BLOM BANK FRANCE

AML MANUAL

Prepared by: Hala Abou Alwan Haidar
Section one: General and Theoretical AML Overview

1.1 Chapter one: International Legal and Organizational origins

1.1.1 Basel Committee- Prevention of criminal use of the banking system for the purpose of money-laundering -December 1988

1.1.2 The International Money Laundering Information Network (IMOLIN)-1998

1.1.3 The Financial Action Task Force on Money Laundering (FATF * GAFI)

1.1.4 Basel Committee Publication no. 85, October 2001

1.1.5 Basel II-June 2004

1.1.6 AML Procedures set by the U.S. Treasury under USA Patriot Act

1.1.7 Sanctioned/Non cooperative countries

1.1.8 CIP – Customer information program.

1.2 Chapter two: Local Origins

1.2.1 U.A.E Central Bank directives N0.24/2000

1.3 Chapter three: Definition & reasons of M L.

1.3.1 Definition

1.3.2 Why do criminals launder money?

1.4 Chapter four: The stages of Money Laundering

1.4.1 Stage one: Placement

1.4.2 Stage two: Layering

1.4.3 Stage three: Integration

1.5 Chapter five: Consequences of Money Laundering:

1.5.1 Consequence one: Finances Terrorism

1.5.2 Consequence two: Undermines Financial System

1.5.3 Consequence three: Expands Crime

1.5.4 Consequence four: Criminalizes Society

1.5.5 Consequence five: Reduces Revenue and Control

1.6 Chapter six: Know your correspondent bank (KYCB) and employees

1.6.1 KYCB:

1.6.2 KYE

Section Two: Procedural AML Practices

2.1 Chapter one: Compliance/AML Organizational Structure

2.1.1 Risk Management

2.2 Chapter two: AML Department – Detailed Practical Procedures (Dubai and Sharjah Branches)

2.2.1 Documents required before opening any account

2.2.2 Account opening procedures (Dubai and Sharjah):

2.2.3 When the signatory information is required? (Dubai and Sharjah):

2.2.4 Account Renewal procedures (Dubai and Sharjah):
2.2.5 Special case: Companies Under Establishment

2.2.6 Documents required after the account is opened.

2.3 Chapter three: Know Your Customer (Dubai and Sharjah Branches):

2.3.1 KYC Policy elements:

2.3.2 Customer’s Interview basics:

2.3.3 KYC Content:

2.3.4 KYC renewal:

2.3.5 Economic Sector:

2.3.6 Setting the Limits

2.3.7 Effective KYC-Risk Mitigation

2.4 Chapter four: Monitoring and Follow up.) Dubai and Sharjah Branches)

2.4.1 Monitoring the account’s flow of transactions (inward-outward transfers, cash deposits, etc.), in general.

2.4.2 Monitoring strategy:

2.4.3 Spotting suspicious activity:

2.4.4 Credit Department:

2.4.5 Swift/OFAC list control:

2.4.6 OFAC Side Station Program:

2.5 Chapter five: Politically Exposed People (PEP/FPEP) (Dubai and Sharjah Branches)

2.5.1 Steps in preparing the PEP list

2.6 Chapter six: Central Bank Notices

2.6.1 Kinds of Notices:

2.7 Chapter seven: Reporting Suspicious Transactions:

2.7.1 Definition:

2.7.2 Responsibility

2.7.3 Reporting:

2.8 Chapter eight: Filing:

2.8.1 KYCs

2.8.2 Swifts

2.8.3 Memos:

2.8.4 Letters:

2.8.5 Capital Certificates

2.8.6 Compliance /AML notes:
1 Section one: General and Theoretical AML Overview

1.1 Chapter one: International Legal and Organizational origins

1.1.1 Basel Committee- Prevention of criminal use of the banking system for the purpose of money-laundering -December 1988

The Basel Committee on Banking Supervision is an institution created by the central bank Governors of the Group of Ten nations (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States). Its membership is now composed of senior representatives of bank supervisory authorities and central banks from the G-10 countries, and representatives from Luxembourg and Spain. It usually meets at the Bank for International Settlements in Basel, where its 12 member permanent Secretariat is located.

The Basel Committee formulates broad supervisory standards and guidelines and recommends statements of best practice in banking supervision in the expectation that member authorities and other nations' authorities will take steps to implement them through their own national systems, whether in statutory form or otherwise.

Basel Committee on Banking Supervision (BCBS) issued in 1988 the first set of three papers under the name “Prevention of criminal use of the banking system for the purpose of money-laundering” that address the importance of establishing sound KYC policies and procedures for guaranteeing the integrity of banking systems. The BCBS encouraged banks to stipulate the basic ethical principles and put in place effective procedures to identify customers, decline suspicious transactions, and cooperate with law enforcement agencies.

The following two papers (1997 and 1998) established, elaborated on the core principles for effective banking supervision.

1 See “Prevention of criminal use of the banking system for the purpose of money-laundering.” http://www.bis.org/publ/bcbsc002.htm#v1d12.
2 See “Core principles for effective banking supervision.” http://www.bis.org/publ/bcbs30a.htm.
1.1.2 The International Money Laundering Information Network (IMoLIN)-1998

IMoLIN is an Internet-based network assisting governments, organizations, and individuals in the fight against money laundering and the financing of terrorism. IMoLIN has been developed with the cooperation of the world's leading anti-money laundering organizations.

1.1.3 The Financial Action Task Force on Money Laundering (FATF * GAFI)

The Financial Action Task Force on Money Laundering (FATF), also known by the French name Groupe D'action Financière Sur Le Blanchiment De Capitaux (GAFI), is an inter-governmental body founded in 1989 by the G7 (Group of Seven (G7), a group of seven industrialized nations of the world, formed in 1976 when Canada joined the Group of Six (United States of America, France, Germany, Italy, Japan, United Kingdom).

The purpose of the FATF is to develop policies to combat money laundering and terrorist financing. The FATF Secretariat is housed at the headquarters of the OECD in Paris.

The primary policies issued by the FATF are the Forty Recommendations on money laundering and the Special Recommendations on Terrorist Financing. Together, the Forty Recommendation and Special Recommendations on Terrorist financing set the international standard for anti-money laundering measures and combating the financing of terrorism. Both sets of FATF Recommendations are intended to be implemented at the national level through legislation and other legally binding measures.


- Implement relevant international conventions
- Criminalize money laundering and enable authorities to confiscate the proceeds of money laundering.
- Implement customer due diligence (eg: identity verification), record keeping and suspicious transaction reporting requirements for financial institutions and designated non-financial businesses and professions
- Establish a financial intelligence unit to receive and disseminate suspicious transaction reports.

---

4 Annex page: 100
Cooperate internationally in investigating and prosecuting money laundering.

The FATF issued 8 Special Recommendations on Terrorist Financing in October 2001, following the September 11 terrorist attacks in the United States. The FATF issued a ninth Special Recommendation on Terrorist Financing in October 2004.

1.1.4 **Basel Committee Publication no. 85, October 2001**

In October 2001, the Basel Committee on Banking Supervision published a paper on "Customer Due Diligence for Banks", which was supplemented in February 2003 by the "General Guide to Account Opening and Customer Identification". The aim of the paper was to provide customer identification and know-your customer framework that may serve as a benchmark for banking supervisors to establish national practices and for banks to design their own KYC programs. The guidance provided in the paper enjoys broad international support from banking regulators. This paper identifies four essential elements for a sound KYC programme, as follows: customer acceptance policy, customer identification, ongoing monitoring of higher-risk accounts, risk management.

1.1.5 **Basel II-June 2004**

Basel II is the second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. The purpose of Basel II, which initially was published in June 2004, is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. Advocates of Basel II believe that such an international standard can help protect the international financial system from the types of problems that might arise should a major bank or a series of banks collapse. In practice, Basel II attempts to accomplish this by setting up rigorous risk and capital management requirements designed to ensure that a bank holds capital reserves appropriate to the risk the bank exposes itself to through its lending and investment practices. Generally speaking, these rules mean that the greater risk to which the bank is exposed, the greater the amount of capital the bank needs to hold to safeguard its solvency and overall economic stability.

Basel II is an international Accord that requires banks and financial services firms to have a more rigorous risk sensitive framework for the assessment of regulatory capital, and sets international capital adequacy standards to ensure that lenders can meet their obligations.
1.1.6 **AML Procedures set by the U.S. Treasury under USA Patriot Act**

The USA PATRIOT Act was passed by the United States Congress in 2001 as a response to the September 11, 2001 attacks. It has ten titles, with the third title ("Title III: International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001") written to prevent, detect, and prosecute international money laundering and the financing of terrorism.

Title III is itself divided into three subtitles. The first subtitle, entitled Subtitle A: International Counter Money Laundering and Related Measures, is designed to put measures into place that counter international money laundering. It does this by requiring that financial institutions take several new special measures against money laundering — identification is dealt with particularly; by restricting or prohibiting the use of certain types of bank accounts; through adding further legislation that regulates a financial institution's dealing with foreign concerns; by adding new penalties for non-compliance of the law; and through regulations that are designed to facilitate and encourage reporting and communication between financial institutions and the U.S. government.

1.1.7 **Sanctioned/Non cooperative countries**

Executive summary of the October 2007 NCCTS report shows the following: The eighth annual review of the FATF’s non-cooperative countries and territories (NCCTs) initiative summarizes the NCCTs process and updates the situation on the jurisdictions identified as non-cooperative and those monitored as of June 2006.

In October 2006, the FATF removed Myanmar from the NCCTs list. To ensure continued effective implementation of reforms in Myanmar, the FATF monitored developments there for a period of time after de-listing, in consultation with the relevant FATF-style regional body (FSRB), and paying particular attention to the areas of concern laid out in this NCCT report. While some progress has been made, the FATF will continue to monitor Myanmar for the time being.

The FATF de-listed Nigeria in June 2006, and monitored that country’s progress in implementing reforms until June 2007, when the FATF ended its formal monitoring. Similarly, Nauru (having been de-listed in October 2005), was subject to formal monitoring until October 2006, when FATF ended the monitoring period. Nauru is a member of the Asia Pacific Group on Money Laundering (APG), an FSRB, which has mechanisms to review members’ progress in implementing
AML/CFT measures. Nigeria is a member of GIABA (Groupe Inter-Gouvernemental d'Action Contre le Blanchiment de l'Argent en Afrique), an FSRB, which also has mechanisms to review members’ progress in implementing AML/CFT measures.

1.1.8 **CIP – Customer information program.**

1.1.8.1 **Definition of CIP**

Customer Identification Programs: Getting to Know You

If you opened a new bank or other financial account recently, you may have noticed you had to supply a lot more personal information than in the past. You may have assumed you had to prove you are you as a guard against the growing crime of identity theft. Not so.

Customer identification programs (CIPs) are now required by federal law to prevent financing of terrorist operations and money laundering. The requirements go beyond just verifying your identity. Banks must now keep records of identifying information and check customer names against terrorist lists. This applies to anyone who opens a new account.

1.1.8.2 **Financial institutions covered by CIP**

The PATRIOT Act requires CIPs for a broad category of companies that fall under the definition of “financial institution”, a term defined by the Bank Secrecy Act. A partial list of business sectors that qualify as “financial institutions” was published along with the final CIP Rule. The list includes:

- Commercial banks.
- Agencies and branches of foreign banks in the United States
- Thrifts (savings and loan institutions)
- Credit unions
- Private Banks
- Trust companies
- Investment companies
- Brokers and dealers in securities
- Futures commission merchants
- Insurance companies
- Travel agents
- Pawnbrokers
- Dealers in precious metals
- Check cashers
- Casinos
- Telegraph companies
1.2 Chapter two: Local Origins

1.2.1 *U.A.E Central Bank directives N0.24/2000*

This circular regulated the procedures for Money Laundering by setting up rules for most of the related banking transactions.

1.2.1.1 Definition of Money Laundering:

Money Laundering refers to any transaction aimed at concealing and/or changing the identity of illegally obtained money, so that it appears to have originated from legitimate sources, where in fact it has not.

This definition includes monies that are destined to finance terrorism or criminal acts.

1.2.1.2 Documents/information required by AML department for account holders or for new accounts:

1.2.1.2.1 Individual’s Accounts:
- Full name of account holder.
- Current address and place of work.
- Physical checking of the passport and keeping a copy thereof initialed by the account opening officer under “true copy of the original”.

1.2.1.2.2 Juridical Persons:
- Copy of a valid trade license to be on file at all times.
- Name and address of the account holder.
- Names and addresses of partners.
- For public shareholding companies, the bank should maintain the names and addresses of shareholders whose shareholdings exceed 5%.

1.2.1.2.3 Cooperative/Charitable/Social/Professional Societies:
Original certificate, signed by Minister of Social Affairs, confirming their identities and permitting them to open bank accounts, and whether they are
allowed to collect donations and make financial transfers out of the UAE through some of these accounts.

1.2.1.2.4 Update of Information
All subsequent changes in the information provided on account holders should be updated regularly.

1.2.1.2.5 Account Holders Name
It is strictly prohibited to open accounts with assumed names or numbers. The bank should always rely on account holder’s name as in the passport (short name may be used) or trade license in case of juridical persons.

1.2.1.3 Dealings and Transactions with Non-Account Holders/Walk-in Clients

1.2.1.3.1 Payment by Cash for Transfers/Drafts for Amounts in Excess of AED 40,000 or its Equivalent
Physical checking of the client’s identification card, passport etc, and keeping a copy thereof initialled by the account opening officer under “true copy of the original”.
Name and Full details of the beneficiary.
The above information is then entered into the special form (CB9/2000/1), which is initialled by the client and the Head of Foreign department.

1.2.1.3.2 Incoming Transfer/Draft/Travellers’ Cheques to be Paid in Cash to a Non-Account Holder in Excess of AED 40,000 or its Equivalent
Physical checking of the client’s identification card, passport etc, and keeping a copy thereof initialled by the account opening officer under “true copy of the original”.
Form (CB9/2000/2) should be filled in, and filed in a special file.
1.2.1.3.3 Deposit in the Accounts of Clients
Where cash funds or travellers’ cheques are to be deposited into an existing account by a person/(s) whose names do not appear on the mandate for that account, or are not the usual employees or messengers of the account holder, particular attention and prudence are required.
If it appears that the transaction is carried-out on behalf of another person, vigilance is required, i.e. it becomes necessary to identify that person and record his details.

