USAID
FROM THE AMERICAN PEOPLE

BUILD AML/CFT CAPACITY AT COMMERCIAL BANKS

INTERACTIVE AML/CFT TRAIN-THE –TRAINER FOR COMMERCIAL BANKS

June18, 2008

This publication was produced for review by the United States Agency for International Development. It was prepared by Izzidin Hussein Razem, Subcontractor to BearingPoint Inc.

BUILD AML/CFT CAPACITY AT COMMERCIAL BANKS

INTERACTIVE AML/CFT TRAIN-THE-TRAINER FOR COMMERCIAL BANKS

SUSTAINABLE ACHIEVEMENT OF BUSINESS EXPANSION AND QUALITY (SABEQ)

CONTRACT NUMBER: 278-C-00-06-00332-00

BEARINGPOINT, INC.

USAID/JORDAN ECONOMIC OPPORTUNITIES OFFICE (EO)

JUNE 18, 2008

AUTHOR: IZZIDIN HUSSEIN RAZEM

DELIVERABLE: 1.4.1.17.23.1 INTERACTIVE AML/CFT TRAIN-THE-TRAINER FOR COMMERCIAL BANKS

CONTENTS

EXECUTIVE SUMMARY

Under the USAID-funded Sustainable Achievement of Business and Quality program (SABEQ), the consultants performed the following assignment:

1- Training Needs Assessment (TNA) at commercial banks in the area of AML/CFT.

2- Development of AML/CFT train-the-trainer material.

Different scientific methods were used to perform the above assignment; meetings and interviews, TNA questionnaire, and discussions with the AML/CFT compliance officers at commercial banks. Also, discussions with the Anti-Money Laundering Unit (AMLU) at the Central Bank of Jordan and the Association of Banks in Jordan (ABJ).

The consultants realized the need for uniformity amongst commercial banks in the area of AML/CFT.

They also realized the need for a proper compliance committee to be constituted under the ABJ and AMLU umbrella.

The AML/CFT train-the-trainer material was developed and supplemented to this report. However, it has to be tested before using it as a final product. This is recommended to be done by the newly set up committee of five AML/CFT compliance officers from commercial banks who volunteered to do so.

It is highly recommended to provide the material in Arabic so that all banks' staff would benefit from the training.

INTRODUCTION

This consultancy was conducted as part of SABEQ project aiming at building AML/CFT Compliance Capacity at commercial banks and providing AML/CFT train-the-trainer material.

Two consultants worked on this project; one Jordanian local consultant Mr. Izzidin Razem, and one expatriate advisor from US Treasury Department Mr. James Wright.

The consultants worked closely with the Anti-Money Laundering Unit at the Central Bank of Jordan (AMLU) and the Association of Banks in Jordan (ABJ) as well as the Financial Services Component at SABEQ (FSC) and the commercial banks.

In achieving the consultancy targets, the consultants conducted the following:

1- Visiting eleven banks to collect data and envisage on-spot requirements and needs.
2- Analyzing training needs through a questionnaire devised for this purpose.
3- Meetings and discussions with the AML/CFT compliance officers from the commercial banks.

The consultants realized the need for a proper committee from the AML/CFT Officers rather than the present one constituted at the ABJ. Therefore, a new committee of five AML Officers was set. The consultants convened a meeting with them and discussed the training material layout which had been prepared.

The training material is presented in modules, and consists of twelve modules covering most banking activities.

Based on the training needs analysis, the material is also supplemented by thirteen AML/CFT cases covering different banking activities.

METHODOLOGY

In the training needs assessment (TNA), the consultants used the following methods:

1. Meetings and Interviews.
2. Questionnaire.
3. Brainstorming and discussion.

1. Meetings and Interviews:

The following interviews have been conducted with the concerned staff at the following banks:

	Bank Name	Interviews	Job Title
1.	Jordan Commercial Bank	Bassam Salman	AML Compliance Head
		Shireen Krishan	AML Compliance Officer
2.	Capital Bank	Manal Omer	Head of Compliance
3.	Arab Jordan Investment Bank	Saed Budeiri	AGM – Operations
		Osama Natshe	Compliance Officer
4.	Arab Banks Plc	Mechael Matossian	Group Compliance Head
		Mohamad Dabbour	Compliance
5.	Cairo Amman Bank	Farouk Amouri	Head of Compliance
		Yousef Amira	AML Officer
6.	Union Bank	Mu'nes Haddadin	Head of Compliance
7.	Ahli Bank	Samer Abdallah	Head of Compliance
8.	Blom Bank	Maen Zu'bi	Head of Compliance and AML
9.	Standard Chartered	Katia Hazboun	Head of Legal and Compliance

10. Bank of Jordan	Nida' Isis	AML Officer
11. Societe Generale	Majdi Ajaj	Compliance Manager

However, other meetings were conducted with the Association of Banks Director General (ABJ), the AMLU of the Central Bank of Jordan (CBJ), and the SABEQ program officers. **(Appendix 1)**

2. TNA Questionnaire

A 19-item questionnaire was devised and specifically designed for the training needs assessment (TNA) exercise. **(Appendix 2)**.

The questionnaire has been given to following banks to complete, however only the following has been gathered back and analyzed:

Bank	No. Completed/Analyzed
1. Jordan Commercial Bank	5
2. Arab Jordan Investment Bank	4
3. Standard Chartered	3
4. Capital Bank	3
5. Blom Bank	5
6. Cairo Amman Bank	5
7. Ahli Bank	0
8. Arab Bank Plc.	0
9. Union Bank	5
10. Bank of Jordan	5
11. Societe Generale	4

Total No. of Questionnaires collected and analyzed	39

1. Hours of AML/CFT training received:

   * Less than 15 hours : 67%

   * 16 hours and more : 33%

2. Awareness of Jordanian AML law 46/2007:

   * 21% are unaware.

3. Awareness of responsibility under the law:

   * 13% are unaware

4. Two out of 39 said that their banks do not have AML/CFT policies and procedures (5%). Whereas, 28% do not have copies of their policies and procedures. Moreover, 13% think that their policies and procedures are not clearly correlated with the law requirement.

5. The following training components took the following need priority:
   a. How to detect suspicious customers/transactions/red flags.
   b. Examples of money laundering processes/typologies.
   c. Regional and local guidelines and regulations.
   d. International entities concerned with AML/CFT.
   e. Awareness and background information.
   f. KYC implementation methodologies.

6. Rating the existing training:

   Excellent : 23%

   Good : 61%

   Weak : 16%

7. Ignorance about the following entities:

   * FATF : 31%

   * Basel Committee : 20%

   * OFAC : 19%

   * AMLU/Jordan CBJ : 11%

8. Un-realization of risks and high risk Products/ Business/ Customers/ Geography.
   * 26% either they simply do not know or stated wrong examples of high risks.

9. 25% do not know how money can be laundered through their departments/sections.

10. Nearly half (49%) face customer relations problems in implementing AML/CFT requirement.

11 More than 30% feel there is a conflict between applying AML/CFT requirements and the bank's prosperity and growth.

3. Brainstorming and Discussion Session

This session was held on May 14, 2008 after the consultants (James Wright and Izzidin Razem) have gone through meetings and interviews with the banks and other discussions with ABJ and AMLU.

The importance of this session also lies in having 23 compliance and AML officers representing 18 banks under one roof of the ABJ.

The session resulted in the following:

3.1 Compliance AML/Officers Suggestions

The AML Compliance Officers suggested the following training components:

1. Awareness and culture of AML/CFT not only for Banks employees, but also for customers and the community at large.
2. Developing AML policy and procedures.
3. Special training for compliance officers.
4. Need to train Auditors and lawyers (as part of the legal system) on AML/CFT issues.
5. USA Patriot Act.
6. Break down training into modules tailored for each business unit in the bank.
7. AMLU to standardize "minimum required standards for AML compliance" at all Jordanian Banks, i.e. issues like KYC, verification, due diligence, correspondent banking, lists of names…..etc.
8. Need to explain Jordan Laws and Regulations on AML/CFT.

3.2 AML Compliance Committee:

The following AML compliance officers volunteered to work with the consultants (James Wright and Izzidin Razem) on the project as an Ad hoc Committee:

1- Mr. Mohamed Momani – Audi Bank.

2- Mr. Saher Abdel Hadi – Arab Bank.

3- Majdi Ajaj – Societe Generale.

4- Mu'nes Haddadin – Union Bank.

5- Shireen Krishan – Jordan Commercial Bank.

3.3 Priority List of Training Needs:

The training needs gathered and realized by the consultants were listed and given to the AML compliance officers in the meeting to discuss and prioritize. This was a brainstorming exercise resulted in the following priority list.

1. Knowledge of Jordan AML Laws and Regulations.
2. Awareness and background information.
3. Knowledge of Bank's Policies and Procedures.
4. Knowledge of International Guidelines and Regulations.
5. Identifying risks according to customer, business, geography, product.
6. Identifying red flags in business units/departments.
7. How to detect and investigate suspicious activities.
8. Compliance Communication Etiquette customers, managements, employees, AMLU/CBJ.
9. Typologies

Other suggested training components:

1. Risk classification of customers.
2. Patriot act and correspondent Banks.
3. Awareness and culture.
4. How to verify source of funds.
5. Compliance communication etiquette.
6. How to identify ML at each business unit.
7. How to prepare for AML examination.

Training Levels Priority

1. Front office staff.
2. Compliance and MLRO's
3. Executive Management.
4. Middle and back office staff.
5. Department/unit heads.

