff.
- Unusually large cash transaction made by an individual or company whose ostensible business activities would normally be generated by cheques. Letters of credit, and other instruments.
- Customers who wish to maintain a number of clients' accounts that do not appear consistent with the type of business including transactions that involve nominee names.
- Substantial increases in cash deposits that are subsequently, within a short period of time, transferred out of the account or transferred to a destination not normally associated with the customer.

Off-Shore International Activity

- Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- Customers who make regular and large payments, including wire transaction, that cannot be clearly identified as bona-fide transaction to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs, proscribed terrorist organizations.
- Building up of large balances, not consistent with the turnover of the customer's business and subsequent transfer to accounts held overseas.
- Unexplained electronic fund transfers by customers "out going and incoming" without passing through an account.
- Frequent request for foreign currency drafts or other negotiable instruments to be issued.
- Frequent paying in foreign currency drafts particularly if originating from overseas.

Wire Transfer Operators

- Customer experiences a sudden increase in wire transfer activity that cannot be explained.
- Customer receives international transfers that cannot be explained.
- Customer receives many small incoming wire transfers or deposits of checks and money orders and then requests wire transfers to another city or country.
- Customer uses wire transfers to move large amounts of money to a secrecy haven country.
- A non-account holder receives incoming wire transfers under instructions to the bank to "pay upon proper identification" or to convert the funds to cashier checks and mail them to the non-account holder.

Account Officer, Rick management and Credit Administration-loans

- A customer's stated purpose of the loan does not make economic sense.
- A customer's unwilling to disclose the purpose of the loan requested.
- The beneficiary of the loan is an offshore company.

Customer Service Department/Tellers:

- Customers who deposit cash by numerous credit slips so that each individual deposit is of a small value but the total of all such deposits is a significant sum.
- Any individual or company whose account shows virtually no normal personal banking or business related activities but is used to receive or disburse out large sums of money which have no obvious purpose or relationship with the account holder or his business.

- Customers who appear to have accounts with the several financial institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of funds.
- Paying in large third party cheques endorsed in favor of the customer.
- Large cash withdrawals from a previously dormant or inactive account or from an account, which has just received an unexpected large credit from a broad.
- Customers who together, and simultaneously use separate tellers to conduct large cash transactions or foreign exchange transactions.
- Insufficient use of normal banking facilities e.g. avoidance of high interest rate facilities for large balances.
- Larger number of individuals making payments into the same account without an adequate explanation.

Investment Related Transactions:

- Purchasing securities to be held by the financial institution in safe custody. Where this does not appear to be appropriate given the customer's apparent standing.
- Back to back deposit/loan transactions with subsidiaries of, or affiliates of overseas financial institutions in known drug trafficking areas.
- Requests for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing.
- Large or unusual settlements of securities in cash form.
- Buying and selling of a security with no discernable purpose or in circumstances, which appear unusual.

Account Officer, Risk Management and Credit administration-Loans

- The customer proposes to secure the loan with obligations from offshore banks.
- A customer purchases bonds or stocks and his/her sole purpose of doing so is to use them as loan collateral.
- A customer uses a cash deposit to collateralize a loan.
- A customer pays down a large problem loan suddenly, with no reasonable explanation for the source of funds used for the repayment.
- Request to borrow against assets held by the financial institution of a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
- Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

Exhibit 1

سجل الوثائق المعلقة									
العلامة الأولية									
التاريخ	العميل	رقم الحساب	الموظف المسؤول	تاريخ فتح الحساب	الوثائق المعلقة	الاستحقاق	تاريخ المراجعة	الملاحظات	التوقيع
العلامة الثانوية									
التاريخ	العميل	رقم الحساب	الموظف المسؤول	تاريخ فتح الحساب	الوثائق المعلقة	الاستحقاق	تاريخ المراجعة	الملاحظات	التوقيع

Exhibit 2

شهادة معرف

(تعبأ بواسطة المعرف)

اسم مقدم/ة الطلب :.....

عنوان مقدم/ة الطلب :.....

.....

1–تم التأكد من هوية مقدم الطلب وتم مطابقة جميع الوثائق المقدمة ونؤكد بان الاسم والعنوان في الطلب صحيح.

2–جميع المستندات والوثائق ممكن استلامها في الحالات الآتية. (اختيار أ أو **ب)**

أ– مرفقة بالطلب

ب– جميع الملفات تزود إليكم عند الطلب أو عند طلب المحكمة.

(يجب اختيار 3 أ أو 3 ب)

3 أ – مقدم/ة الطلب يعتبر شخصي وليس معين للمنصب أو وصي أو وكيل لتقديم الطلب.

3 **ب** – مقدم/ة الطلب يعتبر (معين للمنصب أو وصي أو وكيل.....)

لشخص آخر وجميع المستندات متوفرة لدينا ويمكن تزويدها لكم عند الطلب.

اسم الجهة المعرفة:.....

التوقيع:.....الاسم:.....

المنصب : .....التاريخ:.....

Exhibit 3

تقرير العمليات المشكوك فيها						
التاريخ	اسم العميل	رقم الحساب	تفاصيل العملية	اسم الموظف المبلغ	توقيع اللجنة	القرار/الإجراءات