1.2.1.3.4 Suspicious Transactions
In case of suspected money laundering transaction, the identity of the customer must be verified at any rate and in the same way as described above, regardless of the amount, whether the concerned amount is less or more than AED 40,000 or its equivalent.

1.2.1.3.5 Safe Deposit Boxes
Details of customers who rent boxes measuring 70 cm x 70 cm x 70 cm should be maintained.
In case of non residents renting such boxes (70 cm x 70 cm x 70 cm), the Central Bank should be provided with copies of the forms containing details of each one of them.
In case of renting more than one box, the aggregate volume should be treated as the volume of one box.

1.2.1.4 Possible Forms of Money Laundering
1.2.1.4.1 Possible Money Laundering via Cash Transactions
Unusually large cash deposits made by an individual or a company whose ostensible business activities would mainly be conducted by cheques or other instruments.
Substantial increase in cash deposits by any customer or financial institution without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer.
Customers who deposit cash in numerous stages so that the amount of each deposit is below the amount prescribed as an indicator, but the total of which is equal to or exceeds the amount prescribed as an indicator.
Company accounts whose transactions, both deposits and withdrawals are mainly conducted in cash rather than in negotiable instruments (e.g. cheques, L/C’s, drafts. Etc.), without an apparent reason.

Customers who constantly pay-in or deposit cash to cover requests for bankers’ drafts or money transfers or other negotiable instruments, without an apparent reason.

Customers who seek to exchange large quantities of low denomination banknotes with no obvious reasons. In such case, if the amount exchanged is AED 40 thousand or equivalent in other currencies, form CB9/2000/3 should be filled and placed in a special file.

Customers who transfer large sums of money outside the country with instructions for payment in cash, and large sums transferred from outside the country in favour of non-resident customers with instructions for payment in cash.

Unusually large cash deposits using “ATMs” or “cash deposit machines” to avoid direct contact with the employees of the bank or other financial institution, if such deposits are not consistent with the business/normal income of the concerned customer.

### 1.2.1.4.2 Possible Money Laundering via Customers Accounts

Customers who maintain a number of trustee or customers’ accounts not required by the type of business they conduct, particularly if there were transactions which contain names of unknown persons.

Customers who have numerous accounts and pay-in amounts of cash to each of these accounts, whereby the total of credits is a large amount, except for institutions which maintain these accounts for banking relationships with banks which extend to them facilities from time to time.

Any individual or company whose account 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 for a purpose not related to the account holder and/or his business (e.g. a substantial turnover in the account).

Customers who have accounts with several financial institutions within the same locality and who transfer the balances of those accounts to one account, then transfer the consolidated amount to a person abroad.

Paying-in large third party cheques endorsed in favor of the account holder, when there does not seem to be relevance to the account holder and his nature of business.

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

A large number of individuals who deposit monies into the same account without adequate explanation.
Unusual large deposits in the accounts of a jewelry shop whose accounts have never witnessed such deposits, particularly if a large part of these deposits is in cash.
Special attention should be paid for transfers originating from, or destined to countries which do not apply the FATF Recommendations or do not ensure that its financial institutions implement those Recommendations.

1.2.1.4.3 Possible Money Laundering via Investment-Related Transactions

Purchasing of securities to be held by the Bank in safe custody, where this does not appear appropriate given the customer’s apparent standing.
Loan transactions against pledge of deposits of a subsidiary or subsidiaries with financial institutions outside the country, especially if these were in countries known for the production or processing of drugs or are large markets for drugs, as per the list issued by the Central Bank from time to time.
Individuals or commercial institutions who bring in large sums of money to invest in foreign currencies or securities, where the size of the transactions is not consistent with the income of the concerned individuals or commercial institutions.
Buying or selling of securities with no discernible purpose or in circumstances which appear unusual.

1.2.1.4.4 Possible Money Laundering via International Banking and Financial Transactions

Customers introduced by a branch outside the country, an affiliate or another bank based in one of the countries in which drugs are produced or processed.
Building up of large balances, not consistent with the known turnover of the customer’s business, and the subsequent transfer to account(s) held abroad.
Frequent requests for travellers’ cheques, foreign currency drafts or other negotiable instruments for amounts exceeding the limit prescribed as indicator for no obvious reasons.
Frequent paying-in of travellers’ cheques or foreign currency drafts, exceeding the limit prescribed as indicator for no obvious reasons, particularly if originating from abroad.
1.2.1.4.5 Possible Money Laundering Use of Trade Finance Instruments

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. In this connection, the bank adheres to the following:

The Bank should ensure that transport of goods is not carried out through a shipping company owned by the applicant, and that the beneficiary of the letter of credit is not also owned by the applicant.
Amounts of letters of credit submitted by the customer to the bank and to the Customs/Port/Airport authorities should match the original.
Checking of documents should be on selective and regular basis with the shipping companies and Customs/Port/Airport authorities.
The size of the facilities should be in line with the securities on hand, nature of the business and net worth of the customer.
The merchandise of any L/C should be commensurate to the line of business of the client.
For high value L/C’s (in excess of the equivalent of AED 500K), credit report on beneficiary must be called for from their bankers. The report(s) must include “ownership” details as well as business details of the beneficiary (endeavour must be made to get these details).

1.2.1.4.6 Possible Money Laundering via Secured and Unsecured Loans

Customers who repay classified/problem loans before the expected time and for larger amounts than anticipated.
Customers who request loans against assets held by the financial institution or third party, where the origin of those assets is not known, or that the assets are inconsistent with the customer’s standing.
Customer/customers who request a financial institution to lend them or arrange loans for them with a third party, where the source of the customer/customers financial contribution in such loans is unknown.
1.2.1.5 Special Regulations

1.2.1.5.1 Inward remittance from KSA / Draft issued by KSA

Banks.

Saudi Arabian Monetary Agency requested to closely monitor the flow of remittances received from the Kingdom -of Saudi Arabia and to block transfers of suspicious funds from the Kingdom,

Step one: by following the instructions in circular no. 24/2000 accurately.

Step two: by implementing the following additional 5 procedures:

Procedure one: Providing the agency details about the entities wherein an aggregate of AED. two million or more is transferred into their accounts within a period of maximum six months (as per Form N0-02-2/2001- attached) after deduction of funds relating to money market transactions or documentary credits. Also for individuals wherein a total of AED. 500 thousands or more is transferred into their accounts within a period of maximum six months.

Procedure two: Providing the agency with Suspicious Transactions Reports (STR) in each case where a transfer of AED. 40,000 or more is received from the Kingdom of Saudi Arabia to be paid to the beneficiary in cash.

Procedure three: When receiving a remittance or a demand draft from the Kingdom of Saudi Arabia in an amount of Riyals (100) one hundred thousand or more you must obtain a Certificate of Remittance from the remitting bank (or the financial entity) / issuer of the demand draft in the Kingdom (as per the attached format of the certificate) or otherwise the remittance must be returned and the demand draft not to be encashed. Likewise if items 4 or 5 are ticked on the certificate, the remittance must be returned and the demand draft not to be encashed.

Procedure four: To bar certain accounts from receiving any transfers from the Kingdom of Saudi Arabia, in order to avoid abuse of these accounts. (U.A.E will provide us with a list of these accounts later).

Procedure five: To decline opening of accounts for Saudi nationals if third parties would be given Power of Attorney to operate the account, except in certain cases subject to Central Bank prior approval.
1.2.1.5.2 Offshore Companies

An offshore company is a company which does not conduct substantial business in its country of incorporation. They are sometimes known as non-resident companies. In other words it is a company that is registered in a country other than the one in which it conducts most of its business, usually for tax purposes.

Because of the limited amount of publicly available information in connection with offshore companies, there is usually a high level of hidden costs at the administrative level.

For example, to open a bank account in the name of an offshore company, and to comply with relevant anti-money laundering regulations, the bank will normally require large quantities of corporate documentation to be notarised and apostilled in the jurisdiction of incorporation, and may require opinions from local lawyers in that jurisdiction as to the capacity and power of the company to open and operate a bank account.

Any reasonably sophisticated money launderer will establish a bank account in a financial haven as a corporation rather than as an individual with a "numbered account". To increase the appearance of legitimacy, it is preferable that such a company already has a history of actual activity. Once the corporation is set up, a bank deposit is then made in the haven country in the name of that offshore company.

The incentive for businesses to be registered in offshore havens is to escape the severe tax and registration regulations on domestic companies. They can funnel large amounts of capital to and from offshore countries without the need to declare the transactions to domestic fiscal authorities.

On the condition that it does no business where it is set up, having an international business (IBC) or "offshore" corporation enables its owners to act with complete anonymity and not pay taxes.

In many jurisdictions it is not even required to keep corporate books or records and thus is perfect for concealing the origin and destination of goods in international commerce. Companies can even be capitalized with bearer shares, so that while there is no owner on record anywhere, the person who physically possesses the share certificates owns the company.

In general, but of course not always the case, “domestic customers” may be at a lower risk due to the easy availability of information and verification about such customers. Offshore customers, who do not have a domestic business or residence, should be treated at a higher risk as the ability to obtain and verify information about such customers may be limited.

Offshore customers also should be classified in terms of their country of origin. This is because the level of anti-money laundering regulation and enforcement varies considerably from country to country.
1.2.1.5.3 Insurance Companies

Insurance company is a company or corporation whose business it is to insure against loss, damage, or death.

The U.A.E Ministry of Economy and Planning has issued regulations to insurance companies/ brokers and accountants/ auditors in the UAE, detailing the customer’s identifications and suspicious transactions reporting requirements.

In addition to this, important regulations were jointly produced by FinCEN (Financial Crimes Enforcement Network) and U.S. Treasury as 31 C.F.R. 103.137 on December 5, 2001 and largely focus on requiring insurance companies to form anti-money laundering programs.

The following information/documents must be collected and retained:

a) Proof of legal existence of Applicant company:
   ➢ Trade License (if relevant in country of incorporation)
   ➢ Certificate of Incorporation
   ➢ Memorandum and Articles of Association
   ➢ Board Resolution permitting authorized signatories’ application.

b) Proof of Applicant company’s physical address in country of origin and physical address within the UAE (when applicable):
   ➢ Original utility bill
   ➢ Copy of lease/purchase agreement
   ➢ Original statement from a financial institution
   ➢ Letter from public authority or external auditor.

c) Contact details of Applicant Company:
   ➢ Office telephone number(s)
   ➢ Office fax number(s); and
   ➢ Office email address; and
   ➢ Website address.

d) Names and addresses of all controlling individuals of the Applicant Company and its assets.

e) Declaration by authorized signatories of the Applicant Company that the beneficial owners mentioned in (4) are the sole beneficial owners of the Applicant Company. (In case of Applicant Company being non publicly traded)

f) Identities and addresses of all signatories of Applicant company the expression ‘Controlling Individual’ here means a shareholder, beneficial owner or a manager.
(g) Identities and addresses, if different to those at (4) and (6), of:

Individuals holding Powers of Attorney from Applicant company;
Third party mandate holders of Applicant Company

(h) Understanding the relationship that exists between the principals of the applicant company and the powers of attorney/third party mandate holders.

(i) Names and address of all partners in partnerships

(j) Details of Applicant company’s previous business including:
   - Main products; and
   - Name and address of previous business; and
   - Main customers and suppliers; and
   - Main activities geographical areas; and
   - Volume of activities over last two years.

(k) Indication of the anticipated volume and type of activity to be conducted by the Applicant company.

(l) Understanding the source of funds originating from the Applicant company.

(m) First class bank reference whereby Applicant company has been known to the issuing bank for at least two years.

(n) Last two years audited Applicant company financial statements.

(o) External Auditors name and address.

1.2.1.5.4 Money Exchangers

Under the Federal Law No. 4, the U.A.E. Central Bank has issued Anti-Money Laundering Regulations which reflect the Forty Recommendations on combating Money Laundering, and the Eight Special Recommendations on combating Terrorist Financing, issued by Financial Action Task Force (FATF) established by G7 countries.

Financial Institutions including Money Services providers licensed to operate in the U.A.E. are legally liable to comply with these regulations requiring but not limited to; due diligence checks, monitoring of financial transactions to detect and report possible money laundering transactions.
Accordingly, every Money Exchanger must take the necessary procedural and control measures to provide its support in the fight against money laundering and the financing of terrorism.

These measures are summarized as follow:

1. Ascertainment of customer identity
2. Establishment of ultimate beneficial owner of funds
3. Enhanced know your customer/due diligence
4. Internal Reporting of Unusual /potentially suspicious transaction
5. Reporting of unusual / suspicious transactions
6. Staff Training
7. Internal security measures - Know your staff
8. Confidentiality of records and suspicious transactions
9. Internal Audit’s role

1.2.1.5.5 Shell Companies

The term “shell company,” as used herein, refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little to no independent economic value. In other words, it is a company that has no independent assets or operations of its own, but is used by its owners to conduct specific business dealings or maintain control of other companies.

As noted in the 2005 U.S. Money Laundering Threat Assessment, shell companies have become common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate.

The use of shell companies provides an opportunity for foreign or domestic entities to move money by means of wire transfers or other methods, whether directly or through a correspondent banking relationship, without company owners having to disclose their true identities or the nature or purpose of transactions. A review of Suspicious Activity Report data reveals that shell companies in the United States have been used to move billions of dollars globally.

The following elements are cited repeatedly in Suspicious Activity Reports involving shell companies:

a) An inability to obtain – whether through the Internet, commercial database searches, or direct inquiries to the foreign correspondent bank whose

customer is the originator or the beneficiary of the transfer – information necessary to identify originators or beneficiaries of wire transfers.

b) A foreign correspondent bank exceeds the anticipated volume projected in its client profile for wire transfers in a given time period, or an individual company exhibits a high amount of sporadic activity that is inconsistent with normal business patterns.

c) Payments have no stated purpose, do not have reference goods or services, or identify only a contract or invoice number.

d) Goods or services of the company do not match the company’s profile based on information previously provided to the financial institution.

e) Transacting businesses share the same address, provide only a registered agent’s address, or raise other address-related inconsistencies.

f) An unusually large number and variety of beneficiaries receive wire transfers from one company.

g) Frequent involvement of beneficiaries located in high-risk, offshore financial centres.

h) Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.