TRAINING MATERIAL

In preparing and writing the training material, the following factors have been taken into consideration:

1. The needs and gaps realized by the consultants in the current training performed at the banks, which were touched during the meetings and interviews conducted at the survey phase.
2. The priorities of the training needs which have been discussed with the representatives of the banks in a brainstorming session.
3. The suggestions provided by the banks either through interviews and meetings or through the questionnaire used.
4. The questionnaire analysis results.
5. Thoughts and ideas exchanged with ABJ and AMLU.
6. The consultant's expertise.

TRAINING MATERIAL COMPONENTS

The training material consists of twelve modules as follows:

Module 1: Cash Transactions – Tellers

Module 2: Customer Services Relationships (CSR)

Module 3: Jordan AML/CFT Laws and Regulations.

Module 4: Wire Transfers

Module 5: Trade Finance

Module 6: Private Banking

Module 7: Risk-Based Approach in AML/CFT

Module 8: Real Estate Lending

Module 9: USA Patriot Act

Module 10: Internal/External Audit

Module 11: Compliance Communication Etiquette

Module 12: Lending and Investment

The training material was also annexed with thirteen different cases. Most of them are true cases, but customized to the training needs. The cases cover most of the banking activities as follows:

Case 1: Hypothesis

Case 2: New Account Opening

Case 3: Account Opening

Case 4: Transfers

Case 5: Bankers Draft/Cheque

Case 6: Cheques for Collection (B/C'c)

Case 7: Customer Profile Analysis.

Case 8: Guarantees (L/G's) / PEP

Case 9: Dormant Account/Off-Shore business

Case 10: Corporate Account

Case 11: Loans

Case 12: Transfers, Front Companies, Off-shore

Case 13: Real Estate, Third Party Funds

RECOMMENDATIONS

1. It is highly recommended to arabize the material to achieve the full target. It has been realized that a good proportion of the banks' staff needs the training material in Arabic.

2. The addition of tests for the training modules is recommended especially when the material is transformed into an interactive media (CBT). A quiz or a small test is recommended to be added at the end of each module of the 12 modules.

3. As the provided material was intended for a short-time training (quick shots), it is recommended to provide references for further readings or materials for those who need more information.

4. It is recommended to utilize the 5 compliance offices volunteered to work with the consultants, in the testing of the training material provided. These compliance officers showed keenness and interest to do so. They are the following:

1. Mohamad Momani	-	Audi Bank
2. Saher Abdel Hadi	-	Arab bank plc
3. Majdi Ajaj	-	Societe Generate
4. Mu'nes Haddadin	-	Union bank
5. Shireen Krishan	-	Commercial Bank

APPENDICES

Appendix: 1: List of meetings conducted.

Appendix 2: Questionnaire

Appendix 3: SABEQ Project Material

APPENDIX 1

List of Meetings Conducted for SABEQ Project

APPENDIX 1

List of Meetings Conducted for SABEQ Project

I: Izzidin Razem

J: James Wright

Monday May 5, 2008

1. SABEQ Office (I.J)
   Glenn Tasky, Asma Abu-Taleb, Nahla Bashiti

Tuesday May 6, 2008

2. ABJ – Dr. Adli Kandah (I J)
3. AMLU- Adnan, Samia and Ra'ed (I)

Wednesday May 7, 2008

4. Jordan Commercial Bank (I J)
5. Capital Bank (I)

Thursday May 8, 2008

6. Arab Jordanian Investment Bank (I)
7. Arab Bank plc (I J)

Sunday May 11, 2008

8. Cairo Amman Bank (I)

Monday May 12, 2008

9. Union Bank (I J)
10. Ahli Bank (I J)
11. Blom Bank (I J)

Tuesday May 13, 2008

12. AMLU – Adnan (I)
13. Standard Chartered (I)

Wednesday May 14, 2008

14. ABJ Meeting with Compliance Officers (I J)

Sunday May 18, 2008

15. Bank of Jordan (I)
16. Societe Generale (I)

Wednesday May 21, 2008

17. SABEQ Office (I J)

    Meeting with the 5 volunteers

Thursday May 22, 2008

18. CBJ/AMLU + Joe Parker and Ayman Al-Qasem (I J)

APPENDIX 2

Questionnaire

SABEQ PROJECT

AML/CFT COMPLIANCE CAPACITY AT COMMERCIAL BANKS

AML/CFT TRAINING QUESTIONNAIRE

Bank/Branch: ——————————————————————

Position /Dept.:——————————————————————

Years of Experience: ——————————————————————

——————————————————————————————

1. Hours of AML/CFT training received :
   ----- 1 – 15 hours
   ----- 16 – 30 hours
   ----- More than 30 hours
2. Do you know your bank Compliance Officer?
   ----- yes ------ no
3. Are you aware of the Jordanian AML Law no 46/2007?
   ------ yes ------ no
4. Are you aware of your responsibility under the AML Law 46/2007?
   --------- yes ------- no
5. Does your bank have internal policies and procedures for AML/CFT?
   --------- yes --------- no
6. Do you have a copy of them?
   --------- yes -------- no

7. Do the Policies and Procedures clearly correlate with the requirements of Law
   --------- yes --------- no
8. Are the goals and objectives of fighting ML/TF important?
   --------- yes ---------- no
9. What type of AML/CFT training you need (tick all what applicable
   ------ Awareness and background information
   ------ KYC implementation methodologies
   ------ International entities concerned with AML/CFT
   ------ Regional and local guidelines and regulations
   ------ Examples of money laundering processes / typologies
   ------ How to detect suspicious customers/transactions/red flags
10. How do you rate the AML/CFT training given at your bank?
   ------ excellent ------- good ------ weak
11. If you doubt a customer doing a transaction with you, what would you do?
   ----- refer the customer to your manage
   ----- refrain from doing the transaction and apologize to the customer
   ----- complete the transaction and report it to your manager/compliance
12. Tick appropriate space if you know or not about the following entities involvement in AML/CFT:
   - Basel Committee ----- yes ----- no
   - FATF ----- yes ----- no
   - OFAC ----- yes ------ no
   - AMLU /Jordan CBJ ----- yes ------ no

13- Do you know the risks of ML/TF?

------ yes ----- no

14- Give one example on each of the following High Risk:

A. Bank product/service risk:

B. customer/business risk:

C. Geographic risk:

15. Do you know how money can be laundered through your department/section?

-------- yes ------ no

16. Do you face customer relations problems in implementing AML/CFT requirements?

------ yes ------- no

17. Do you feel a conflict between applying AML/CFT requirements and the Bank's prosperity and growth?

------ yes ------ no

18. Do you know the difference between money laundering and terrorist financing?

------- yes ------- no

19. Provide any other comments or ideas for the proper and most needed training on AML/CFT :

Appendices 3
SABEQ Project Material

Appendices 3

SABEQ Project Material

SABEQ PROJECT MATERIAL

Build AML/CFT Capacity at
Commercial Banks

Interactive AML/CFT Train-The-Trainer for Commercial Banks

Prepared by:
James Wright, Izzidin Razem

June, 2008

SABEQ Project Material Modules

Module 1: Cash Transactions – Tellers

Module 2: Customer Services Relationships (CSR)

Module 3: Jordan AML/CFT Laws and Regulations.

Module 4: Wire Transfers

Module 5: Trade Finance

Module 6: Private Banking

Module 7: Risk-Based Approach in AML/CFT

Module 8: Real Estate Lending

Module 9: USA Patriot Act

Module 10: Internal/External Audit

Module 11: Compliance Communication Etiquette

Module 12: Lending and Investment

Cases

M O D U L E 1

Cash Transactions - Tellers

Tellers more than any other bank employee meet more customers more often and perform more bank transactions. In the fight against money laundering and terrorism financing, they are the first lines of defense. Their daily routine is receiving customers face to face. Therefore they should be alert to any unnatural or nervous behavior from customers without letting them notice their suspicion.

Target Employees:

- Tellers/Cashiers
- Teller Operation Supervisors.
- Customer Services Representatives (CSR's)
- Account Managers.

Be alert for:

1. Customers whom are unusually nervousness
2. Customers who are annoyed at having to follow certain reporting procedures
3. Customers refusing to carryout transactions after they have been informed of certain reporting requirements
4. Notice any unusual gesture or movement.
5. Two people apparently working together, with one conducting the transaction and the other observing not far from the teller window

Remember to:

1. Keep smiling and cool.
2. Satisfy the customer and please him/her.
3. Do not stop serving the customer/completing the transaction.
4. Have your job responsibilities and due diligence done.
5. THEN, if you have any doubt or suspicion, fill a Suspicious Transaction Report (STR) or report, by the stipulated means of communication, to your compliance.

Potentially Unusual Transactions or Activities or customer behaviors (RED FLAGS)

1. Large cash deposits or withdrawals which are unusual for that customer's activities.

2. Large numbers of small deposits which add up to a considerable sum.

3. Simultaneous cash transactions by apparently related customers.

4. Large cash withdrawals made from a business account not normally associated with cash transactions.

5. Large cash deposits using night safe facilities, thereby avoiding direct contact with the branch staff.

6. Large cash deposits made to the account of a natural or legal person when the apparent business activity of the natural or legal person would normally be conducted in cheques or other payment instruments.

7. Large cash withdrawal shortly after large credit from abroad.

8. Sudden large cash withdrawal from low activity account.

9. Unusually large and frequent deposits made by a natural or legal person whose ostensible business activities would normally be generated by cheques and other instruments.

10. Regular transfers abroad by non account-holder using small denominations or various currencies.

11. The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

12. The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

13. Deposits for a business entity in combinations of monetary instruments that are a typical of the activity normally associated with such a business (e.g, deposits that include a mix of business, payroll and social security cheques).

14. Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of the credits is significant.

15. Customers who constantly pay in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable or readily marketable instruments.

16. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

17. Numerous deposits of small amounts, through multiple branches of the same bank or by groups of natural persons who enter a single branch at the same time. The money is then frequently transferred to another account, often in another country.

18. Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

19. Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

20. The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

Difficult Situations:

The following difficult situations can be handled in the following way:

1. A customer has been observed carrying out a transaction that is unusual for the customer and under the advisement of management not only is a suspicious transaction report filed, but also the customer's transaction is not carried out.

When the customer asks why his transaction is not carried out.

The teller or customer representative replies that because the customer is requesting a transaction that is not the unusual transaction for the customer; the bank's policy is not to carryout the transaction at that time until it is reviewed by upper management.

2. When a customer is asked for the source of funds when opening an account, he replies that Bank B doesn't require such information.

The customer representative replies that their bank is just following the law and that if Bank B doesn't follow the law, eventually the regulators will find out. Does the customer want to do business with a bank that could have serious regulator problems? Problems which could have an impact on him?

M O D U L E 2

Customer Services Relationships (CSR)

Target Employees:

- Customer Services Representatives (CSRs)
- Account Managers.
- Tellers

A. Indicators for bank accounts to be considered when establishing a customer relationship with the bank:

1. Opening of more than one account by a customer is his name in the same bank without a clear reason, and existence of internal transfers among these accounts.

2. Payments or transfers by many individuals to a single account whether in cash or through internal transfers.

3. Opening of a customer of more than one account in the name(s) of his family members and being authorized to operate these accounts on their behalf.

4. Opening the account by customer with his continuous management of the account without him physically appearing to the bank staff for a long period of time.

5. The existence of bank accounts with address outside the region of the bank.

6. Existence of a large number of movements of large amounts in the account while the balances is maintained at a low or fixed.

7. Current or saving accounts used only to receive incoming drafts from abroad in a continuous manner.

8. Any individual or business whose account shows no normal personal or business related activities but is used to receive or spend large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

9. Reluctance to provide normal information when opening an account, providing minimal, fictitious or conflicting information, or information which is difficult or expensive to verify.

10. Customers who appear to have accounts with several banks in the same area, especially when the bank is aware of regular consolidation process from such account prior to a request for onward transmission of the funds.

11. Matching of debits with credits paid by cash on the same or previous day.

12. Paying large third party cheques n favor of the customer.

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

14. Substantial increase in deposits cash or negotiable instruments by professional firms or company if the deposits are promptly transferred between other customer company accounts.

15. Customer who decline to provide information which normally would make them eligible for credit or other valuable banking services.

16. Insufficient use of banking facilities (e.g. avoidance of high interest rate facilities for large deposits).

17. Maintaining a number of trustee or customers accounts not required by the type of business a customer conducts, particularly when cash deposits in such accounts are noticeable large amounts and include banking transactions conducted by persons whose names are listed in the circulars of the Central Bank.

18. A customer omits recording his permanent address on the application form for opening an account.

B. <u>List of possible types of high risk customers</u>

1. Non-resident customers.

2. Safe custody and safety deposit boxes.

3. Customer granted facilities against cash deposit.

4. Trusts and fiduciaries.

5. Existing customers changing to a new and different business.

6. Off-shore customers.

7. Account opened by intermediaries (lawyer, accountants…).

8. Customers failure to provide identification evidence.

9. Customers from high risk countries.

10. Politically Exposed Persons (PEP's)

11. Customer refused by other banks.

12. Money Service business (MSB) customers.

13. Charities and no-profit organizations.

14. Non-face to face customers.

15. Savings accounts in the name of third parties – savings schemes (e.g. Jam'iya account).

M O D U L E 3

Jordan AML/CFT Laws and Regulations

Target Employees:

- All Staff members.

A. Central Bank of Jordan (CBJ) Regulations on Money Laundering and Combating of Financing of Terrorism before Legislation 46/2007:

1. Circular No. 210/97, dated 18.11.1997 (Cancelled).

2. Circular No. 10/2001, dated 5.8.2001 (Cancelled).

3. Circular No. 29/2006, dated 28.9.2006 (Operative)

B. Banking Law No. 28/2000
Article No (93):

a. If a bank learns that the execution of any banking transaction or the receipt or payment of funds is related to or could be related to any crime or illegitimate act, the bank shall immediately notify the Central Bank accordingly.

b. Notwithstanding the provisions of any other legislation, upon receiving a notice pursuant to paragraph (a) of this Article, or upon knowledge from another source that the bank has been asked to execute a banking transaction or to receive or pay funds related or could be related to a crime or an illegitimate act, the Central Bank shall issue an order to such bank to refrain from executing the transaction or receiving or paying the funds for a period not exceeding thirty days. In the meantime, the Central Bank shall notify any official or judicial authority of the matter.

c. Disclosure of information by a bank under the provisions of this Article shall not be regarded as a breach of the obligation to maintain banking confidentiality. Such bank or the Central Bank shall bear no consequent liability.

C. Criminal Law No. 16/1960 and its amendments:

Article No. (147)

1. Terrorism is the use of force or threat of force to carry out an individual or collective act aimed at disturbing public order or endangering public safety and security by causing damage to the environment, public facilities or property, private property, international facilities or diplomatic missions, occupying or taking over such premises, endangering national resources or causing suspension of the application of the provisions of the Constitution and laws.

2. Any act relating to any banking transaction, in particular the deposit funds in any bank in the Kingdom or in any financial institution engaging in banking operations or the transfer of such funds by them to any party whatsoever shall be deemed a terrorist offence if it emerges that such funds are suspect and related to a terrorist activity. In this case, the following measures shall apply:

    a. Preventive seizure of such funds by a decision of the Prosecutor General and prohibition of their use until such time as investigative measures have been taken;.

    b. Investigation of the case by the Prosecutor General, acting in coordination and cooperation with the Central Bank and any domestic or foreign party concerned. If he finds that the banking transaction in question is related to a terrorist activity, the case shall be referred to the competent court.

    c. Any person who commits such crime shall be liable to a term of hard labor, and the staff member of the bank or financial institution who was responsible for effecting the transaction, if he had knowledge of the facts, shall be liable to imprisonment. The funds seized shall be permanently confiscated.

D. Anti-Money Laundering Law 46/2007

Synopsis from Jordan Regulations

(Law 46/2007 and CBJ 29/2006)

1. Commitment (Article 14):

The parties subject to the rules of this law shall commit to the following: (Article 14).

- They shall exert due diligence so as to know the customer's identity, his legal situation and his activity, as well as to know the true beneficiary through the

relationship existing between them and the customer and to carry out a continuous following up of the operations effected within a limit of a continuous with the customers.

- They shall not deal with persons of unknown identity or of untrue or illusory names.

- The unit shall be immediately notified, by the means or from adopted by it, about the suspected operations whether effected or not.

- They shall abide by the instructions issued by the regulators for implementing the rules of this law.

2. What is Due Diligence? (29/2006)

Central Bank of Jordan identifies due diligence in its regulation 29/2006 as; the identification and verification of customer of customer identification and beneficial owner and the continued follow up on transaction that are conducted through an on going relationship. Additionally, the verification of the nature of all future relationships between the bank and the customer and its purpose.

3. What Customer Identification Means?

Central Bank of Jordan procedures to identify and verify customer identity:

A. The bank should put in place systems to identity and verify customer identification to comply with the requirements.

B. The bank should view the official documents to identify the customer and to have a copy of those documentation signed by the relevant bank employee to certify that they are original copies.

C. The bank should take the required procedures to verify the validity of the data and information obtained from the customer using reliable, independent sources.

D. The following should be considered in normal person identification procedures:

- The full name of the customer.
- Phone numbers and work address.
- Permanent residential address.
- Nationality

- Activity type.
- Beneficial owners.
- Purpose of conducting business relationship.
- Names of persons authorized to sign on customers behalf.
- Any other information the bank considers necessary.
- Minor accounts: The bank should have the documents related to the
- Person who represent them legally to act on those accounts.

4. Tipping off (Article 15):

The law prohibits any disclosure of information, or tipping off customers or beneficiaries, directly or indirectly by any mean, about any of the procedures of notification or investigation or inquiry relevant to suspicious operations other than to the competent authorities.

5. Penalties (Article 24, 25):

Article 24: The law imposes penalties on all individuals involved, including the main perpetrator, the intervener and the instigator, a five year prison temporary hard labor and a fine of up to 1 million Jordan Dinars; repeat offenders receive double the penalty.

Article 25: Penalties also apply to banks and their staff members if they violated articles 14 & 15 of this law. The penalties could include imprisonment for a period of six months or payment of a fine up to ten thousand Jordan Dinars or a combination of both punishments.

M O D U L E 4

Wire Transferes

The wire transfer function in financial institutions is considered to be high risk and should be a high priority for monitoring. Certain wire transfers require customer due diligence and international best practices recommend that certain information be disclosed by the originating bank, intermediate bank and beneficiary bank.

Target Employees

- Customer service representatives
- Account mangers
- Wire transfer personnel
- Private banking

Reference

A. Central Bank of Jordan (CBJ) Regulations on Money Laundering and Combating of Financing of Terrorism before Legislation 46/2007

B. Circular No 29/2006, dated 28.9.2006

Wire Transfer Defined

A wire transfer is defined as any transaction carried out through the bank by electronic means on behalf of an originator person with a view to making an amount of money available to a beneficiary person at another bank regardless that the originator and beneficiary are the same person

Occasional Customer Defined

An occasional customer is defined as the customer who is not tied with a continuous relationship with the bank.

Wire Transfers Requiring Customer Due Diligence

Any wire transfer conducted by an occasional customer regardless of its amount must undergo customer due diligence. Customer Due diligence (CDD) is defined as the verification of the customer's identity and the beneficial owner and continuous follow- up on transactions that are conducted through ongoing relationships. Additionally the identification of the nature of all future relationships between the bank and the customer and its purpose.

The following transactions require customer due diligence for occasional customers:

(a) If the value of the transaction or (several transactions that appear to be linked) is above JD (10,000) or its equivalent amount in other currencies

(b) If the occasional transactions are suspected to be money laundering or terrorism financing

(c) Any wire transfer conducted by an occasional customer

If the bank is unable to complete customer due diligence measurements, it should not open the account or engage in any banking relationship with the customer or perform any transaction with the customer or perform any transactions to his/her account.

Required Information to be included in Each Wire transfer

For wire transfers which exceed JD 700 or any equivalent amount in other currency which is sent or received by all banks subject to Regulations of Anti-Money Laundering and Terrorist Financing No. (29/2006) Article 5, the following information shall be included:

For ordering Bank information

Originator's name, account number, national number or the identification document number, national number or the identification document number and nationality for a non-Jordanian. In the absence of an account for the wire transfer originator, the bank should establish a system by which a unique identity number is provided to the transfer originator.

For intermediary bank

Provisions to insure that the above information (ordering bank information) remains with the wire

For Beneficiary bank

If the bank processes an intermediary element of a wire transfer chain ratherthan being an originator or beneficiary bank, then the bank must ensure that all information that is attached to the wire transfer is retained with it.

The bank should put effective systems in place to identify the lack of wire transfer originator information required by the above. The bank should adopt effective risk-based procedures to deal with wire transfer originator information. One of these procedures is to, request the incomplete information from the wire transfer ordering bank. Otherwise the bank should undertake risk-based procedures in order to determine if it needs to refuse the wire transfer. Such a refusal would be based on the belief that the missing information is an indicator of unusual or suspicious activity.

In these cases the bank should consider making a suspicious activity report to the FIU immediately.

Suspicious Wire Transfers

a. wire transfer activity from high-risk countries where the customer has no apparent business purpose or when the activity is inconsistent with a customer's business or history

b. Periodic wire transfers from a personal account to high-risk countries

c. Large incoming wire transfers on behalf of a foreign client with little or no explicit reason.

d. Frequent or large dollar volume of wire transfers to and from high-risk countries.

e. Frequent wire transfers of large dollar amount.

f. Funds transferred in and out of an account on the same day or within a relatively short period of time.

g. Wire transfers ordered in small amounts, in an apparent effort to avoid triggering reporting requirements.

h. Transfers routed through multiple foreign or domestic banks.

i. wire transfers payments or receipts with no apparent links to legitimate contracts, goods or services.

j. Deposits of funds into several accounts, usually in amounts less than the required reporting threshold, and then placed into one master account and transferred, often outside the country.

k. Payment instructions to financial institutions to wire transfer funds abroad and instructions to expect an incoming wire transfer of funds in equal amounts of dollars or other currency from other sources.

l. The stated occupation of the customer is not in keeping with the level of the wire transfer.

m. Large wire transfers abroad with cash payment instructions.

n. Large cash withdrawals from a previously dormant accounts, or in which a significant amount of money had just been wired in from abroad.

o. Using an account as a temporary "pool account" for funds that are eventually transferred abroad.

p. Frequent large wire transfers in the account of a client from countries associated with drug manufacturing and trafficking,

q. Frequent wire transfers from the account of a legal entity into the account of a natural person, with no reference to the nature of the transfers.

r. Unusual wire transfers between connected accounts or accounts the have the same administrator or connected administrators.

s. Using credit lines and other financing means to make external transfers when the normal activity of the client does not justify the transaction.

t. Using wire transfers to make external down payments for imports where the merchandise was not shipped, the operation was not performed, the service was not provided until the deadline stipulated in the contract, not followed by the reimbursement of the down payment.

u. Frequent or large wire transfers for persons who have no account relationship with the institution.

v. Client receives wire transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with the normal course of business for the client.

w. Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity.

x. Wire transfers to free trade zones that are not in line with the client's business.

y. Regular deposits or withdrawals of large amounts of cash using wire transfers to, from or through countries that either are known sources of narcotics or whose money laundering laws are ineffective.

z. Any wire transfers to/from a third party when the identity of the beneficiary or counter-party is undisclosed

M O D U L E 5

Tarde Finance

(L/C's) Letters of Credit, (DC's) Documents for Collections

Trade-based money laundering is spread now more than the classical money laundering schemes through cash or transfers or Bank Drafts. It is the use of letters of credit, documents for collections, and other trade finance transactions to move money between countries.

Target Employees:

- Trade Finance personnel (L/C's, L/G's, D/C's)
- Customer Services Representatives.
- Account Managers.
- Branch Managers.

What is Trade-based money laundering?

The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, or of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

Red Flags for Trade-based money laundering:

1. Items shipped that are inconsistent with the nature of the customer's business (eg. A steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).

2. Customers conducting business in high-risk jurisdictions.

3. Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.

4. Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions (eg. Equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, and crude oil).

5. Obvious over- or under-pricing of goods and services.

6. Obvious misrepresentation of quantity or type of goods imported or exported.

7. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.

8. The shipment does not make economic sense (for example, the use of a forty-foot container to transport a small amount of relatively low-value goods).

9. The size of the shipment appears inconsistent with the scale of the exporter or importer's business activities.

10. The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities).

11. The transaction involves the receipt of cash or payment of proceeds (or other payments) from third party entities that have no apparent connection with the transaction.

12. The transaction involves the use of front (or shell) companies.

13. Shipment locations or description of goods not consistent with letter of credit.

14. Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.

15. Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the name of parties should prompt additional Office of Foreign Assets Control (OFAC) review.

16. Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.

17. Significant discrepancies appear between the descriptions of the goods on the bill of lading (or invoice) and the actual goods shipped.

18. Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.

M O D U L E 6

Private Banking

The guidelines for private banking module are based on the Wolfsber AML principles on private banking relationships.

Target Employees:

- Private Banking Officers
- Account Managers
- Customer Services Representatives (CSR)

The following guidelines are understood to be appropriate for private banking relationships.

1. **The bank will take reasonable measures to establish the identity of its clients and beneficial owners and will only accept clients when this process has been completed.**

2. Beneficial ownership must be established for all accounts. Due diligence must be done on all principal beneficial owners identified.

3. Accounts held in the name of money managers and similar intermediaries. The private banker will perform due diligence on the intermediary and establish that the intermediary has a due diligence process for its clients, or a regulatory obligation to conduct such due diligence, that is satisfactory to the bank.

4. Where the holder of a power of attorney or another authorized signer is appointed by a client, it is generally sufficient to do due diligence on the client.

5. Practices for walk-in clients and electronic banking relationships.
   A bank will determine whether walk-in clients or relationships initiated through electronic channels require a higher degree of due diligence prior to account opening. The bank will specifically address measures o satisfactorily establish the identity of non-face-to-face customers.

6. It is essential to collect and record information covering the following categories:
   a. Purpose and reasons for opening the account.
   b. Anticipated account activity.
   c. Source of wealth (description of the economic activity which has generated the net worth)
   d. Estimated net worth.

e. Source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening)
f. References or other sources to corroborate reputation information where available.

7. The circumstances of the following categories of persons are indicators for defining them as requiring additional diligence:
    a. Persons residing in and/or having funds sourced from countries identified by credible sources.
    b. Persons engaged in types of business activities or sectors known to be susceptible to money laundering.
    a. "Politically Exposed Persons" (frequently abbreviated as "PEPs"), referring to individuals holding or having held positions of public trust, such as government officials, senior executives of government corporations, politicians, important political party officials, etc., as well as their families and close associates.

    Relationships with Politically Exposed Persons may only be entered into with the approval from senior management.

    The reviews of PEPs must require senior management's involvement.

M O D U L E 7

Risk-based Approach in AML/CFT

Target Employees:

- Compliance Officers.
- AML/CFT Officers
- Risk Management Employees.
- Branch Managers

Risks can be identified and classified according to customer, business, product and service or geography.

A. Geographic High Risks:

Some customers are located in countries or conduct business with countries or areas where a higher risk of money laundering and terrorism financing exist. There is no definitive independent system for classifying territories and countries by their money laundering propensities, so most institutions should prepare their own criteria. Factors are whether or not a customer is from or has business ties with high-risk countries or areas. Financial institutions might consider the general reputation of the countries in question. Other countries may have politically unstable regimes and high levels of public or private sector corruption. Still others may be widely known to have internal drug production or to be in drug transit regions. The US State Department issues an annual report called "International Narcotics Control Strategy Report" rating countries on their money laundering controls. A Berlin-based organization, Transparency International publishes a yearly Corruption Perceptions Index, which rates countries on perceived corruption. Once such risks are compared and assimilated, jurisdictions can then be designated according to risk.

The following other identifiers are significant:

1. Drug producing countries.
2. Drug transshipment countries.
3. Drug user countries.
4. Secrecy jurisdictions/Tax havens.
5. Eastern Europe and Former Soviet Union.
6. African countries known for corruption.
7. High-risk countries and territories listed by FATF or any other international entity.
8. OFAC listed countries.