Providing services to shell companies involves varying degrees of risk, depending on the ownership structure, nature of the customer, the services provided, purpose of the account, the location of services, and other associated factors. The potential to abuse shell companies for illicit activity must be recognized, and financial institutions/banks must be vigilant in monitoring such companies on an ongoing basis.

Financial institutions/banks are expected to assess the risks involved in each shell company relationship and take steps to ensure that the risks are appropriately and effectively identified and managed.

Accordingly, all financial institutions/banks should review their anti-money laundering and, as appropriate, suspicious activity reporting programs to ensure that internal policies, procedures, controls, systems and training programs are
designed to prevent, detect, and report possible money laundering and other financial crime involving shell companies.\textsuperscript{6}

If a financial institution/bank discovers suspicious activities such as those listed above and knows, suspects or has reason to suspect the transactions involve the use of the country or foreign-based shell business entities to launder illicit funds or to enable the furtherance of a crime, the institution/bank must file a Suspicious Activity Report in accordance with the suspicious activity reporting regulations and use the narrative to completely and sufficiently describe the suspicious conduct.

The financial institutions/banks should provide all required and relevant information about the conductor(s) and transactions, including, as applicable, the names and account numbers of all originators and beneficiaries of domestic and international wire transfers, the names and locations of shell entities involved in the transfers, and the names of and information regarding any registered agents or other third parties.\textsuperscript{7}

\textbf{Note:} It is strictly prohibited to have relationship directly or indirectly with institutions that have no physical presence (Shell banks & companies).\textsuperscript{8}

\textit{1.2.1.5.6 PEP-FPEP}

\textbf{1.2.1.5.6.1 Definition}

PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations [and] important party officials’….etc.

FATF notes that business relationships with family members or close associates of PEPs involve reputational risks similar to those involved with PEPs themselves and extends its definition to include those categories.

\begin{center}
An effective compliance program also should include screening shell companies for possible OFAC-related sanctions references, while also getting assurances from a shell company representative that the principals of the company have been screened as well. For guidance on complying with OFAC-related sanctions, financial institutions should refer to the Foreign Assets Control Regulations for the Financial Community available at: [http://www.treas.gov/offices/enforcement/ofac/regulations/t11facbk.pdf](http://www.treas.gov/offices/enforcement/ofac/regulations/t11facbk.pdf).
\end{center}

\begin{enumerate}
\item [4] \textsuperscript{6}
\item [7] \textsuperscript{6}
\item [8] \textsuperscript{6}
\item [8] Amendment of circular 24/200-date 17/06/2008
1.2.1.5.6.2 What are the risks?

PEPs have been recognized as a particular money-laundering risk because of their perceived connection with corrupt (or financially irregular) regimes. In its 2003-04 Typologies Report, FATF provided case studies of the involvement by PEPs in money laundering and observed that:

The source for the funds that a PEP may try to launder are not only bribes, illegal kickbacks and other directly corruption-related proceeds, but also may be embezzlement or outright theft of State assets or funds from political parties and unions, as well as tax fraud. In certain cases PEP may be directly implicated in other types of illegal activities such as organized crime or narcotics trafficking.

PEPs that come from countries or regions where corruption is endemic, organized and systemic seem to present the greatest potential risk; however, it should be noted that corrupt or dishonest PEPs can be found in almost any country’.

Basic procedures to be applied before opening any PEP account:

**Step one:** Have appropriate risk-based procedures in place to determine whether a customer is a PEP.

**Step two:** Obtain appropriate senior management approval for establishing or maintaining business relationships with such customers.

**Step three:** Take reasonable measures to establish the source of wealth and source of funds of such customers.

**Step four:** Conduct enhanced ongoing monitoring of the business relationship.9

**Note:** As for the FPEP: the addendum of circular 24/2000 dated 17/06/2008, set the following new regulations to be applied:

**Definition:** A FPEP is defined as a senior official in the executive, administrative, military, or judicial branches of a foreign government, immediate family members, and close associates.

**Procedures**

Having systems and controls in place to determine whether a potential customer, an existing customer, or the beneficial owner is a FPEP.

**Setting procedures for obtaining written approval from senior management to open FPEP’s accounts.**

The AML Department follows similar procedure to the ones applied for the PEP.

1.3 Chapter three: Definition & reasons of M L.

1.3.1 Definition

Money laundering is the name given to the process by which illegally obtained funds are given the appearance of having been legitimately obtained. Money laundering is a process whereby the origin of funds generated by illegal means is concealed (drug trafficking, gun smuggling, corruption, etc.). The objective of the operation, which usually takes places in several stages, consists in making the capital and assets that are illegally gained seem as though they are derived from a legitimate source, and inserting them into economic circulation. Money laundering is not a new phenomenon: it's as old as crime itself. Criminals have always endeavoured to conceal the origin of illegally generated funds in order to erase all trace of their wrongdoings. Nevertheless, the forms and dimensions of this type of crime have evolved in recent years. Since the seventies, the escalation of the drug market and globalization of organized crime have led to a collective raised awareness with regard to the problem of money laundering.

1.3.2 Why do criminals launder money?

**Reason one:** Hide Wealth: Criminals can hide illegally accumulated wealth to avoid its seizure by authorities.

**Reason two:** Avoid Prosecution: Criminals can avoid prosecution by distancing themselves from the illegal funds.

**Reason three:** Evade Taxes: Criminals can evade taxes that would be imposed on earnings from the funds.

**Reason four:** Increase Profits: Criminals can increase profits by reinvesting the illegal funds in businesses.

**Reason five:** Become Legitimate: Criminals can use the laundered funds to build up clean businesses and provide legitimacy to their business.
1.4 Chapter four: The stages of Money Laundering

1.4.1 **Stage one: Placement**
The first stage is called Placement. At this stage, illegal funds or assets are first brought into the financial system. When illegal funds are placed in the financial system, they become more liquid.

1.4.2 **Stage two: Layering**
It is the process of distancing the placed funds from their illegal origins. At this stage, money launderers use many different techniques to layer the funds. These techniques include use of multiple banks and accounts, use of professionals who act as intermediaries and use of corporations and trusts. The funds may be shuttled through a web of many accounts, companies, and countries in order to disguise their origins.

1.4.3 **Stage three: Integration**
At the Integration stage, the laundered funds are made available for investment in legitimate or illegitimate businesses. At this stage, the illegal money has achieved the guise of legitimacy.
1.5 Chapter five: Consequences of Money Laundering:

1.5.1 Consequence one: Finances Terrorism
Money laundering provides terrorists with funds to carry out their activities. The 9/11 attacks on the Twin Towers in the USA were enabled through laundered funds.

1.5.2 Consequence two: Undermines Financial System
Money laundering expands the black economy, undermines the financial system, and raises questions of credibility and transparency.

1.5.3 Consequence three: Expands Crime
Money laundering encourages crime because it enables criminals to effectively use and deploy their illegal funds.

1.5.4 Consequence four: Criminalizes Society
Criminals can increase profits by reinvesting the illegal funds in businesses

1.5.5 Consequence five: Reduces Revenue and Control
Money laundering diminishes government tax revenue and weakens government control over the economy.
1.6 Chapter six: Know your correspondent bank (KYCB) and employees

1.6.1 KYCB

According to ACAMS International Glossary of Key Money Laundering Terms and Acronyms, the term 'know your correspondent bank (KYCB)' is used to describe a set of money laundering control policies and procedures employed in determining the beneficial owners of a respondent bank and the type of activity that will be 'normal and expected' for this bank.

'Know your correspondent bank' is a key tool in detecting suspicious activity and money laundering activity because correspondent accounts are often used as conduits to launder criminal proceeds in international settings. The USA Patriot Act of 2001 enacted a number of statutory provisions that bear directly on the procedures U.S. financial institutions must follow in connection with their foreign correspondent banks.

Know Your Correspondent Bank’ is now a duty because of the heavy risks under new laws and regulations. For Example: Dealing with shell banks that have no physical presence in any jurisdiction is prohibited in the U.S. Payable-through accounts that serve foreign banks are fraught with money laundering risks.

1.6.2 KYE

Know your customer and your employee is the heart of AML. The increased risks now facing all financial institutions make it essential they have sound “Know Your Customer” policies and procedures. Recent cases have elevated “Know Your Employee” to a major role. An improperly screened employee can cause as many problems as a bad customer. KYC and KYE involve the entire institution, including human resources and security departments and board of directors.

---

10 SEE ANNEX
11 Know your correspondent bank
12 Know your correspondent field
13 Emphasized in complete chapter in section two.
2 Section Two: Procedural AML Practices

2.1 Chapter one: Compliance/AML Organizational Structure

2.1.1 Risk Management

2.1.1.1 Types of risks

There are three main types of risk handled by the risk management in banks. These risks are as follows:

2.1.1.1.1 Credit risk
The potential financial loss resulting from the failure of customers to honour fully the terms of a loan or contract. Increasingly, this definition is being expanded to include the risk of loss in portfolio value as a result of migration from a higher risk grade to a lower one;

2.1.1.2 Market risk
The risk to earnings arising from changes in interest rates or exchange rates, or from fluctuations in bond, equity or commodity prices. Banks are subject to market risk in both the management of their balance sheets and in their trading operations.

2.1.1.3 Operational risk
The potential financial loss as a result of a breakdown in day-to-day operational processes. Operational risk can arise from failure to comply with policies, laws and regulations, from fraud or forgery, Money Laundering, or from a breakdown in the availability or integrity of services, systems or information14.

After summarizing the definitions of the above mentioned risks, we will focus on one Risk which is in various cases a result of deficient Anti Money Laundering procedures.

This diagram below summarizes what lies beneath the operational risk

14 Elmer Funke Kupper *-Risk Management In Banking
OPERATIONAL RISK

TRANSACTION RISK
- Transaction risk
- Execution error
- Booking error
- Settlement error
- Commodity delivery risk
- Documentation/contract risk

OPERATIONAL CONTROL RISK
- Exceeding limits
- Rogue/Dishonest trading
- Fraud
- Money laundering
- Security risk
- Key personnel risk
- Processing risk

SYSTEM RISK
- Programming error
- Model/methodology error
- Mark-to-market error
- Management information
- IT systems failure
- Telecommunications failure
2.1.1.2 AML/Compliance Staff

BLOM Bank France is structured in the following way:

Three main departments report directly to the Risk Manager:
a. Anti Money Laundering Department
b. Legal Department
c. Credit Administration Department

The AML Department is structured as follows:

2.1.1.3 Central /Branch –Compliance-AML Department

The Risk Management is based in Dubai branch, accordingly the Central AML Department is based in Dubai.
This department is constituted of the AML Head and two AML Administrators. Sharjah AML department, which reports to Dubai AML Head, is constituted of two AML Administrator.
2.1.1.4 AML/Compliance Department Responsibilities and General Internal Procedures.

AML Department’s main mission, in summary, is composed of two main responsibilities:

To advance the professional knowledge, skills and experience of the AML Compliance Staff for the detection and prevention of international money laundering, to promote the development and implementation of sound anti-money laundering policies and procedures, and to ensure full adherence.

To implement Know-Your-Customer procedures, to perform background investigation on customers and transactions based on internal and public information and to monitor and trace money/funds channeled through customer accounts in order to identify suspicious activity (if any), process Suspicious Activity Reports (SAR) internally, and report results to the competent authority. To cooperate with regulatory authority on any on-going investigation involving any account holders.

In order to ensure the above responsibilities the AML Department Head should:

Receive new rules and regulations from the Bank’s Risk Management and from the Governmental entities (including the Central Bank) concerning fraud detection and anti-money laundering practices.

Ensure that the information is passed to employees through Department Heads. Identify contradictory jurisdictional risks dependent on legislation, regulation, and secrecy laws, continuous review of the FATF recommendations and other initiatives of the BASEL due diligence principles.

Manage and supervise the AML Department in Dubai and Sharjah Branch.

To provide training to the staff of AML, both in Dubai and Sharjah Branches, and the rest of the Bank employees; to inform them and / or update their information in order to prevent fraud and anti-money laundering problems.

Ensure that required information is available for all customers, in Dubai and Sharjah Branches, and that the KYC form is properly filled, signed, and renewed as required.

Ensure that customer’s declarations should be transparent. Should the AML/Compliance Head feel unconvinced with the statements provided or if the customer refuses to give the required details, the account opening or the relationship must be rejected/ended.

Control bank operations, question employees and supervisors on suspected issues/clients that disrespect bank rules and regulations and prepare accurate reports to the Risk Manager in order to take appropriate action such as closing of account or to report any suspicious transaction to the Anti-Money Laundering unit with Central Bank of the U.A.E.
Coordinate with Governmental entities; including the sharing information, preparing needed reports, and taking necessary actions according to the sector practices.

Note: the circular 24/2008 was amended on the 17th of June 2008 emphasizing the following regulations

Compliance officers should:

- Go through the fit and proper test.
- Screen all the employees in areas related to AML. Their function should be subject to an independent audit function, and the internal audit function should ensure that such audits are carried out periodically and reports are submitted to the chief executive.
- Undergo periodical training, in addition to in-house-frequent training to conduct case studies, keeping in view life cases, related to ML & TF STRS.
2.2 Chapter two: AML Department – Detailed Practical Procedures (Dubai and Sharjah Branches)

In order to open any account, every customer has to approach the AML Department. The AML Department distinguishes two account categories, Individual Account and Company’s account.

2.2.1 Documents required before opening any account

Every category mentioned above has basic requirements which should be satisfied before the account opening final decision. The requirements are as follow:

2.2.1.1 Individual account:

- Passports- valid date –ID for Locals
- Resident visa- if the customer is a resident in emirates-valid date.
- Specifying the kind of transactions the account will be opened for.(Especially if the individual account will show corporate and business transactions-entrepreneur).
- The currency.
- Type of account (current-saving-time deposit).
- A letter indicating the nature of business of the customer, job description-salary certificate, trade license etc….
- Last bank statement (6 months)
- Tel #, fax #, email address of the customer as well as Mail address P.O.Box.
- DEWA / SEWA\textsuperscript{15} Bill or leasing contract.