(e.g. Suggested List of High Risk Countries):

Afghanistan	Gambia	Mauritania
Algeria	Georgia	Mauritius
Angola	Ghana	Mexico
Armenia	Guatemala	Micronesia
Azerbaijan	Guinea	Mongolia
Bangladesh	Guinea-Bissau	Montenegro
Belarus	Guyana	Montserrat
Benin	Haiti	Morocco
Bolivia	India	Namibia
Bosnia & Herzegovina	Iran	Nauru
Brazil	Iraq	Nepal
Brunei Darussalam	Jamaica	Nicaragua
Burkina Faso	Kazakhstan	Niger
Burma	Korea (DPRK)	Nigeria
Burundi	Kenya	Niue
Cambodia	Kyrgyzstan	Pakistan
Congo (Republic)	Laos	Panama
Cuba	Lativa	Paraguay
Djibouti	Lesotho	Peru
Dominican	Liberia	Thailand
East Timor	Madagascar	The Bahamas
Ecuador	Macau	Venezuela
Equatorial Guinea	Malawi	Vietnam
Eritrea	Mali	
Ethiopia	Malta	
Fiji		

Regional High Risk Areas

A bank may be located in a region where surrounding countries or countries of close proximity are high risk. This is particularly true when close to areas experiencing conflict. Banks must be aware of the kinds of money laundering and terrorism threats poised by those countries. In relationship to this, border areas with such a country may pose significant risk.

Domestic High Risk Areas

Certain areas within a country may pose a risk for money laundering and terrorism, for example certain high crime areas, tourist areas, areas in close proximity to smuggling activities or drug production. Banks must consider not only areas historically considered high risk, but new emerging areas as well. Bank branches located in or near such locations require enhanced due diligence policies, procedures and controls.

B. <u>High Risk Businesses</u>:

1. Non-bank financial institutions such as money transmitters,
2. Check cashers and remittance services.
3. Travel agencies.
4. Casinos.
5. Import/export companies.
6. Jewel/gem/precious metal dealers.
7. Off-shore subsidiaries of banks and corporations.
8. Car/boat/plane dealerships.
9. Leather goods stores.
10. Broker/dealers.
11. Used truck/auto/machine part manufacturers.
12. Real estate brokers.
13. Art & antique dealers.
14. Any cash-intensive business such as restaurants, retail stores and parking garages.

*** What to Look for:**

- The use of shell companies where it appears to be an unnecessary complication and the using of less reputable legal and financial advisers to set up and/or maintain the corporation.

- Appropriateness of turnover levels, sudden fluctuations in turnover, variations in deposit/payment patterns due to a small number of large transaction; large purchases of travelers cheques or money orders resulting in encashment from a variety of countries, or the reverse.

- Payments to countries on the "FATF Non Cooperative List" outside of normal patterns; large purchases of travelers checks; fluctuations in transaction patterns out of line with normal business patterns.

- Trading patterns with high-risk countries not normally associated with the commodity in question; unusual fluctuations in turnover or types of financial instruments used.

C. <u>High Risk Products/Services</u>:

Any product which allows a customer to readily convert cash to a monetary instrument, or any product or service which allows a customer to readily move value from one jurisdiction to another and which conceals the source of those funds.

1. One off transaction/product.
2. Private banking facilities.
3. Non-customer wire transfers.
4. Complexity of transaction.
5. E-banking services: ATM, Internet banking, Electronic transfers, Credit cards, Smart cards.
6. International connected services/correspondent banking.
7. Trade finance services with no sensible reasoning or economical rationale (especially Documentary Credits).

Financial institution managers must consider the following:

Does the product or service have the following characteristics?

Have an especially high transaction or investment value?

Favor anonymity and allows payments to third parties?

Have unusual complexity?

Support high transaction volume?

Involve cross border transactions?

Support high speed movement of funds?

Require government verification of customer eligibility?

Another factor is the delivery channel of the product. Can the product be bought online?

The kinds, frequencies and amounts of funds used in bank products and services are another factor. Some customers may not be considered high risk by the minimal use of bank products or services, but when use of products and services is increased and the volume of transactions

and amount of funds used is high, this may require the customer to be placed in a high risk category.

D. High Risk Customers:

1. Non face-to-face customers.
2. Customers of safety Deposit Boxes.
3. Trusts and fiduciaries.
4. Off-shore customers.
5. Politically Exposed Persons (PEP's)
6. Powers of Attorney.
7. Money Service businesses (MSB"s)
8. Charities and Non-profit organizations.
9. Customers with complex ownership structures.
10. Customers with previous known criminal history.
11. Non-Resident Customers.
12. Customers failing to meet the standard verification requirement.

M O D U L E 8

Real Estate Lending

Target Employees

- Lending staff
- Private Banking
- Trust Managers
- MLRO
- Customer Services Representative

While the laundering of money through real estate may bring attention to the real estate community as a whole, commercial banks need to be vigilant because the second most common technique is that of using mortgages. Criminals that have no shortage of cash to invest in real property may obtain mortgages to avoid suspicions associated with large personal financing. Criminals may seek a mortgage to limit their equity in a home to minimize personal financial loss if the property is forfeited to the government. Criminals often use the illicit obtained funds for collateral, down payments and loan payments.

A. Money laundering Techniques

Registering of properties and/or a mortgage in the name of a nominee that hides the criminal ownership and source of financing for the property are the most common techniques. Such nominees include relatives, friends, business partners, lawyers, and shell or legitimate companies.

Manipulation of properties, over valuation or under valuation is another technique. Over valuation of real estate is when criminals over value properties in ordered to obtain the largest possible mortgage. This can be achieved by manipulation of the appraisal. Under evaluation of real estate is accomplished by the criminal omitting part of the purchase price. The amount listed on the contract is paid for with the mortgage. The part not appearing on the contract is paid in cash under the table. When the property is sold at fair market value, the criminal has converted the illegal income into what appears to be legitimate sales proceeds.

Flipping of properties entails the purchasing of properties with illicit funds and selling properties in a series of transactions each time at a higher price. This could include for example the reclassification of agricultural land as building land. Parties involved in the sales are from the same criminal organization. Land is ultimately sold to a legitimate buyer. Two objectives can be achieved, laundering of money and profit from the sale of the property.

A draft FATF Study, Money Laundering & Terrorist Financing through the Real Estate Sector focused on the use of corporate vehicles.

Launderers often:

- Use cash or certificates of deposits as collateral for loans
- payoff loans early
- default and leave collateral
- don't use proceeds for loan purpose
- (This often involves bank collusion)
- Possible characteristics money laundered loans are:

  - Request to borrower against assets held by the bank or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
  - Loans made on the strength of a borrower's financial statement, which reflects major investment in, and income from businesses incorporated in bank secrecy haven countries
    Request for loans to offshore commercial companies, or loans secured by obligations of offshore banks
  - Loan proceeds unexpectedly channeled offshore

- Third parties, unknown to the bank, who provide collateral without any discernable, plausible reason and have no close relationship with the customer

The lending department of the bank should as part of its loan review examine for:

(1) Loans repaid unexpectedly with funds from unknown sources or loans paid off with assets sold with no valid explanation;

(2) Loans dormant while other accounts are active;

(3) Loan purpose is not justified and the loan collateral proposed is cash;

(4) Loans not included in bank loan reports to the Central Bank of Jordan;

(5) Loans inconsistent with the earnings capacity of the borrower;

(6) Loan proceeds unexpectedly wired into an offshore bank or to a third party;

(7) Loan applications collateralized with certificates of deposit issued by a bank or an investment company from a high- risk country;

(8) Loan applications from offshore companies or for loans collateralized with offshore bank obligations;

(9) Loan applications made by new clients introduced by professional intermediaries (lawyers, financial advisors, intermediation companies, etc);

M O D U L E 9

USA patriot Act

Target Employees:

- Compliance Officers.
- AML/CFT Officers

US Money laundering legislation before September 11, 2001.

1. Money Laundering Control Act of 1986.
2. Omnibus Anti-Drug Abuse Act of 1986.
3. Anunzio-Wylie Anti-Money Laundering Act of 1992.
4. Money Laundering Suppression Act of 1994.

USA Patriot Act:

1. Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.

2. Ten sections or titles.

3. Title 3: International Money laundering abatement and Anti-Terrorist financing Act of 2001.

1- Findings and Purposes

- ”Correspondent banking facilities are one of the banking mechanisms susceptible in some circumstances to manipulation by foreign banks to permit the laundering of funds by hiding the identity of real parties in interest to financial transactions**”.**

- “Private banking services can be susceptible to manipulation by money launderers, for example corrupt foreign government officials, particularly if those services include the creation of offshore accounts and facilities for large personal funds transfers to channel funds into accounts around the globe”.

2- Section 311 – Special Measures

► Treasury Secretary, in consultation with others, authorized to impose special measures for domestic financial institutions and domestic financial agencies if determined that:

- Jurisdiction outside the US
- One or more financial institutions operation outside the US.
- One or more classes of transactions within or involving a jurisdiction outside the US.
- One or more types of accounts from institutions operations outside the US.

► **Are of "primary money laundering concern" to the US.**

- Maintain records and/or file reports with concerning aggregate amount of transactions or concerning each transaction.
- Beneficial ownership – take reasonable and practicable steps, as determined by the secretary, to obtain and retain information on beneficial ownership of any account maintained in the US by a foreign person.
- Payable-through accounts – ascertain identity and related information of customers using the account.
- Correspondent accounts – ascertain identities and related information regarding each customer who has use of correspondent account.
- Barring financial institutions from having correspondent relations with financial institutions.
- Orders for special measures must be issued along with a proposed rule (except prohibition)
- Order can only last for 120 days unless rule is in place by the end of the 120 days period.
- Secretary to issue regulations defining beneficial ownership of account addressing issues such as authority of fund, direct, manage and control account.

3- Section 312 – Special Due diligence

► Each financial institution that establishes, maintains, administers private banking accounts and/or correspondent accounts in the US for non-US person shall establish appropriate due diligence, and when appropriate, enhanced due diligence policies procedures and controls that are reasonable designed to detect and report instances of money laundering.

- **If correspondent accounts is requested or maintained by or on behalf of a foreign bank operating.**

► Under an offshore banking license.

► Banking license issued by a foreign country that has been designated non-cooperative with international anti-money laundering principles.

► Designated by the secretary as warranting special.

- Ascertain for each foreign bank, the shares of which are not publicly traded, the ownership.

- Conduct enhanced scrutiny of such accounts to guard against money laundering and report suspicious transactions.

- Ascertain whether foreign bank provides correspondent accounts to other foreign banks and if so identify those foreign banks and relate due diligence information.

- For Private Banking Clients

► Defined as:

- A client who is required to maintain a minimum aggregate deposit of funds or assets (in one or more accounts) of not less than $1,000,000.

    - Accounts established on behalf of one or more individuals who have a direct or beneficial ownership interest in the accounts.

    - Is assigned to or managed by an officer, employee or agent of the institution acting as a liaison between the institution and the client.

► Ascertain the identity of the nominal and beneficial owners, source of funds in order to guard against money laundering and report suspicious transactions.

► Conduct enhanced scrutiny of accounts maintained by foreign political figures, their immediate families and close associates.

4- <u>Section 313 – Shell Bank Prohibition</u>

► US financial institutions cannot establish or maintain correspondent accounts for or on behalf of a foreign bank that does not have a physical presence in any country – 60 days to terminate.

► Exception

- If the foreign bank is an affiliate of a bank that maintains a physical presence in the US or a foreign country.

- Is subject to supervision by a banking authority in the country regulating the affiliated institution.

- Physical presence definition.

5- Section 319 – Forfeiture of Funds

► Financial institution that maintains a correspondent account in the US for a foreign bank shall maintain in the US.

- Records identifying the owners of the foreign bank (by 12/25/2001)
- The name and address of a person residing in the US who is authorized to accept service of legal process for records regarding the correspondent account (by 12/25/2001)

► 7 days to provide information upon government request.

► Failure by correspondent to comply with or challenge summons or subpoena results in termination of account within 10 days of notice from government.

► Penalty - $10,000 per day.

6- Section 352 – Anti-Money Laundering Programs

► Each financial institution is required to establish an anti-money laundering program that includes, at a minimum:

4. Development on internal policies, procedures and controls.

5. Designation of a compliance officer.

6. Ongoing employee training programs.

7. Independent audit function to test programs

7- **Section 314** – Cooperation between financial institutions, law enforcement and regulators in sharing of information.

8- **Section 326** – Regulations on verification of identification.

9- **Section 327** – Bank Holding Company Act – now must consider effectiveness of companies efforts to combat money laundering, including overseas branches.

10- **Section 356** – SARs for Broker/Dealers – regulation published by January 1, 2002, rule finalized by July 1, 2002.

11- **Correspondent Banking**

- Under the act a financial institution must not establish, maintain, administer or manage a correspondent account in the US for or on behalf of a foreign bank that does not have a physical presence in any country.

- Establish records of ownership of their bank in order to assist US correspondent banks.
- Appointed an agent in the US to accept service of legal process for records regarding each correspondent account.

- Complete model certificates.

- Taken reasonable steps to ensure correspondent accounts are not being used to indirectly provide banking services to "shell banks"

- If requested, be able to produce records within 120 hours about anti-money laundering compliance or customers.

M O D U L E 10

Internal / External Audit

Internal /External audits are frequently a major source of criticism by regulators when conducting AML/CFT examinations. In addition to this criticism, regulators require the offending institutions to dramatically increase its independent testing or internal audit performance.

Effective internal/external audits are essential to the success of an AML/CFT program for several reasons.

1. Examiners use internal /external audits during the AML/CFT examination. Early in an examination regulators assess an internal/external audits thoroughness and findings, as well as how effective it tracks management's corrective action. Audits are also important to determine whether they, the examiners, can rely upon the audit group's results to better scope their work. If the examiner is unable to rely upon the independent audit, then they will have to broaden their scope of review and the depth of their testing.

2. Bank Management uses the internal/ external report. Audits are vital because, if done properly, they will inform senior management, compliance, and the lines of business and board of directors of AML/CFT compliance program weaknesses. If management and the board are unaware of deficiencies they are unable to devote resources necessary to develop and implement corrective action to remedy problems.

Target Employees

Internal Audit staff

Risk Management staff

MLRO

Board of Director's Audit Committee

Key to a successful internal/external audits are the following:

1). Highly qualified individuals performing the audit so that the bank can rely upon the findings and conclusions.

(2). A AML/CFT audit that is independent and performed by individuals not involved with the bank's AML/CFT compliance staff and whether persons conducting the audit report directly to the board of directors audit committee.

(3) An independent audit that is comprehensive, and timely.

Minimum Standards

Internal/external audits should at a minimum cover the following:

(1) The overall integrity and effectiveness of the AML/CFT program, including policies, procedures, and processes.

(2) AML/CFT risk assessment.

(3) AML/CFT reporting and record keeping requirements.

(4) Customer identification and verification program implementation.

(5) The role, responsibilities, independence and resources of the MLRO

(6) Training adequacy, including content, training schedule, and attendance tracking.

(7) Personnel adherence to the bank's AML/CFT policies, procedures, and processes.

(8) Appropriate monitoring of high-risk subjects (products, service, customers, and high-risk geographies.)

(9) The integrity and accuracy of management information systems used in the AML/CFT compliance programs, such as reports used to identify large currency transactions, reports to aggregate daily currency transactions, and to identify certain funds transfer and/or monetary instrument sales transactions.

(10) The adequacy of the audit coverage of the AML/CFT monitoring systems. If an automated system is not used to identify or aggregate large transactions, determine whether the audit or independent review includes review of other documentation to determine whether large currency transactions are accurately identified and reported.

(11). Coverage of the bank's suspicious transaction reporting system.

(12). Recommendations for corrective action.

(13). Sampling and testing to determine if the banks AML/CFT compliance program is effective

(14) Conclusion regarding the adequacy of the bank's internal /external audit.

Sampling and testing to determine if the banks AML/CFT compliance program is effective

At a minimum an AML/CFT internal audit should sample:

- customer accounts recently opened,

- transaction of high risk customers
- transactions from high risk products and services
- transactions involving high risk countries
- correspondent account files
- selected wire transfers

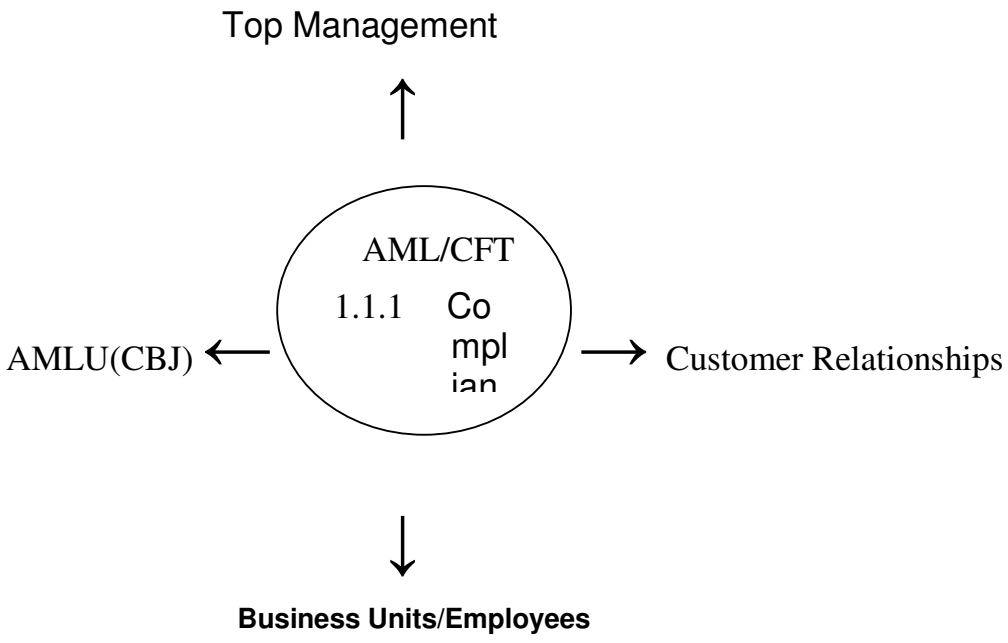
M O D U L E 11

Compliance Communication Etiquette

The compliance function (especially the AML/CFT Compliance) is very sensitive and important in the bank. Its importance lies in being the focal point of communication between the two structural levels of the bank; top management and other business units (employees) of the bank. The compliance also stands at the front of the bank before the regulatory body. At the same time, they have to keep good relationships with the bank customers.

Target Employees:

- Line Managers
- Compliance Officers
- Heads of Business Units
- Internal Auditors
- MLRO's



The Basel Committee on Banking Supervision, in its paper dated April 2005, entitled "Compliance and the Compliance Function in Banks" provided the following ten principles under the following titles:

Responsibilities of the board of directors for compliance

Principle 1

The bank's board of directors is responsible for overseeing the management of the bank's compliance risk. The board should approve the bank's compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the board or a committee of the board should assess the extent to which the bank is managing its compliance risk effectively.