2.2.1.2 Company’s account:

- Trade license-original copy. In case the company is registered outside the U.A.E, this copy has to be authenticated by the Ministry of Foreign Affairs in the mother company and the U.A.E Consulate in addition to the U.A.E Ministry of foreign affairs.
- The memorandum of association (authenticated if the company is registered outside the U.A.E).
- A resolution provided by the Board of Directors giving the Chairman or the General Manager or any person chosen the power to open an account on the

\textsuperscript{15} Dubai Electricity Water Authority/Sharjah Electricity Water Authority.
behalf of the company and operate all its transactions. (Also it has to be authenticated in case it is registered outside the U.A.E).

- Last balance sheet of the company.
- Invoices and contracts signed by the company and third parties which reflect mostly the core business of the company as well its financial status.
- Last 6 months bank statement of the company’s account as well as for the main shareholders in the company.
- Full description of the business of the company.
- Purpose of opening the account in our bank.
- The expected financial flow of the company’s account in our books.
- Passport copies and resident visas (in case they are resident) of all the shareholders; partners; managers….
- Tel #, fax #, email address, mailing address P.O.BOX of the company and the share holders.
- DEWA/SEWA bill or leasing contract.

2.2.2 Account opening procedures (Dubai and Sharjah):

2.2.2.1 BLOM Bank France-UAE

After satisfying the above mentioned requirements, the following procedures are applied:

**Step one:** Client fills the questionnaire form then signs it\(^\text{16}\).

**Step two:** Client fills in and signs an account application form (Contract)\(^\text{17}\).

**Step three:** He/She mentions the type of account (s) to be opened.

**Step four:** In case the Client wants to send instructions by fax/email, he/she fills in and signs a “Fax Standing Instructions” form\(^\text{18}\).

**Step five:** In case of Time Deposit/saving, Client fills in and signs an additional application (specified for time deposit accounts /Savings).

**Step six:** In case of joint account, client fills additional form for joint accounts knowing that there are two joint account forms (And-And/Or).

**Step seven:** Client signs the signature card.

\(^{16}\) See annex
\(^{17}\) See annex
\(^{18}\) See annex
**Step eight:** In case the customer or the company wants to grant a power of attorney to a third party, the principal and the attorney sign additional form titled Power of Attorney form.

**Step nine:** In all cases, AML/Compliance Dept must check the original ID and stamp the copy “original seen”. All the received documents have to be dated.

**Step ten:** In case of personal account, Dubai AML dept checks the customer’s and the authorized signatories’ names in the OFAC list program. While Sharjah AML Dept. sends Dubai AML Dept the names in order to be checked.

**Step eleven:** In case of corporate accounts, Dubai AML Dept checks the company’s, shareholders, and the authorized signatories’ names in the OFAC List Program. While Sharjah AML Dept send the required to Dubai to be checked.

**Step twelve:** In case of corporate accounts, AML Departments have to ensure Identifying & obtaining satisfactory evidence on the identity of the beneficial owners of companies and business opening accounts or remitting money. And understanding the ownership and control structure of all legal entities, in addition to ensuring that every person who is acting on behalf of another must have proper legal authority to do so.

**Step thirteen:** In case of corporate account, the client must submit the original trade license and all related documents, the AML Dept takes copies after stamping it original seen, and writing the date on it.

**Step fourteen:** For corporate clients AML Dept sends Legal Department the application and the legal documents for taking the legal point of view.

**Step fifteen:** Legal Department checks documents and returns sets of documents to AML Dept (CAH).

**Step sixteen:** The AML Dept. prepares the data entry form and sends it for approval to both the Branch and Risk Managers.

**Step seventeen:** After approval, AML Dept sends all the account application forms to Customer Service/Current Account Head.

**Step eighteen:** CAH checks all the application and hands them over to CAH Assistant (CAHA) based on the Account opening application form (s) as well as the other documents, CAH assistant or clerk opens the account in the ICBS.

**Step nineteen:** After being opened and activated on the system, CS/CA Dept send the file to the AML Dept for finalizing the official KYC form.

---

19 Amendment of circular 24/2000.date 17/06/2008
20 Current Account Head
21 Customer Service/Current Account
22 See annex: KYC forms
**Note 1:** In case of any additional feedback required for A/C opening formalities and procedures in Sharjah Branch, AML Head is contacted.

**Note 2:** In order to open the account, customer may approach UAE branches directly or any BLOM foreign branch.

### 2.2.2.2. Steps for opening accounts at Blom Bank SAL –Lebanon and BSO (Bank of Syria and Overseas) - Dubai and Sharjah Branches.

Customers who wish to benefit from our inter-banking communication between our UAE and Lebanon/Syria branches usually resort to the AML department for account opening.

Note: In Sharjah Branch, customers may come to the executive secretary in addition to the AML Department to open these accounts.

The documents required for account initiation is similar to those needed for Blom Bank France UAE. When approached by a customer, he is requested to start filling the A/C opening forms either in Arabic or English whichever suits his needs. The customer is requested at first to choose the type of account needed, which are illustrated below:

- A Check/time deposit account (current)
- A blocked/sight savings account (saving)
- A joint account
- A collective account
- A secret time deposit account
- A secret joint time deposit account

After selecting the appropriate type, the client is asked to choose the branch and write down his name on the first page. After doing so, he is requested to sign and write the date at the bottom of the page.

**Note:** The customer is requested to sign and write the date at the bottom of each page, along with writing down the phrase “Read and Approved” if instructed by the footer of the A/C opening page.

Also, all the customers are requested to sign and write the date on the pages titled:

- “Central Office for Credit Risk” 
- نظام المصلحة المركزية للعملاة المتخلفين عن
- “الإيفاء"
The customer has to proceed after signing the necessary pages along with the abovementioned pages, to fill the “Information About the Client” page located in the end of the booklet (2 sided page).

Finally, our client has to sign the two specimen signature cards at the end of the A/C opening booklet, on both sides (left and right). The AML Staff present at time should write his name and sign on the bottom of the signature card. The documents should be attached in the end of the A/C opening booklet.

The head of compliance should attach an introduction letter, introducing the customer, and declaring that the information was filled, and signed during his presence, and forward it to the concerned branch.

Similar procedures apply for other BLOM Branches.

Note: Sharjah Branch assists in account opening formalities for our branches in Lebanon, Jordan and Syria. For other overseas branches, customers are requested to complete the necessary formalities at Dubai Branch.

2.2.3 When the signatory information is required? (Dubai and Sharjah).

Verification of a signatory's identity is required both when a new account is opened and when a signatory changes on an existing account. Required signatory information is the same as any new individual customer.

2.2.4 Account Renewal procedures (Dubai and Sharjah):

Step one: In case of renewal, Customer is contacted by either Current account Dept or AML Dept.

Step two: when the customer approaches the bank personally for account renewal, he signs new account opening forms infront of the CA Department.

Step three: Second, customer personally approaches the AML Dept., he fills new questionnaire, and answers the updating AML Questions.
Step four: AML Dept. updates the account’s KYC accordingly²³.

Step five: In case of contacting the customer by phone or email, we acquire all necessary information.

Step six: In case an old customer is unreachable by any means, AML Dept. investigates other related accounts and check the required information. If dissatisfied, the 181 (Etisalat phone central) is contacted, to check any contact details accordingly an email or fax is sent. In case of failure AML Dept. set the alarm note on the ICBS system. Finally AML Dept. sends letters to the customer’s P.O.Box (in case available or valid), requesting the required information.

Step seven: In the renewal process, all mentioned information applicable to new KYCs have to be stated, in addition to the analytical study of the account movement in general, AML Dept makes sure that it is satisfactory, logical, and complying with the information taken, especially line of business, highlighting the customer’s source of income in general.

Step eight: In all cases, once AML Dept. finishes a KYC, the KYC is circulated to the AML Head, the Branch Manager, and Risk Manager for signature.

Step nine: After being signed, the KYC is updated in the ICBS by the AML Head.²⁴

Step ten: AML Head sets the Inward Transfers’ category in addition to the cash deposit ceiling based on the financial flow of the clients’ business and the account average report.

Step eleven: Every KYC is normally valid for a maximum period of two years, depending on the clients’ profile, which is continuously checked and reviewed and amended accordingly.

2.2.5 Special case: Companies Under Establishment

Some clients approach the bank to facilitate their company’s establishment especially issuing a Capital certificate for companies. Accordingly, these steps should be taken:

Step one: Open an account for the company after following the regular AML procedure explained in the manual in 2.2.1.

Step two: The customer should deposit the capital amount in his account.

Step three: Inform customer service department in order to freeze the capital and to deduct the fees from the company’s account as follows:

---

²³ See annex-Renewal KYC form
²⁴ See annex- the updating ICBS page
300 AED For Free Zone Companies
- 600 AED For Limited Liability Companies

**Step four:** The whole file should be given to the legal department in order to study the case and specify the number of shares for each shareholder.

**Step five:** The secretary will type the certificate according to the lawyer’s instructions.

**Step six:** The certificate will be signed by the Branch Manager/Authorized Office.

**Step seven:** 4 copies should be kept as follows:
- One copy should be signed by the customer when he receives the original certificate and this copy is kept in a separate file in the AML Dept.
- Copy with the legal department
- Copy with the Financial Control Department.
- Copy with the Customer Service Department.

**Step eight:** Customer Service Department will not release the capital’s amount until the original Trade License is issued and brought in front of either the AML Dept or the legal Department for signing it and stamping it with an original seen stamp.

### 2.2.6 **Documents required after the account is opened.**

Always AML Dept makes sure that every financial transaction in the account flow of the customer has to be complying with the facts and information supported and taken during the interview and of course translated into a complete KYC.

Every time a transaction exceeds the expectations mentioned in the KYC, satisfactory and supportive documents have to be requested from the customer in order to approve the transaction.

In case of non cooperative customers, case has to be reported.

Examples of documents requested:
- Invoices
- Contracts
- Bills
- Balance sheets
2.3 Chapter three: Know Your Customer (Dubai and Sharjah Branches):

The objective of Know Your Customer policy is to look past the appearance of the customer and obtain visibility into the sources of the customer's money. Customer Acceptance and Customer Identification are two related processes that help create this visibility.

Knowing your customer well, may prevent damage to the bank's reputation and avoid fraud or excessive risk in financial transactions involving the customer.

2.3.1 KYC Policy elements:

KYC policy has three major elements:

2.3.1.1 Customer Acceptance
The basic objective of this policy is to identify the sources of the customer's money, Customer Acceptance involves understanding:

1) The Customer (individual, company, bank, etc.),
2) The type of account
3) The country of origin.

2.3.1.2 Customer Identification:
Establishing the identity of customers is central to the KYC policy both for the customer acceptance or rejection decision and for the ongoing monitoring of customers' accounts and transactions, and to classify the customer and build the appropriate information base and documentation in relation to the customer. By doing this, comfort can be obtained that legitimate customers are being dealt with; in addition to this, ‘base line’ of documented information can be created to monitor future transactions.

2.3.1.3 Accounts and Transactions Monitoring:
In an effective KYC policy, customer accounts and transactions are properly classified in terms of risk and are regularly monitored. (Emphasized later).
2.3.2 **Customer’s Interview basics:**

Interviewing the customer must assure the following principles:
- Conducting on-going customer due diligence CDD on the business relation ship.
- Obtaining information & undertaking another customer due diligence when the accuracy is doubted.
- Establishing the purpose and intended nature of the business relation ship while entering a banker-customer relation ship.
- Undertaking CDD for every account opened prior to 14/11/2000 to ensure that there are no risks in continuing such relationships\textsuperscript{25}.

The important elements to be taken into consideration during the interview with the customer are:

- Customer’s abnormal behaviour
- Customer’s origins
- Source of income and funds
- Line of business / financial exposure
- Risks
- The transfers he/she expecting to receive. when, where, how much, and why?

2.3.2.1 **Customer’s Abnormal Behaviour**

Customers’ Abnormal behaviour can also be a tip-off for suspicious activities. Look for such abnormal behaviour keeping in mind your customer's normal behaviour:

- Nervousness or erratic actions
- Problem in producing correct identification
- Provision of unusual explanations
- Failures to provide explanations
- Comments regarding suspect origins or activities

\textsuperscript{25} Ammendment of circular 24/200-date 17/06/2008
2.3.2.2 Origins
The geographical origins of the customers may involve different levels of risk.

A customer may have several origins. In the case of an individual, it could mean country of citizenship, place of birth or principal place of residence or business. In the case of a corporation, it could mean jurisdiction of incorporation or regulation, principal place of business or location of principal assets.

In general, but of course not always the case, domestic customers may be at a lower risk due to the easy availability of information and verification about such customers. Offshore customers, especially the ones who do not have a domestic business or residence, should be treated at a higher risk due to the limited ability to obtain and verify information about such customers.

Offshore customers should be classified in terms of their country of origin. This is because the level of anti-money laundering regulation and enforcement varies considerably from country to country.

2.3.3 KYC Content:
Step one: Clear translation of the supportive documents explained in the previous paragraphs.
Step two: Nationality, residency status.
Step three: Complete and thorough addresses, contact details including emails-line of business and source of income.
Step four: The purpose of opening the account.
Step five: The reason of opening the account at our bank.
Step Six: The account flow future expectations.
Step seven: Exposure to another account or group of accounts.
Step eight: Banking relations and statements (BLOM overseas or another bank’s customer in case of bank overseas customer, cooperation between branches has to be effective and satisfactory).
Step nine: Facilities, in case granted.
Step ten: Mentioning the documents provided.
Step eleven: Internet pages selected to support the customer’s declarations.
Step twelve: Economic Sector.
Step thirteen: Content of the email sent to the AML Unit abroad.
(explained below in the notes-No.5)
**Step fourteen:** OFAC list: making sure that the customer (personal or corporate) is not mentioned in the OFAC list.\(^{26}\) (the same goes for the shareholders in a corporate account).

**Step fifteen:** In case of KYC Update: Average report of the past year should be mentioned for cash deposits, cash withdrawals, Inward transfers, and outward transfers.

**Notes**
1) Always AML Dept makes sure the customer is not blacklisted.
2) PEP/FPEP Customers are set in a category with special procedures-(will be discussed later in the manual).
3) In Dubai Branch, KYCs are signed by the AML Head, Risk Manager, and Branch Manager.
4) In Sharjah branch, KYCs are signed by AML Administrator and the Branch Manager.
5) In case the customer (personal, corporate) deals with any other BLOM Branch round the world, an email is sent to the AML Unit in the correspondent branch requesting a complete KYC report which could directly affect the account opening decision.

2.3.4 **KYC renewal:**

**Step one:** All mentioned information applicable to new KYCs have to be stated, taking into consideration the updated information.

**Step two:** In addition to the analytical study of the account movement in general, AML Dept makes sure it is satisfactory, logical and complying with the information provided, especially line of business, highlighting the customer’s source of income in general.

**Step three:** AML Dept. should inform in writing (using the data entry form followed when opening any account), the Customer Service Department with any amendment in the KYC information. The category amended should be highlighted on the mentioned form.

**Step four:** Customer Service Dept. amends the categories highlighted in the ICBS.

2.3.5 **Economic Sector:**
The economy may be classified into subdivisions called sectors (also called industries), these sectors maybe divided into sub sectors.
- Personal accounts are categorized into two kinds:

\(^{26}\) Office Of Foreign Assets Control
- Corporate account & Individuals operating business transactions through the bank are categorized according to the line of business, (emphasized in the table below).
This table of sectors, as set by the central bank, for categorizing each account is as follow:

<table>
<thead>
<tr>
<th>Sector code</th>
<th>Sector Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>Staff Blom Bank France</td>
</tr>
<tr>
<td>1010</td>
<td>Cultivation Of Crops</td>
</tr>
<tr>
<td>1020</td>
<td>Poultry Farming</td>
</tr>
<tr>
<td>1030</td>
<td>Fishing</td>
</tr>
<tr>
<td>1040</td>
<td>Agriculture other activities</td>
</tr>
<tr>
<td>2010</td>
<td>Crude Petroleum and Natural Gaz</td>
</tr>
<tr>
<td>2020</td>
<td>Mining Other activities</td>
</tr>
<tr>
<td>3010</td>
<td>Food</td>
</tr>
<tr>
<td>3020</td>
<td>Beverages</td>
</tr>
<tr>
<td>3030</td>
<td>Textile Leather Footwear Cloth</td>
</tr>
<tr>
<td>3040</td>
<td>Furniture Fixture Wood Product</td>
</tr>
<tr>
<td>3050</td>
<td>Paper and Paper Products</td>
</tr>
<tr>
<td>3060</td>
<td>Chemical and Chemical Product</td>
</tr>
<tr>
<td>3070</td>
<td>Petroleum Refining and Chemicals</td>
</tr>
<tr>
<td>3080</td>
<td>Basic Metal Products</td>
</tr>
<tr>
<td>3090</td>
<td>Fabricated Metal Product</td>
</tr>
<tr>
<td>3110</td>
<td>Other Manufacturing</td>
</tr>
<tr>
<td>4000</td>
<td>Electricity, Gas and Water</td>
</tr>
<tr>
<td>5010</td>
<td>Construction Of Building</td>
</tr>
<tr>
<td>5020</td>
<td>Other Construction</td>
</tr>
<tr>
<td>6011</td>
<td>Construction Materials</td>
</tr>
<tr>
<td>6012</td>
<td>Motor Vehicles</td>
</tr>
<tr>
<td>6013</td>
<td>Other Wholesale</td>
</tr>
<tr>
<td>6020</td>
<td>Retail Trade</td>
</tr>
<tr>
<td>7010</td>
<td>Taxi and Other Land Transport</td>
</tr>
<tr>
<td>7020</td>
<td>Water Transport</td>
</tr>
<tr>
<td>7030</td>
<td>Air Transport</td>
</tr>
<tr>
<td>7040</td>
<td>Warehousing and Storage</td>
</tr>
<tr>
<td>7050</td>
<td>Other Transport Activities</td>
</tr>
<tr>
<td>8010</td>
<td>Insurance Companies</td>
</tr>
<tr>
<td>9010</td>
<td>Hotels and Restaurants</td>
</tr>
<tr>
<td>9020</td>
<td>Repair Works</td>
</tr>
<tr>
<td>9030</td>
<td>Recreational Services</td>
</tr>
<tr>
<td>9040</td>
<td>Other Services</td>
</tr>
<tr>
<td>10010</td>
<td>Foreign Government</td>
</tr>
<tr>
<td>10020</td>
<td>Central Government</td>
</tr>
<tr>
<td>10030</td>
<td>Local Government</td>
</tr>
<tr>
<td>11000</td>
<td>Personal</td>
</tr>
<tr>
<td>12000</td>
<td>All Other</td>
</tr>
<tr>
<td>70000</td>
<td>Banks</td>
</tr>
<tr>
<td>8020</td>
<td>Other Financial Institutions</td>
</tr>
</tbody>
</table>
The AML Department mentions the Economic sector on the data entry form and sends it to the Customer Service Department where it is set in the ICBS.

### 2.3.6 Setting the Limits

#### 2.3.6.1 Dubai Branch

Inputs / amendments/cancellation of limits which are mentioned in the KYC of every account are done by the AML Head. This amendment is preapproved by the Risk and Branch Managers who sign the KYCS.

#### 2.3.6.2 Sharjah Branch:

Inputs / amendments/cancellation of limits which are mentioned in the KYC of every account are done by the AML Dept. This amendment is preapproved by the Branch Managers who sign the KYCS.

#### 2.3.6.3 Control:

A report titled “Daily Updates LOG-KYC information” is produced by the ICBS and checked by the AML Head in Dubai for both Branches, and then the Sharjah section is sent to Sharjah Branch for their checking.

#### 2.3.6.4 List of limits:

##### 2.3.6.4.1 Inward /Outward Transfers

New Accounts: these limits are set according to the following criteria: account flow, line of business, financial exposure, the customer’s logical declarations, the customer’s customers, the official balance sheet of the customer’s company…etc

Old accounts under the renewal process: the setting of limits is done according to the keys mentioned above, in addition to a basic thing which is the average reports calculated by the ICBS system.
Table of limits:
This is the table of limits followed in setting up the limits in the ICBS:

<table>
<thead>
<tr>
<th>Client Category</th>
<th>Limit (amount in AED per month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>0</td>
</tr>
<tr>
<td>F</td>
<td>40,000</td>
</tr>
<tr>
<td>E</td>
<td>50,000</td>
</tr>
<tr>
<td>D</td>
<td>100,000</td>
</tr>
<tr>
<td>C</td>
<td>200,000</td>
</tr>
<tr>
<td>H</td>
<td>400,000</td>
</tr>
<tr>
<td>I</td>
<td>800,000</td>
</tr>
<tr>
<td>B</td>
<td>1,100,000</td>
</tr>
<tr>
<td>A</td>
<td>1,800,000</td>
</tr>
<tr>
<td>J</td>
<td>2,500,000</td>
</tr>
<tr>
<td>K</td>
<td>3,000,000</td>
</tr>
<tr>
<td>L</td>
<td>3,600,000</td>
</tr>
<tr>
<td>M</td>
<td>4,200,000</td>
</tr>
<tr>
<td>N</td>
<td>5,000,000</td>
</tr>
<tr>
<td>O</td>
<td>7,000,000</td>
</tr>
<tr>
<td>P</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Q</td>
<td>12,000,000</td>
</tr>
<tr>
<td>R</td>
<td>15,000,000</td>
</tr>
<tr>
<td>S</td>
<td>18,000,000</td>
</tr>
<tr>
<td>T</td>
<td>300,000</td>
</tr>
</tbody>
</table>

2.3.6.4.2 Cash deposits
Cash deposits are set numerically according to the account flow of the customer, in addition to the key points mentioned in 3.6.4.1-new accounts.

2.3.7 Effective KYC-Risk Mitigation
There are five types of risks that an effective KYC policy can help to mitigate

2.3.7.1 Reputation Risks
The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong KYC policy helps to prevent a business from being used as a vehicle for illegal activities.
2.3.7.2 Operational Risks:
Operational risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management, and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If a KYC policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business will be viewed as operationally unsound.

2.3.7.3 Legal Risks:
Legal risk: If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations. Apart from regulatory risk, involvement in illegal activities could lead to third-party judgments and unenforceable contracts. In addition, professionals working within many financial and other professional sectors may also personally be subject to legal action or prosecution. Due to the nature of business, these risks can never entirely be eliminated. However, if a business does not have an effective KYC policy, it will be inviting legal risk. By strictly implementing and following KYC policies, a business can mitigate legal risk to itself and its staff.

2.3.7.4 Concentration Risks:
Concentration risk: This type of risk occurs on the assets side of a business if there is too much exposure to one customer or a group of related customers, or on the same economic sector. It also occurs on the liabilities side if the business holds large concentrations of funds from one customer or group (in which case it faces liquidity risk if these funds are suddenly withdrawn). By implementing an effective KYC policy, a business can identify the entire scope of the asset and liability risk faced in relation to each customer and group of customers.

2.3.7.5 Financial Risks:
If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve any money that the customer owes.27

2.4 Chapter four: Monitoring and Follow up. (Dubai and Sharjah Branches)

Monitoring & spotting the account’s transactions doesn’t exclusively mean the ensured suspicious ones, it also includes the attempted & the unusual ones. The bank has to ensure the reporting of transactions which appear as an attempt to launder money and/or finance a terrorist, terrorist organization and/or terrorist activity. In addition to this, investigating the background and purpose of transactions deemed to be “unusual” and to set forth their findings in writing, even in the event it is not considered necessary to report the transactions to the AMLSCU as suspicious.

In case the findings are documents; they should be maintained for inspection by the competent authorities for a period of at least five years.28

The monitoring should be done by the AML Department, in addition to all bank departments.

This way of combating is composed of the following:

2.4.1 Monitoring the account’s flow of transactions (inward-outward transfers, cash deposits, etc), in general.

2.4.1.1 Foreign Department:
Inward and outward transfers are executed in the foreign department, what the AML Department is concerned about is the following:

Foreign Department Head (FDH) receives instructions as described above from an Account Holder to affect an Outward Transfer. The instructions should include the following basic information:
1. Date
2. Currency and amount in figures and words
3. Beneficiary’s details (Full name and account number or IBAN if in Euros)
4. Beneficiary’s Banker and its full address
5. Details of payment
6. Account Holder’s account number and authority to debit it
7. Authorized signature if instructions are received in writing

Note: The addendum of circular 24/2000-dated 17/06/2008 sets regulations to ensure the following:

28 Addendum of circular 24/2000-dated 17/06/2008
Careful & systematic verification of the identity (name and address) of the remitter in all cases where the value of a transaction reaches AED 2000, or equivalent in other currencies or more for money exchangers AED 3500 in other currencies or more.

Mentioning the name and address of the remitter and either an account number or a unique reference number in the payment instruction.

Effective risk based procedures should be adopted for identifying and handling transfers that lack complete originator in every inward transfers.

2.4.1.2 A Walk-in client

Rule 1: The bank cannot pay walk-in clients/non customers any amount equal or exceeding 10,000 USD received under their name.

Rule 2: The bank should not open an account for the reason of paying the amount received.

Rule 3: The bank can pay such amounts only for existing customers receipt.

Rule 4: All amounts less than 10,000 USD can be paid, after satisfying the following conditions:

Client fills in an application form. She/He fills in the name, Beneficiary Acct no, name and address of the bank, the amount, currency, purpose of payment.

FDC takes photocopy of the Client’s ID.
Client hands over the application form along with the Anti-Money Laundering form to FDC.
2.4.1.3 Customer Service Department:
Customers approach CA/CS Dept. in order to deposit cash and cheques.

Cash amounts below 10,000 AED are deposited at the main counters of the bank.

Cash amounts exceeding 10,000 AED are deposited at the Head teller counter.

2.4.1.4 AML Monitoring (Dubai and Sharjah Branches):
AML Dept. always make sure that every financial transaction in the account flow of the customer has to be complying with the facts and information supported and taken during the interview and of course translated into a complete KYC.

Every time a transaction exceeds the expectations mentioned in the KYC, satisfactory and supportive documents have to be requested from the customer in order to approve the transaction.

In case of non cooperative customers, case has to be reported.
2.4.2 Monitoring strategy:

2.4.2.1 Alarm notification/suspicious transactions:

Any relatively large cash transaction i.e. cash deposit, inward, or outward remittance, as well as cheques deposit will immediately notify assigned heads/managers by an alarm message in the ICBS.

At the 1st stage, an alarm signal will be displayed on the head of portfolio and loans/fixed deposits monitor, who in turn should notify the head of compliance and anti-money laundry. At a later phase, and should the cash transaction involve larger amounts of money, an alarm will be displayed at our branch manager’s screen who as well will contact the head of compliance/AML regarding the specific case.

Consequently, the AML head will contact the customer directly, and inquire about the details of the operation. The client should be requested to provide supporting documents concerning this large transaction, which can take the form of bills, invoices, selling or business contracts, etc… When the compliance head finds the documents adequate enough, the transaction will be processed accordingly.

2.4.2.2 Checking of Reports:

In Dubai Branch: the basic checking is done by the Risk Manager and the AML Dept. there are few reports which are also checked by the Branch Manager- (emphasized below).
In Sharjah Branch: the checking is done by the Branch Manager and the AML Dept., and then it is sent to DUBAI Branch to be rechecked.

2.4.2.3 Checking procedures:

Procedure one: AML Head, Risk Manager and Branch Manager checks, and signs the Money Laundering Report which is circulated on daily basis. This report lists all the transactions which exceeded the account’s limits.

Procedure two: They also check the report which lists all the detailed cash transactions exceeding 40,000 AED, as per U.A.E Central Bank regulations, this report is constituted mainly of:
Account to account transfers.
- cheque withdrawals
- cash deposits
- cash payments for customers at other branch

**Procedure three:** Another similar report is checked by the Risk, Branch and AML Head is the one which lists all detailed cash transactions exceeding 7,500 Euros. (It is composed of the same transactions mentioned in the 40,000 AED report).

**Procedure four:** Report of Transactions exceeding 15,000 Euros is also checked by the same staff, it lists the following:
- Account to account transfers.
- Cheque withdrawals
- Cash deposits
- Cash payments for customers at other branch
- Trust receipts paid
- Draft issuance
- Deposit cancellations
- Cheque settlements
- Export L/C
- Maturity loans
- Cheques account to account
- Inward transfers
- Outward transfers

Every transaction which is suspected must be kept on hold until AML Dept. receives satisfactory documents in support of this transaction, and it has to be directly related to the line of business of the client, company, etc.... These supportive documents have to be either invoices, contracts, selling/buying, contracting...etc. In addition to this, the customer has to provide us with the balance sheet of the company.