Responsibilities of senior management for compliance

Principle 2

The bank's senior management is responsible for the effective management of the bank's compliance risk.

Principle 3

The bank's senior management is responsible for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the board of directors on the management of the bank's compliance risk.

Principle 4

The bank's senior management is responsible for establishing a permanent and effective compliance function within the bank as part of the bank's compliance policy.

Compliance function principles

Principle 5: Independence

1. The compliance function should have a formal status within the bank.
2. There should b a group compliance officer or head of compliance with overall responsibility for coordinating the management of the bank's compliance risk.
3. Compliance function staff, and in particular, the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have.
4. Compliance function staff should have access to the information and personnel necessary to carry out their responsibilities.-

Principle 6: Resources

The bank's compliance function should have the resources to carry out its responsibilities effectively.

Principle 7: Compliance function responsibilities

The responsibilities of the bank's compliance function should be to assist senior management in managing effectively the compliance risks faced by the bank.. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department should be clear.

Principle 8: Relationship with Internal Audit

The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function.

Principle 9: Cross-border issues

Banks should comply with applicable laws and regulations in all jurisdictions in which they conduct business, and the organization and structure of the compliance function and its responsibilities should be consistent with local legal and regulatory requirements.

Principle 10: Outsourcing

Compliance should be regarded as a core risk management activity within the bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the head of compliance.

Compliance Communication Guidelines:

A. Senior Management

1- As Basel Committee paper suggested, there should be an executive or senior staff member with overall responsibility for coordinating the identification and management of the bank's compliance risk and for supervising the activities of other compliance function staff.

2- Relationship with other management functions within the bank; Risk management and Internal audit.

3- Formal reporting to senior management (at least annually).

4- Freedom to express and disclose findings to Senior Management or Board of Directors or a Committee of the Board.

5- The right to conduct investigations on branches of the compliance policy.

6- Advise senior management on compliance laws, rules and standards.

B. Bank Business Units/Staff members

1. The right to communicate with any business unit or staff member and obtain access to any records or files necessary for functioning.

2. Seeking help or assistance from other business units (e.g. Legal or Internal audit).

3. Educating and training of staff members on compliance issues.

4. Act as a contact point within the bank for compliance queries from staff members.

5. Formal system to facilitate communication with all business units and staff members including (STR's) suspicious transaction report, whistle blowing or hot line.

C. Customers Relationships.

1. The compliance culture should concentrate on maintaining good relationships with customers through their branches and that good faith relationship prevails.

2. Staff members at the front end should understand that reporting customers or filling STR's does not necessarily create a hostile relationship or a termination to this relationship.

3. If customers show negative or hostile/angry impressions being under scrutiny or verification, be the opposite and keep serving them. Do not tipp-off your customers.

4. Remember: reporting (filling an STR) is your ultimate responsibility before affecting the customer's request or during the processing or even after.

D. AMLU (CBJ)

1. The relationship between the bank compliance and the AMLU is a legal regulatory one.

2. The responsibility of reporting any suspicious case to the AMLU should only occur if there are reasonable grounds for suspicion.

3. Unusual is not suspicious, therefore requires no reporting. Instead, it is only an indication or a red flag requiring further investigation and scrutiny until reaches the level of suspicion.

4. The CBJ, in its AML/CFT regulation No. 29/2006, stated some examples of unusual transactions like:
   a) Any cash transaction above JD 20,000.
   b) Any transaction with no clear economic reasoning.
   c) Large or complicated transactions which sounds, extraordinary.

5. Article 2 of Law 46/2007 defines the suspicious transaction as any transaction thought for any justified reason that it is related to proceeds of any crime of those stipulated in the law.

M O D U L E 12

Lending and Investment

Corporate customers are more vulnerable to the involvement in money laundering knowingly or unknowingly as they enjoy good facilities from their bankers and have suitable channel to pass money through.

Target Employees:

- Loans Officers
- Credit Facilities Employees
- Credit and loans administrators.
- Trade Finance Staff.

In handling corporate customer's transactions:

A. Be alert to the following indicators/red flags:

1. Large, unexpected or unprecedented F/X transaction instructions
2. Large or unusual settlement of securities in cash form.
3. Purchase of securities to be held in safe custody for no apparent reason.
4. Last minute changes to settlement instructions.
5. Rapid buying and selling of securities for no discernible purpose.
6. Increased use of safe deposit facilities, particularly using sealed packets.
7. Regular, large, unexplained instructions from countries commonly associated with drugs, terrorism, organized crime.
8. Any large transaction or series of transactions which appears unusual given our knowledge of the customer, his business and his normal account activity.
9. Frequent requests for, or paying in of, foreign currency drafts or travelers cheques.

B. Review loans and investments of customers introduce
C. d by foreign banks or from high-risk countries.

D. Examine investments to determine the following:

1. Accounts opened with large cash deposits or frequent purchases, for amounts that are large or unjustifiably split up, of financial instruments paid for in cash;

2. Dormant/inactive accounts that suddenly becomes active with large cash transactions.

3. Transactions not in keeping with normal practice in the market (e.g. market size, frequency, prices, early terminations of products at loss) especially where cash or refund checks to a third party are involved.

4. The customer engaged in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.

5. The customer made a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

6. The customer's account has unexplained or sudden extensive funds transfer activity, especially in accounts that had little or no previous activity.

7. The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk, bank secrecy haven or a country associated with terrorist activity (i.e., sanctioned countries, non-cooperative nations,), if applicable.

8. Securities presented for redemption in cash or for the purchase of other securities, without going through the customer's current account.

9. Buying and selling of a securities with no discernable purpose, in circumstances which appear unusual and not linked to investment or risk diversification.

10. Partial or total disposal of securities with the transfer of amounts to financial centers different from those specified in the contract, or in favor of persons other than those in whose names the securities were registered, or to persons in whose names they have been jointly registered only in the last few months of the investment contract..

Cases

Case 1: Hypothesis

Case 2: New Account Opening

Case 3: Account Opening

Case 4: Transfers

Case 5: Bankers Draft/Cheque

Case 6: Cheques for Collection (B/C'c)

Case 7: Customer Profile Analysis.

Case 8: Guarantees (L/G's) / PEP

Case 9: Dormant Account/Off-Shore business

Case 10: Corporate Account

Case 11: Loans

Case 12: Transfers, Front Companies, Off-shore

Case 13: Real Estate, Third Party Funds.

Case 1 : Hypothesis

TO KNOW ALAUNDERER, THINK LIKE ONE

Get $ 10 M (how do you do this part is your own business).

1. Fly overseas to a certain Region and take your millions with you.

2. Some "Areas" or regions sell legitimate off-the-shelf companies (some with complete board of directors). Buy one of these companies over the internet through a Lawyer.

3. Open a Bank Account in one of the banks under the company's name and deposit the balance of your money (knowing that no regulator impose financial penalty over banks).

4. When you arrive home, borrow $ 10 million from the company overseas by wire transfers.

5. Use funds to open a cash business (Restaurant" "Gas-petrol station" "Selling Cell phones – Prepaid Phone Cards" "Pizza Royalties chain stores" "Construction Material" "Buy one get one free" etc..

6. Appoint a jobless relatives to assist you on commission basis/sale.

7. At the end of each week take proceeds from your illegal money and deposit funds at the "Bank" as being from legitimate business.

Based on the above, do you think the launderer has done a good job?

Case 2 : New Account Opening:

- **Antonios is a Greek individual came to a foreign bank branch in Athens to open an account and start a relationship with the bank.**

- When asked by the CSR and Branch Manager about the purpose and the business relationship, Antonios said that he was one amongst a group of businessmen to buy the Olympic Airlines for a total of 1 billion Dollar deal.

- Antonios asked the bank at the beginning to open a current account to receive a 50 million Dollar transfer from Canada.

- The bank welcomed Antonios, but verified the Olympic selling deal from the Olympic Airlines themselves who they gave negative answer.

Indicators:

- Alleged information given by the customer.

Case 3: Account Opening

- A non-resident gentleman came to a bank to open a new account. The bank asked him to bring a reference letter from a reputable bank/financial institution as his home country is listed as a high risk country for corruption and drugs trafficking.

- The customer brought a letter from a financial institution duly signed by two signatories. The bank verified the signatories of the institution; one signature was correct but the other one was not found in the signatories book. The bank wrote to the institution asking confirmation on the signature and the signatory, but never received an answer, nor received the customer again.

Indicators:

- High risk country.
- False or forged document.
- Absence of verification

Case 4: Transfers:

- Omar Polski is a local citizen, but using his Polish (Polland) passport, he maintains a personal savings account in one of the banks in his home country.

- The customer is doing a lot of deposits into the account through other branches of the bank (inter-branch) and sometimes through ATM. He also asks frequently for outward transfers mainly to Polland.

Indicators:

- Using remote banking facilities.
- Frequent transfers with no supporting rationale.

Case 5: Bankers Draft/Cheque

- Mr. Clean has a corporate account in his residence country in one of the leading banks. He has an import/export business, and got an excellent trade finance facilities from his banker.

- One day, he came to another bank in the same country where he has a personal account and asked the bank to accept a cheque for JD 4.5m to be deposited to his personal account.

- When the bank asked about the source of fund, the customer said that it is his main banker's draft. This was not satisfactory to the bank, therefore they asked his main banker about the origin of the draft. The answer was "a transfer in USD from the US to the customer's account", but he asked for a draft in JD. The customer was refused and reported.

Indicators:

- Moving the money by layering using more than one banking product and more than one bank with no economic or justifiable reason.