**Procedure five:** Report of Large of cash operation greater than 5,000 Euros by clients.

**Procedure six:** Monthly report summarizing all the transactions listed in the reports mentioned above
2.4.3 **Spotting suspicious activity:**

The matter of monitoring the daily transactions is of prime significance. As to the AML department’s concern with this issue, it is mainly focused on the following:
- Cash deposit
- Outward transfers
- Inward transfers

During the daily process of monitoring the daily report, the AML Head/administrator or person in charge develops an idea of the most active daily accounts, which in turn facilitates this process.

Any relatively large amount which exceeds the predefined limit (already set by the AML Head) will be investigated according to the following steps:

**Step one:** Checking the customer’s file/KYC for clues as to whether this particular transaction applies to this case, in terms of line of business, affiliates (local or international), and scale of operations. Example:
A company once received an inward transfer which by far exceeded their limit. Yet, upon reviewing their KYC and previous RPT invoices, it was found that the sender’s reference is widely acclaimed internationally, and that a vital relationship between the parties has been already established.

**Step two:** Checking the TRS/RPT reference number invoice with the foreign department. As said before, links concerning the origin of the payments could be established, as to whether the sender/receiver’s line of business concur, as well as details of payment.

**Step three:** Contacting the customer: Upon unsatisfactory evidence pertaining to the transaction, the person in charge should contact the customer and inquire about the details of the payment. Supporting documents are a must, which may be manifested by invoices, bills, business contracts, whichever fulfills the necessary requirements.

2.4.4 **Credit Department:**

The credit Department has three main roles regarding Anti Money Laundering regulations. This Department has to cooperate with the AML Department informing it with any suspicious or unclear case. These roles are explained in the figure below:
2.4.5 **Swift/OFAC list control:**

**Swift:** Society for Worldwide Interbank Financial Telecommunication.

Due to the increase in worldwide financial activity, terrorism, fraud, and money crimes have all targeted banks worldwide. The increasing risk of doubtful activity triggered a need for effective, as well as efficient monitoring of interbank activity. Software solutions, thanks to today’s technological breakthroughs have much aided in this process, by developing a unique method of matching black – listed names listed on the SDN OFAC directory.

Specially Designated Nationals (SDNs) are organizations and individuals who are restricted from doing business with the United States or American companies, or Americans. This includes terrorist organizations, individual terrorists, and state sponsors of terrorism (such as Iran, and North Korea). The list of specially designated nationals is maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC).

During the process of this monitoring, any violations such as matched names with the OFAC list must be authorized for release by the head of AML/compliance.
department, whereby he/she should precisely compare the names and addresses of the blocked swift message and act accordingly. Any matching case should NOT be released, and must be correctly verified by contacting the concerned people/organization and requesting the necessary identification documents.

Steps:

**Step one:** Swift Messages appear on the system

**Step two:** In case of clear violation, AML Head/Risk Manager blocks the swift message-AML Administrators may block the message upon approval of AML Head or Risk Manager.

**Step three:** The person in charge checks with the foreign Department for details of payments, identities, addresses…etc.

**Step four:** In case of dissatisfaction, the client is contacted for documentary verification.

**Step five:** The swift message may be released upon receipt of satisfactory documents proving a void relationship between the concerned parties.

2.4.6 **OFAC Side Station Program:**

This program is constituted of the following:

- Detection Archive viewer: it helps detecting violation reports
- Event viewer: it lists details of the violation messages (creation date, violation severity, application, and type….etc).
- Report viewers: it lists the complete violation message report.
- Name checker: it checks several fields such as: name, address, city, country. In addition to the violation, its percentage, similarities, category, remarks” such as date, place of birth….etc”.

**Note:** Customers should not be informed of scrutinization of their transactions in any suspicious Money laundering operations and/or terrorist financing\(^{29}\).

\(^{29}\) Addendum of circular 24/2000-date 17/06/2008
2.5 Chapter five: Politically Exposed People
(PEP/FPEP)(Dubai and Sharjah Branches)

A politically exposed person or PEP is any individual having possessed or currently possessing an official government, political, or foreign status. The World Bank, Basel committee, European Union, as well as other renowned worldwide legal legislative authorities all define PEP in a different way. Yet, the common grounds between all is that a PEP is a high risk individual, which should be given primary importance in monitoring or any other financial related activity. The high risk nature originates from well known cause: corruption. Corrupt PEPs have large access to government resources and largely affiliated with a network of foreign government officials and international organized crime, and will unfortunately use these resources for doubtful purposes. The scope of identifying PEP is not simple and straightforward, since any cousin, family member, parent, closely acquainted individual or organization might be considered as PEP.

Given the market conditions in the UAE, many members in the royal family are either shareholders or sponsors for commercial purposes, these members are not actually politically involved, hence these may not be considered as PEP.

2.5.1 Steps in preparing the PEP list
As per the bank’s head office in Paris, a report indicating certain criteria is affected on a monthly basis. This report reflects on an ample side of our politically exposed clientele’s monthly transactions, and is carried out meticulously for both Dubai and Sharjah branches.

2.5.1.1 Step one: Identifying the client
The first step in any account opening procedure is confirming the true identity, which is most of the time corroborated via original identity credentials such as passports. Passports usually indicate the political category if any, by stating that the passport is diplomatic or of government/military nature. As soon as a PEP is identified, it is sorted out under the PEP category, which is given prime importance in terms of monitoring and reporting any conspicuous activity. PEP letters are indicated in capital besides the A/C name, in line of keeping the A/C under scrutiny.
2.5.1.2 **Step two: Inspection**

With reference to the previous report correlating to the previous month’s time period, our clients’ account statements/balances, and monthly average transactions are updated according to the specific time period of the report, which is usually 30 days. By doing so, any sudden trend in any activity will be spotted directly. Beneath is a sample of a single PEP A/C included in the monthly report, indicating up to date balance, and monthly activity in relation to the specified time period.

*(PEP report 10/01/2008 – 10/02/2008)*

<table>
<thead>
<tr>
<th>Sr.</th>
<th>A/c No.</th>
<th>Account Name</th>
<th>Account Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12345</td>
<td>XYZ Customer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>He is a government official.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A/C Opening Date: 30/03/2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>KYC status: Valid till 10/10/2010</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A/c Type</td>
<td>Balance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saving</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Client Term Deposit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A/c AverageTransactions in AED</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transactions</td>
<td>Average</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cash Deposit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cash Withdrawal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inward Transfers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outward Transfers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDC Checks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Checks in clearing</td>
<td></td>
</tr>
</tbody>
</table>

Politically exposed people are sorted out since the beginning of their banking relation with Blom Bank France, in order to assure a safe and smooth flow of operations.

2.5.1.3 **Step three: Reporting**

Every month, a PEP report is sent to the Head Office.

*Note: same procedures are followed for the FPEP.*
2.6 Chapter six: Central Bank Notices

2.6.1 Kinds of Notices:

There are seven kinds of Central Bank notices which are:
1) Court cases
2) Cancellation of court cases,
3) Chequebooks
4) AML1
5) AML2
6) Accounts inquiry (Dubai courts).
7) Financing of commercial Buildings.

A special secure Dialup connection is assigned by the central bank, only to be used by Blom Bank France AML employee in charge.
The steps of connecting to Central Bank Email:
Click on the dialup connection named “central bank” on the desktop
Open internet explorer, and choose the central bank link which is http://131.5.10.10/exchange
Enter user name and password assigned to you.

2.6.1.1 Court cases:

We deal with this kind of notices by a secure Email System according to the following steps:

Step one: Print the notice
Step two: Delete the mail
Step three: Stamp the printouts
Step four: Circulate, in order to be checked/ signed in the following order:
- Head of Customer Service (Dubai)
- Head of IT Department (Dubai)
- AML Administrator (Sharjah)
- Branch Manager (Sharjah)
- Assistant Branch Manager (Sharjah)
- Head of the AML Department (Dubai)
Fill in the response of the notice according to the saved reply template. Convert it to PDF Send it to the central bank through the court cases secure email which is circular and file it. (Refer to annex page titled response court cases).

P.S. We should follow up the notices regularly

Our legal department will take the necessary action in case any notice matches any of our clientele name/account number.

In case of URGENT court cases, the notices should be circulated within 2 days maximum and sent back to the central bank via secure email.

2.6.1.2 Cancellation:

We deal with this kind of notices by the secure Email System according to the following steps:

**Step one:** Print the notice  
**Step two:** Delete the mail  
**Step three:** Stamp the printouts  
**Step four:** Circulate, in order to be checked/ signed in the following order:  
- Head of Customer Service (Dubai)  
- Head of IT Department (Dubai)  
- AML Administrator (Sharjah)  
- Branch Manager (Sharjah)  
- Assistant Branch Manager (Sharjah)  
- Head of the AML Department (Dubai)

These circulars are to be filed after completion of the above mentioned steps, since no reply is required.

2.6.1.3 Cheque books:

We deal with this kind of notices by the secure Email System according to the following steps:

**Step one:** Print the notice  
**Step two:** Delete the mail  
**Step three:** Stamp the printouts  
**Step four:** Circulate, in order to be checked/ signed in the following order:
- Head of Customer Service (Dubai)
- Head of IT Department (Dubai)
- AML Administrator (Sharjah)
- Branch Manager (Sharjah)
- Assistant Branch Manager (Sharjah)
- Head of the AML Department (Dubai)

These circulars are to be filed after completion of the above mentioned steps, since no reply is requested.

The Head of customer services department adds the wanted names to a special black list for future reference and distributes copies to the concerned departments.

2.6.1.4 AML 1

We deal with this kind of notices by the secure Email System according to the following steps:

Step one: Print the notice
Step two: SAVE the mail- in case the response is required on the same document.
Step three: Stamp the printouts
Step four: Circulate, in order to be checked/signed in the following order:
- Head of Customer Service (Dubai)
- Head of IT Department (Dubai)
- AML Administrator (Sharjah)
- Branch Manager (Sharjah)
- Assistant Branch Manager (Sharjah)
- Head of the AML Department (Dubai)

Upon completion of circulation, follow the following steps:
- Open the already saved AML1 notice
- Stamp the notice with signature stamp saved on the PC.
- Save the changes.
- Send it to the central bank through the court cases secure email which is AMLSCU1@UAEFIU.CB

P.S. We should follow up the notices regularly

N.B: AML Department refers incase of matching to the legal department who takes the appropriate action.
In case of URGENT AML1 cases, the notices should be circulated within 2 days maximum and sent back to the central bank via secure email.

2.6.1.5 AML2

We deal with this kind of notices by the secure Email System according to the following steps:

**Step one:** Print the notice

**Step two:** Save the mail- incase the response is required on the same document.

**Step three:** Stamp the printouts

**Step four:** Circulate, in order to be checked/ signed in the following order:
- Head of Customer Service (Dubai)
- Head of IT Department (Dubai)
- AML Administrator (Sharjah)
- Branch Manager (Sharjah)
- Assistant Branch Manager (Sharjah)
- Head of the AML Department (Dubai)

Upon completion of circulation, follow the following steps:
- Open the already saved AML1 notice
- Stamp the notice with signature stamp saved on the PC.
- Save the changes.
- Send it to the central bank through the court cases secure email which is AMLSCU2@UAEFIU.CB

P.S. We should follow up the notices regularly

N.B: AML Department refers incase of matching to the legal department who takes the appropriate action.

In case of URGENT AML2 cases, the notices should be circulated within 2 days maximum and sent back to the central bank via secure email.
2.6.1.6 Financing of commercial Buildings (تمويل المباني التجارية)

We receive this kind of circulars by courier and we deal with it as follows:

1. Stamp the notices
2. Circulate, in order to be checked/signed in the following order:
   - Head of Customer Service (Dubai)
   - Head of IT Department (Dubai)
   - AML Administrator (Sharjah)
   - Branch Manager (Sharjah)
   - Assistant Branch Manager (Sharjah)
   - Head of the AML Department (Dubai)
3. Send it to the central bank by fax on the given number (02 – 6653571)

P.S. We should follow up the notices regularly

Our legal department will take the necessary action in case any notice matches any of our clientele name/account number.

2.6.1.7 Accounts inquiry (Dubai Courts):

We receive this kind of circulars by courier and we deal with it as follows:

1. Stamp the notices
2. Circulate, in order to be checked/signed in the following order:
   - Head of Customer Service (Dubai)
   - Head of IT Department (Dubai)
   - AML Administrator (Sharjah)
   - Branch Manager (Sharjah)
   - Assistant Branch Manager (Sharjah)
   - Head of the AML Department (Dubai)

P.S. We should follow up the notices regularly

The legal department is responsible for this kind of notices and they should send a response to Dubai Courts by courier on P.O.Box 4700 Dubai

A copy of the response should be attached to its notice before filing it.
2.7 Chapter seven: Reporting Suspicious Transactions:

2.7.1 Definition:
Suspicious transactions: are any transactions, or attempted transaction, which causes the cash dealer to have suspicions regarding the individuals, monies, or circumstances of the transaction.

The circumstances of a transaction can include those which do not have any commercial logic or are considered abnormal given the history and profile of the account holder.

2.7.2 Responsibility
Any employee who has any kind of responsibility for customer interaction or customer funds handling should report suspicious transactions.

2.7.3 Reporting:
Every February of the year, a report of suspicious transactions, clients and accounts in Dubai and Sharjah Branches, prepared by the AML Head and approved by the Risk Manager is sent to the Head Office in Paris.

the report covers the following fields:
- A/C considered temporary suspicious then proved clean.
- A/C categorized suspicious
- A/C kept under continuous monitoring

Cases reported to the Central Bank

Note 1: Every time the bank decides to close any account for suspicious reasons, the case should be reported to the central bank.

Note 2: The entire Bank’s staff is obliged personally to report when there are reasonable grounds to suspect that the funds are proceeds of criminal activity or to be used for terrorism or terrorist act or terrorist financing, to the head of AML and SCU (AMLSCU).

Contact Adress: ABU Dhabi-
Tel: 0097126668496
Fax: 0097126674501

30 Circular 24/2000-date 17/06/2008
Email: amlscu@cbuae.gov.ae
Online reporting System

31 Addendum to circular 24/2000-date 17/06/2008
2.8 Chapter eight: Filing:

2.8.1 KYCs

We circulate the KYC to be checked and signed by the following persons:
- Head Of the AML Department
- Risk Manager
- Branch Manager

After completion of the circulation the following steps should be done:
Office boys should photocopy the original KYC
File the copy in the customer file
The original copy of the KYC should be given to the AML Department in order to file it in a numbered box file.

P.S. Original KYC’s box files should be kept in the AML Department in a safe place and access to these files is denied to any employee outside the AML Department

2.8.2 Swifts

After releasing the swifts by the Head of AML Department, we should file the swift sheets in a numbered box files by the violated print number.

P.S. The released swift sheets box files should be kept in the AML Department in a safe place and access to these files is denied to any employee outside the AML Department.

2.8.3 Memos:

Memos related to AML are kept in a separate box file, held in the AML Dept, under the name “Memos”.
2.8.4 **Letters:**

Letters are used for different purposes as follow:
- Letters sent to customers for updating their account’s information.
- Letters send to AML Units in other BLOM Branches for investigation.
- Letters sent to other BLOM Branches introducing a customer or new w account

2.8.5 **Capital Certificates**

These certificates are kept in a separated box file under its name, held in the AML Dept.

2.8.6 **Compliance /AML notes:**

These notes are filed with their related documents in 2 separate Box files held in the AML Dept, organized by alphabetical order.
The FATF-40 Recommendations

Introduction

Money laundering methods and techniques change in response to developing counter-measures. In recent years, the Financial Action Task Force (FATF) has noted increasingly sophisticated combinations of techniques, such as the increased use of legal persons to disguise the true ownership and control of illegal proceeds, and an increased use of professionals to provide advice and assistance in laundering criminal funds. These factors, combined with the experience gained through the FATF’s Non-Cooperative Countries and Territories process, and a number of national and international initiatives, led the FATF to review and revise the 40 Recommendations into a new comprehensive framework for combating money laundering and terrorist financing. The FATF now calls upon all countries to take the necessary steps to bring their national systems for combating money laundering and terrorist financing into compliance with the new FATF Recommendations, and to effectively implement these measures.

The review process for revising the 40 Recommendations was an extensive one, open to FATF members, non-members, observers, financial and other affected sectors and interested parties. This consultation process provided a wide range of input, all of which was considered in the review process.

The revised 40 Recommendations now apply not only to money laundering but also to terrorist financing, and when combined with the 9 Special Recommendations on Terrorist Financing provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing. The FATF recognizes that countries have diverse legal and financial systems and so all cannot take identical measures to achieve the common objective, especially over matters of detail. The Recommendations therefore set minimum standards for action for countries to implement the detail according to their particular circumstances and constitutional frameworks. The Recommendations cover all the measures that national systems should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and certain other businesses and professions; and international co-operation.

The original FATF 40 Recommendations were drawn up in 1990 as an initiative to combat the misuse of financial systems by persons laundering drug money. In 1996 the Recommendations were revised for the first time to reflect evolving money laundering typologies. The 1996 40 Recommendations have been endorsed by more than 130 countries and are the international anti-money laundering standard.

In October 2001 the FATF expanded its mandate to deal with the issue of the financing of terrorism, and took the important step of creating the 9 Special
Recommendations on Terrorist Financing. These Recommendations contain a set of measures aimed at combating the funding of terrorist acts and terrorist organizations, and are complementary to the 40 Recommendations.
A key element in the fight against money laundering and the financing of terrorism is the need for countries systems to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and FATF-style regional bodies, as well as the assessments conducted by the IMF and World Bank, are a vital mechanism for ensuring that the FATF Recommendations are effectively implemented by all countries.

**Legal Systems**

*Scope of the criminal offence of money laundering*

**Recommendation 1**
Countries should criminalize money laundering on the basis of United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention). Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.
Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year’s imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.
Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences. Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.
Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

**Recommendation 2**
Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions,
including the concept that such mental state may be inferred from objective factual circumstances.
b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisional measures and confiscation
Recommendation 3
Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State’s ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

Measures to be taken by Financial Institutions and Non-Financial Businesses and Professions
to prevent Money Laundering and Terrorist Financing
Customer due diligence and record-keeping
Recommendation 4
Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.
Recommendation 5
Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.
Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:
- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
there is a suspicion of money laundering or terrorist financing; or
the financial institution has doubts about the veracity or adequacy of previously
obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:
a) Identifying the customer and verifying that customer’s identity using reliable,
independent source documents, data or information.
b) Identifying the beneficial owner, and taking reasonable measures to verify the
identity of the beneficial owner such that the financial institution is satisfied that it
knows who the beneficial owner is. For legal persons and arrangements this
should include financial institutions taking reasonable measures to understand the
ownership and control structure of the customer.
c) Obtaining information on the purpose and intended nature of the business
relationship.
d) Conducting ongoing due diligence on the business relationship and scrutiny of
transactions undertaken throughout the course of that relationship to ensure that
the transactions being conducted are consistent with the institution’s knowledge of
the customer, their business and risk profile, including, where necessary, the
source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d)
above, but may determine the extent of such measures on a risk sensitive basis
depending on the type of customer, business relationship or transaction. The
measures that are taken should be consistent with any guidelines issued by
competent authorities. For higher risk categories, financial institutions should
perform enhanced due diligence. In certain circumstances, where there are low
risks, countries may decide that financial institutions can apply reduced or
simplified measures.

Financial institutions should verify the identity of the customer and beneficial
owner before or during the course of establishing a business relationship or
conducting transactions for occasional customers. Countries may permit financial
institutions to complete the verification as soon as reasonably practicable
following the establishment of the relationship, where the money laundering risks
are effectively managed and where this is essential not to interrupt the normal
conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c)
above, it should not open the account, commence business relations or perform the
transaction; or should terminate the business relationship; and should consider
making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial
institutions should also apply this Recommendation to existing customers on the
basis of materiality and risk, and should conduct due diligence on such existing
relationships at appropriate times.

Recommendation 6
Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.

b) Obtain senior management approval for establishing business relationships with such customers.

c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced ongoing monitoring of the business relationship.
Recommendation 7
Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:
a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.
b) Assess the respondent institution’s anti-money laundering and terrorist financing controls.
c) Obtain approval from senior management before establishing new correspondent relationships.
d) Document the respective responsibilities of each institution.
e) With respect to “payable-through accounts”, be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

Recommendation 8
Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

Recommendation 9
Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.
The criteria that should be met are as follows:
a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.
It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

Recommendation 10
Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.
Recommendation 11
Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

Recommendation 12
The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:
a) Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.
b) Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.
c) Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:
buying and selling of real estate;
managing of client money, securities or other assets;
management of bank, savings or securities accounts;
organisation of contributions for the creation, operation or management of companies;
creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

Reporting of suspicious transactions and compliance
Recommendation 13
If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

Recommendation 14
Financial institutions, their directors, officers, and employees should be:
a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

Recommendation 15
Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:
a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
b) An ongoing employee training programme.
c) An audit function to test the system.

Recommendation 16
The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:
a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.
b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Other measures to deter money laundering and terrorist financing

Recommendation 17
Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

Recommendation 18
Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.
Recommendation 19 *(This Recommendation was revised and the following text was issued on 22 October 2004)*
Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

Recommendation 20
Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.
Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

*Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations*

Recommendation 21
Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations.
Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

Recommendation 22
Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

*Regulation and supervision*

Recommendation 23
Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.
For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes. Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

Recommendation 24
Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:
Casinos should be licensed;
Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino;
Competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

Recommendation 25
The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.

Institutional and other measures necessary in systems for combating Money Laundering and Terrorist Financing

Competent authorities, their powers and resources

Recommendation 26
Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

Recommendation 27
Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialized in asset investigation, and co-operative investigations with appropriate competent authorities in other countries.

Recommendation 28
When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

Recommendation 29
Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorized to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

Recommendation 30
Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities is of high integrity.
Recommendation 31
Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

Recommendation 32
Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements
Recommendation 33
Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

Recommendation 34
Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

International co-operation
Recommendation 35
Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering,
Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

**Mutual legal assistance and extradition**

**Recommendation 36**

Countries should rapidly, constructively, and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

a) Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.

b) Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.

c) Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d) Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

**Recommendation 37**

Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalize the conduct underlying the offence.

**Recommendation 38**

There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-coordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

**Recommendation 39**


Countries should recognize money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation
Recommendation 40
Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorized manner, consistent with their obligations concerning privacy and data protection.
Account opening forms

Figure 1-specimen of signature
This agreement is made between the undersigned:

- Mr./Messrs

- Mr./Messrs

- Mr./Messrs

- Mr./Messrs

And “BLOM BANK FRANCE S.A ____________ branch”, hereinafter referred as “the Bank”

The customer maintains with the Bank an account bearing the above mentioned account N0. For quick service and convenience in the execution of the transactions he may order, the customer expressly requests “Blom Bank France-UAE” to execute the transactions it may receive either from him, or from his representatives, by fax or signed instruction orders in PDF format attached to email messages, in order to execute all transactions with the Bank, including among others all transfer orders, foreign exchange transactions of all types and in all currencies (spot, forward, swap and others), purchase or sale of securities, stocks and bonds, as well as all instructions regarding documentary credits (inward & outward) or to documentary collections (inward or outward)

Though recognizing the substantial risks the use of these means may involve, and taking full acknowledgement of such risks, the customer finally and irrevocably relieves the Bank without any reservation whatsoever, from any responsibility for the damages and prejudices he may suffer due to the transmission of his orders and instructions by fax or by email, and in particular as a result of their fraudulent use, transmission errors, duplicate transmission, or the misuse of the legitimate electronic means of transmission.

The Customer already approves all types of transactions carried out by the Bank in execution of the instructions it received by fax or by email.

The Customer waives his right to exercise any action, recourse or legal proceedings against the Bank claiming any restitution or compensation for the consequences that may result from the execution by the Bank of the instructions received by fax or by email.

The Customer undertakes on the other hand to indemnify the Bank fully for any damage resulting from any claim a third party may lodge to challenge the legitimacy of the execution of such instructions transmitted by fax or by email.

Not withstanding this agreement, the Bank has the right when in doubt, to delay the execution of such instructions for the sake of verifying genuineness and will not be held liable in any way for taking such precaution.

This agreement does not affect other Terms & Conditions governing the account relationship signed by the customer.

These instructions shall remain valid as long as a written revocation has not been notified to and acknowledged by the Bank.

Made in , on / / .

Made in as many copies as ordered
ACCOUNT OPENING APPLICATION

DATE ........../........../2........

Name: ........................................ Base Account Number: ........................................

........................................ Telephone ........................................

Address: ........................................ P.O. Box: ........................................

The Manager, BLOM BANK FRANCE.

1. Will you please open an account in our name with Blom Bank France in ......................... branch

2. We understand that various sub-accounts may be opened in our name in order to facilitate and accommodate the different types of banking transactions that we may require. These accounts may be opened in any currency at your entire discretion whenever you deem it necessary and without our filling for each account a separate account opening form, a separate specimen of signature card, and separate other related account documents. Each account regardless of its type or its currency of denomination carries the same Base Account Number referred to above. This Base Account Number will serve to identify all accounts already opened in our name or to be opened today or at subsequent dates, and signatures contained in the specimen of signature card filled will be binding upon us in all these accounts. Numerical codes will indicate branch, currency, type and order of account. These codes are appended to our Base Account Number, yielding an account number which will serve to identify a particular sub-account of ours.

The opening of accounts under the above Base Account Number does not and shall not preclude our opening of accounts under our own name but with different Base Account Number(s).

However regardless of the number of Accounts opened, whether under the same Base Account Number or under different Base Account Numbers, and whether in the same branch or in different branches of your Bank, all these accounts shall be considered and treated for all purposes as an integral and indivisible part of one single account.

3. We hereby certify that we are aware of the laws and regulations that are effective with regards to money laundering crimes. We pledge as from now on to declare the source of any funds we receive in our account and to produce all the documents as a proof therefor. We also assume the consequences of making false declarations or providing incorrect information hence, we solely bear any claims or penalties resulting from the misuse of this account in whatever way, whether to actually commit or to help committing money laundering. We empower you to lift the banking secrecy from our account and exempt your bank and your staff from any civil or criminal liability resulting from providing such information, or the seizure of our account in compliance with the relevant authorities decisions, and have no right to claim any compensation or indemnity in that regards.

SIGN HERE
4. We undertake to inform you to our agreement or otherwise to the statement of our account(s) within fifteen days from the date of dispatch thereof to our address as registered in your records, and should you not receive our written advice of agreement or disagreement within the time mentioned, you may consider that we have definitely approved such statement(s) of the account as correct.

We further agree that debit interest and related commissions shall be computed monthly and added to the principal to become an integral part of it, and also authorise the Bank to charge to our account(s) such out-of-pocket expenses as may be incurred in connection therewith in the form of postage, insurance, telephone, fax, telex, swift commission and other charges.

5. We hereby declare that you may allow our account(s) to be overdrawn without notifying us. You may credit our account(s) with the value of any bills, cheques, or other instruments belonging to us that may be in your possession whether for collection or for any other purpose and you may debit any account in our name with you with all amounts owed by us to you in respect to guarantees issued, bills, cheques, orders of payment or other negotiable instruments remitted by us for collection or for discount.

6. We hereby also authorise you, at any time without notice, to combine or consolidate all our accounts held on your books and set-off any credit balances, in whatever currency, in any such accounts towards the settlement of all our liabilities to you whether such liabilities are direct or contingent, primary or collateral.

In case of set-off of accounts in foreign currencies the applicable rate of exchange is the rate prevailing at the time of set-off.

7. We agree that you shall have the right to stop our drawings from any or all accounts in our name at any moment and demand reimbursement of any debit balance together with all interest and other charges due to you which will be repayable immediately and this notwithstanding that you may hold security or guarantees to realize in respect thereof.

8. We declare the records and accounts of the Blom Bank France to be correct and final and a conclusive evidence binding on us and we hereby waive any right we have to object to them.

9. Should our current account with you become overdrawn, we hereby authorize you to charge interest at an agreed upon rate of \(_{\text{\%}}\) percent per annum in addition to a monthly commission of half per thousand of the highest overdraft balance during the month. We hereby confirm our agreement to amend the above interest rate in line with market changes, in which case you notify us in writing either by hand or by registered mail. Our agreement to the amended rate is final and binding if you do not receive from us a reply to the contrary within 15 days from our notification, in which case we undertake to settle our overdrawn account immediately. In case of disagreement between us for any possible reason, the interest rate and commission agreed upon will be applied on our debtor accounts during the period of litigation or arbitration and until full settlement, to which rates we have no right to object at later stages.

10. We hereby declare that the aforementioned address is our place of residence for the execution of all our undertakings concerning this account and where we shall receive all your notifications without any objection or protestation later on for any reason whatsoever.

11. We understand that the courts chosen by your bank, whether in the United Arab Emirates or in any other country, have sole competence to deal with any claim or dispute arising between the Bank and ourselves. You shall be entitled to take all provisional measures against us and execute any judgment rendered in your favour against all our financial, movable and fixed assets wherever their location, whether in the United Arab Emirates or abroad.

Signature: ...........................................
JOINT ACCOUNT (AND / OR) OPENING APPLICATION

TO BLOM BANK FRANCE.                      DATE ........................................

BRANCH ........................................ A/C No. ........................................

We the undersigned:

1. ................................................................. 2. .................................................................

3. ................................................................. 4. .................................................................

Jointly and severally request BLOM BANK FRANCE to open in our name a joint account entitled:

Under the following terms and conditions:

1. Each one of the account holders shall have sole and full power to make use of the funds available in the account even after the death of any one of the account holders. Each and every holder will have the power to make deposits, effect withdrawals at any time he chooses without the Bank having any responsibility in advising such transactions to other account holders as the balance in the account belongs to each one of us separately. This right does not originate from any power of attorney or any other empowerment but is generated from a contractual agreement, which binds all parties involved in this joint account.

2. The Bank at his own discretion, unless advised to the contrary, is entitled to deposit in this account any amounts or transfers received by you in the name of any one of the account holders. You are also authorized to overdraw our joint account upon the instructions duly signed by any one of us and in such case, we will be jointly and severally responsible for covering and settling the overdraft.

3. In case of the death of any of the account holders, we hereby confirm, as from now, that any one of the remaining surviving account holders shall have complete freedom to make use, separately, of the existing funds in the account and we undertake jointly and separately and without any severance among us together with the heirs of the deceased to settle, immediately, the debit balance if any.
TIME DEPOSIT ACCOUNT OPENING APPLICATION

To: BLOM BANK FRANCE.

Branch: ........................................ Date: ........................................

I/we hereby request and authorise you to open a Time Deposit Account in my/our name(s) by debiting my/our current account No. ........................................ with the following particulars:

FULL NAME: ........................................ NATIONALITY:

CHosen ADDRESS [e.g. building, street etc.]: ........................................ TEL: ........................................

POSTAL ADDRESS: ........................................ RE: ........................................

ADDRESS IN HOME COUNTRY:

IDENTIFICATION: (preferably passport/copies):

DATE AND PLACE OF BIRTH:

Currency & Amount: ........................................ Deposit No. ........................................

Period of: ........................................ From ........................................

Rate of Interest: ........................................

Unless otherwise instructed by me/us in writing three working days before date of maturity, please dispose of the principal plus accrued interest, as indicated below:

☐ Renew the deposit plus interest for a similar period at the rate applicable on the date of renewal.

☐ Credit my/our account No. ........................................ with your interest plus full value at maturity.

☐ Credit interest earned to my/our account No. ........................................ with you and reinvest the principal for a similar period at the rate applicable on the date of renewal.

☐ Remit the proceeds after deducting your charges, if any, by Mail / Tele / SWIFT transfer to my/our

Account No. ........................................ in

TERMS AND CONDITIONS:

1. Minimum amount for a time deposit is AED. 10,000 for personal accounts and AED. 20,000 for corporate accounts.

2. Each deposit made after or renewed subsequent to the date appearing on the face hereof is subject to the conditions of this Agreement.

3. It is understood and agreed that the Bank is under no obligation to pay a Foreign Currency Deposit in foreign currency unless such currency is readily available at the Bank. In this case the Bank’s tariff will apply.

4. Within a reasonable time after the commencement of the original deposit period, the Bank shall mail to the depositor its last known address a Time Deposit Advice indicating the principal amount of deposit and applicable terms.

5. Unless otherwise agreed by the Bank, withdrawals from Foreign Currency Deposit may be effective only at the maturity of the original or renewal period thereof. Each withdrawal prior to maturity date will be subject to the terms and conditions governing such transactions as established by the Bank at the time of withdrawal.

6. It is understood and agreed that new instructions with respect to deposits in foreign currencies must reach the Bank at least three working days prior to maturity date falling which the existing instructions will be executed.

7. The Bank has the right to refuse this deposit against any liability or exposure towards the Bank.

8. The disposal of funds by the Bank in accordance with the provisions of this agreement shall discharge the Bank from all obligations in respect of the deposit or interest on the same may be.

CUSTOMER SIGNATURE ........................................

Figure 5-time deposit
<table>
<thead>
<tr>
<th>1</th>
<th>Full Name</th>
<th>Address</th>
<th>Tel No.</th>
<th>Occupation</th>
<th>Employer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Full Name</td>
<td>Address</td>
<td>Tel No.</td>
<td>Occupation</td>
<td>Employer</td>
</tr>
</tbody>
</table>

Signature (Single / Jointly)

<table>
<thead>
<tr>
<th>1</th>
<th>Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Name</td>
<td>Signature</td>
</tr>
</tbody>
</table>

FIGURE 6: SAVING ACCOUNT
KYC QUESTIONNAIRE

Questionnaire to be filled by customer:
Confirm and update the information in section “A”
Sign the questionnaire in section “A” and
Answer the questions in Section “B”
If not enough space is available for any of your replies; please continue overleaf

Please confirm and update this information:

We will use the information you give us on this form to update our information database that we hold about you in our records. You can ask a copy of this. This explains how we will use your information now and in the future.

Full Name:

Address where we can contact you:

If you want us to contact you at this address please tick this box: ☐

Phone Number:                Fax Number:

Nationality:                  Email:

<table>
<thead>
<tr>
<th>Date of birth:</th>
<th>Place of birth:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name and address of employer (or place of business if you are self employed):

<table>
<thead>
<tr>
<th>Name and address of employer (or place of business if you are self employed):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Position Held or Job title:

<table>
<thead>
<tr>
<th>Position Held or Job title:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Time with this employer:

<table>
<thead>
<tr>
<th>Time with this employer:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Occupation (or nature of your business if you are self employed):

<table>
<thead>
<tr>
<th>Occupation (or nature of your business if you are self employed):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Your yearly Income:

<table>
<thead>
<tr>
<th>Your yearly Income:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Please tick here if you are self-employed: ☐

Provide Names of Banks you are dealing with and your account numbers:

<table>
<thead>
<tr>
<th>Provide Names of Banks you are dealing with and your account numbers:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
☐ Please provide us with an introduction letter from your Banker.

☐ Please provide us with a copy of the statement of your account for the past 6 months.

Signature:

I confirm that the information on this questionnaire is correct:

Date:

B. Please answer the following questions as fully as possible:

Please give us details why you need to bank and have an account with us:

How have you built your wealth: sources of income?  What are your main sources of income?

(Please tick all that apply)  (Please tick all that apply)

Regular savings  ☐  Employment  ☐

Inheritance  ☐  Investment Income  ☐
Selling a business □ Dividends or investments □
Selling a property □

Provide details of above:

Other (please give details) □

Other (please give details) □

Please provide us an estimate of the amount of your payments in your accounts with us:

□ Cash □ Cash payments per month

□ Inward/Outward transfers per month

Approximate in (AED)

Approximate in (AED)

Figure 6- KYC questionnaire
Date:

<table>
<thead>
<tr>
<th>Branch:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Identification number:</td>
</tr>
<tr>
<td>Account name</td>
</tr>
<tr>
<td>Address of company</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>First Shareholder/Partner (name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residence visa validity (date)</td>
</tr>
<tr>
<td>Address and telephone number (local)</td>
</tr>
<tr>
<td>Address and telephone number (country of origin)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Second Shareholder/Partner (name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residence visa validity (date)</td>
</tr>
<tr>
<td>Address and telephone number (local)</td>
</tr>
<tr>
<td>Address and telephone number (country of origin)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Third Shareholder/Partner (name)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residence visa validity (date)</td>
</tr>
<tr>
<td>Address and telephone number (local)</td>
</tr>
<tr>
<td>Address and telephone number (country of origin)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fourth Shareholder/Partner / Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residence visa validity (date)</td>
</tr>
<tr>
<td>Address and telephone number (local)</td>
</tr>
<tr>
<td>Address and telephone number (country of origin)</td>
</tr>
</tbody>
</table>
Other authorized signatories

("Use space overleaf if necessary). Residence visa validity (date) Address and telephone number (local) Address and telephone number (country of origin)

OFAC:

Passport copies taken-to be stamped true copy yes/no Customer address corroborated:
Yes (explain how) No (give reasons)

Trade License validity (date)

Details of accounts held with other Banks

<table>
<thead>
<tr>
<th>Bank name</th>
<th>Account number</th>
</tr>
</thead>
<tbody>
<tr>
<td>11111111111</td>
<td></td>
</tr>
<tr>
<td>2)</td>
<td></td>
</tr>
<tr>
<td>3)</td>
<td></td>
</tr>
</tbody>
</table>

Co-operatives, charitable and social societies require specific written approval from relevant ministry.

Related document taken Yes / No

Expected monthly turnover in account activity and source of funds
Expected nature of business activity:
(Example dealings to be related to cash, Loans Inter-bank Transfers, Foreign Exchange, Trade Finance).

Customer introduced by:

KYC valid till

(1 year from preparation date)

Remarks:

Prepared and reviewed by:

Risk Manager

Branch Manager

AML Head

Figure 7-KYC-Corporate account
<table>
<thead>
<tr>
<th>KNOW YOUR CUSTOMER (KYC) – INDIVIDUALS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date:</strong></td>
</tr>
<tr>
<td><strong>Branch:</strong></td>
</tr>
<tr>
<td>Customer Identification number</td>
</tr>
<tr>
<td>Account name</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Account holder name</td>
</tr>
<tr>
<td>Residence visa validity date</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Address and telephone number (local)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Address and telephone number (country of origin)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>In case of joint account</strong></td>
</tr>
<tr>
<td>Second account holder name</td>
</tr>
<tr>
<td>Residence visa validity date</td>
</tr>
<tr>
<td>Address and telephone number (local)</td>
</tr>
<tr>
<td>Address and telephone number (country of origin)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Passport copies taken (yes/no) to be stamped true copy</strong></td>
</tr>
<tr>
<td>Customer Address corroborated</td>
</tr>
<tr>
<td>Yes (explain how)</td>
</tr>
<tr>
<td>No (give reasons)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Details of accounts held with other Banks</strong></td>
</tr>
<tr>
<td>Bank name</td>
</tr>
<tr>
<td>1)</td>
</tr>
<tr>
<td>2)</td>
</tr>
</tbody>
</table>
3)

Amount of initial deposit

<table>
<thead>
<tr>
<th>Currency</th>
<th>Amount</th>
</tr>
</thead>
</table>

Paid by:
- [ ] Cash
- [ ] Draft

| Traveller’s Cheques | Transfer-Local/OVERSEAS |

Annual income

OFAC:

Expected monthly turnover in account activity and source of funds

Expected nature of business activity:
(Example dealings to be related to Cash, Loans, Inter-bank Transfers, Foreign Exchange, Trade Finance).

Customer Introduced by

KYC valid till
(1 year from preparation date)

Remarks:

Prepared and reviewed by:

| Risk Manager | Branch Manager | AML Head |

Figure 8-KYC-Individual account
فم أجل اختصاصات المصرفية الشريعة على خلاف أدوؤها قائمة كأنه أم مخفية تأتي علامة.

 выполнен الأعمال في المسابقات الالية أو اختصاصات التي ستمنح لائحة مصرفية للطبقة بال wg. حتى ولو أوقف ذلك إلى تخفيف هذه

 إجابة.

 الطلب الشروط والتفصيل بأن عينة كافة الكهف المنصوب بها يداء الكهفون والحضاك في الكهفون مه، كان اسمها أو صيغها

 التخطيط على الضمانات والوكالات يجملها التطبيق أو تعويمه، وما يجب عليها وفي التطبيق على جميع الأدوات والموارد.

 إجابة المذكورة في جميع اختصاصات المصرفية لهن كليا، أو حسب أو أي عمله.

 تجربة الاقتراض المستندية توظيفها، وفيها ورفع الخدمات وجمع الأوراق القائمة فيها، كلية، أو حسب توجيهات أدوات

 إلا أننا واستخدم المراجعة القائمة لها.

 طلبت إصدار الانتصارات المصرفية في أي نوع كانت، وتعديلها سواء، أو لغد.

 Figure 9-Power of attorney -arabic version
GENERAL POWER OF ATTORNEY

Date:

TO : BLOOM BANK FRANCE.

BRANCH : DUBAI

Gentleman,

This is to advise that

constitutes and appoints

Whose specimen of signature(s) appear(s) below, as my(our) true and lawful attorney(s)-in-fact. In this connection, you are authorised and instructed to accept my(our) signature(s) on my(our) behalf with respect to the following acts and things regarding business transacted with you.

1. Open, maintain and/or reconcile any one or more deposit or other accounts, either in the name of the Principal or otherwise;

2. Deposit any moneys, cheques, drafts, promissory notes or other instruments for the payment of money, also, to endorse for deposit, collection, transmission and remittance, or otherwise, any and all such instruments and to deliver the same to the bank for any of the indicated purposes;

3. Draw, make, execute and deliver any and all cheques, drafts, promissory notes and other instruments for the payment of money payable by or at the bank, and give any orders or directions by letter, telex, telegram or otherwise for the withdrawal, transfer or other disposition of any funds at any time(s) held by the bank on deposit or otherwise available to the principal;

4. Discount and/or negotiate any one or more promissory notes, drafts or other instruments for the payment of money;

Figure 10-Power of attorney-English Version