Case 6: Cheques for collection – Bills for Collection (B/C's)

The bank received from an existing customer 4 checks for collection. The checks were close in dates but same amount, USD 9000 each and were third party checks for the same customer as the payee/beneficiary.

Indicators:

- More than one cheque for same amount just under the reporting threshold.

Case 7: Customer Profile Analysis

- A non- resident customer maintains two current accounts in a bank; one in local currency and the other in US Dollar. His profession is "businessman" which is mentioned in his home country passport. However, details on the business were known or verified at the bank.

- The account profile was flagged out for analysis and further investigation which showed the flowing transfer for 15 months.

- Inward Transfers	Outward
- No.: 14	- Amount: USD 7 m.
- Amount: USD 7.5 m	- Cash withdrawals, third party cheques.

No justification was given by the customer as to why was the money received, and what for, or where to. Transfers were coming from the US through a reputable bank.

Indicators:

- Lack of justifiable details.
- Moving money in and out.
- Absence of economic reasoning.

Case 8: Guarantees (L/G's) PEP

- An Ex-minister of country a (under-developed) lives in neighboring country B (Developed and active in trade).
  The Minister maintains personal and corporate accounts in one of the lading banks in country B since 5 years. His business annual turn-over does not exceed one million Dollar.

- One day, the customer informed his bank that he will be receiving USD 2 million transfer to his account. When he was asked about the purpose, he said he will ask the bank to issue a payment guarantee for the same transfer amount in favor of a governmental tourist agency in country A (his native country), and the transfer amount to serve as a cash collateral.

- A month later, USD 8 million transfer came into the customer's account, and an 8 million guarantee was issued for 3 months and handed over to the customer.

- 50 days later, the customer returned the original guarantee to the bank for cancellation. He also affected some domestic and overseas transfers, and some withdrawals, total of which did not exceed one million dollar. The rest of the inward transfer amount (about USD 7 million) remains in the customer's personal and corporate accounts.

Indicators:

- Politically Exposed Person (PEP)
  The bank must have performed or Enhanced Due Diligence (EDD).

- The customer entered a large trade financing operation beyond his turnover, with no supporting rationale, and not within his business domain.

- The customer received more money through a transfer than he previously told the bank.

- The customer did not provide the bank with documents regarding the subject deal nor has the bank received any document from the guarantee beneficiary.

Case 9: Dormant Account, off-shore business

- A bank noticed that a business account that had been dormant for some years suddenly became active with large-scale fund transfers. The bank account was originally registered to a company registered in an offshore jurisdiction. After US$150,000 was credited into the account, the firm used the funds to buy shares of a recently privatized Eastern-European Company – 'ABC Corp'.

- Three months later Brian, the representative who originally opened the account, deposited a total amount of US$250,000 in cash into the company account. Immediately after depositing the money, he wanted to transfer US$100,000 into a personal account at another bank. He claimed that the money came from his personal funds. When the bank asked him about the origin of these personal funds, he submitted commercial documentation showing that he had sold shares of ABC Corp – worth US$150,000 for US$250,000 to another Eastern- European company 'DEF Corp'. The difference of us$100,000 Brian explained as risk compensation, in the event the initial US$150,000 worth of shares invested in company ABC had been devalued. This would have been fairly high return on capital, when one takes into account that a return of US$100,000 over just three months would have equaled an annual interest rate of over 200 percent.

- The bank disclosed the transactions to the national FIU. By checking the records of its own intelligence and financial databases and liaising with other Egmont members, the FIU developed information that indicated Brian was the real owner of the offshore company. Also, it discovered that Brian was a member of the board of directors of company ABC. This suggested that the shares in company ABC might well have been knowingly sold at a lo

w value to the offshore company before being sold onwards for a higher price to a third party in effect, Brian siphoned off US$100,000 profit by using his own offshore company as a 'hidden ' stage in the share transfer.

- The FIU notified the corresponding law enforcement authorities that Brian was suspected of money laundering and fraud. As a result of the police investigation, Brian was arrested and prosecuted, with the court also confiscating the US$100,000 involved.

Indicators:

- Unusually high rates of return for a low risk business activity.
- Unrealistic explanation given by customer for account activity.
- Re-activation of dormant account.

Case 10: Corporate Account:

A European FIU received two disclosures from two different banks. Marvin, a foreign national, had presented five bank cheques to be credited into his newly opened company account. He told the banks that the US$1,600.000 involved originated from land sales in an African country that had been undertaken by his real estate company. The banks disclosed to the national FIU in view of the scale of the transactions and the lack of supporting data given by Marvin.

Investigations by the FIU established an interesting link to Marvin's father. His father was serving a prison term in another country for fraud, corruption and other criminal activities. Marvin's father had been sentenced to twelve years imprisonment after a foreign bank had collapsed as a result of a large-scale fraud that he had organized.

A while after the initial disclosure, Marvin phoned his bankers to request meetings to discuss further investments by his company, and both institutions made rapid disclosures to the FIU to alert them to the impending meetings. FIU contacted the local police who placed Marvin under surveillance as soon as he re-entered the country. Marvin was subsequently arrested on money laundering charges.

An exchange of information with the foreign country facilitated the preparation of criminal proceedings against Marvin on charges of criminal conspiracy, money laundering, and fraud. The foreign authorities also informed the FIU that Marvin's father had amassed a sizeable fortune. He had re-invested this money into real-estate companies and financing enterprises registered in his own name. Marvin's name and in the names of other family members. In the course of the investigation, Marvin's house was searched. The police found numerous documents related to financial transactions performed by Marvin's father.

Indicators:

New customer attempting large transactions with no supporting rationale.

Case 11: Loans

- A divorcing husband, laundered his U.S. money between Switzerland and Germany.

- Prior to the valuation/equitable distribution hearing in his divorce case, the husband alleged that he had a liability of $29 million owed to a prime bank in Germany because of an arm's-length business loan.. An investigation however revealed that his loan was back-to-back, (i.e a fully collateralized loan in which the borrower and the lender are one and the same).

- The husband had first secretly deposited $30 million into a Swiss bank account and next used that same $30 million to collateralize a Swiss bank guarantee for $29 million. By then using that Swiss bank guarantee as full collateral, the husband persuaded a German bank to issue a personal bank loan to him for $%29 million to be disbursed in Germany.

- After the loan principal was disbursed to him in Germany, The husband intentionally failed to repay his $29 million debt due and owing to the German bank. The husband's loan default meant that the German bank would collect $29 million transferred from Switzerland pursuant to the Swiss bank guarantee which had served as loan collateral. The loan default in Germany was actually the very means used to wash the money the husband had earlier deposited in Switzerland.

- The husband's financial transfers whom above had no economic benefit, as is usually the case where a back-to-back loan is used to hide assets. Back-to back loans however are not only sometimes used to conceal marital assets part of a divorce. They can also regrettably be used in a tax fraud to hide assets and income; by a debtor hiding assets from a creditor; or as a means to disguise monies which are the proceeds of a white-collar or other crime.

Case 12: Transfers, Front companies, Off-shore

Tom was a member of the Chamber of Deputies in his home country. He was able to support his family on his modest government salary until he began to develop a severe gambling habit. Increasingly in debt, and increasingly desperate for money, he formulated a plan to make him rich enough to carry on gambling indefinitely. As a project planner within the Ministry of Finance, he had the power to propose and approve schemes in a specific sector of the annual public works budget. It occurred to Tom that offering to approve schemes in return for a small monetary gift was an ideal solution to his money problems. Unsurprisingly, a number of businessmen were willing to pay him well for the guarantee of government business, and Tom became rich very quickly through his corrupt activities. Tom's friend Gina, who owned an exchange and tourism-company, was willing to help him launder the bribes that he was receiving. She used her employees as 'straw men' to create a number of

different bank accounts through which funds could be laundered – more thanUS$4,000,000 was laundered in total through such accounts. However, the cash payments and subsequent transfer (wire transfer) offshore risked attracting attention, and so Tom developed a more sophisticated laundering method - a fruit-delivery company. This company, which was owned by Gina's husband, laundered US $ 2, 700,000 in three months, disguising the transactions by creating false invoices which, were settled by the businessmen on Toms instructions. In this way, there was no direct link between Tom and the corrupt payments, and the businessmen had invoices to justify the payments should any questions be asked. The fruit company could then transfer the funds offshore as 'settlement' for fruit importation, attracting few suspicions.

However the earlier transactions had not remained unnoticed by the financial institutions involved. In view of the unusually large amounts of cash deposits and the rapid offshore transfers - especially in view of the declared low-income employment of the account holders - the institutions decided to disclose to the national FIU on a variety of accounts.

Following analysis by the FIU, the police had obtained a clear understanding of Tom and his corrupt activities, and have instigated a full investigation. Inquiries showed that Tom had used assessors of the House of Representatives to assist in the approval of his schemes.

One assessor, who did not have any involvement with the criminal operation, had had his signature counterfeited to obtain the necessary authorization. Another assessor had helped Tom by visiting the exchange and tourism company and receiving checks in his name. After receiving the checks, the assessor deposited the money into one of Tom's accounts.

Case Characteristics

PEPs

Front companies

Wire transfers

Trade financing

Offshore country

Case 13: Overvaluation of real estate and use of third party funds

The parents of Mr. X (MR. And Mrs. Y) purchased a residential property and secured a mortgage with a bank. In the mortgage application, Mr. Y provided false information related to the annual income and that regarding the ownership of another property. The property he had listed as an asset belonged to another family member.

Mr. and Mrs. Y purchased a second residence and acquired another mortgage at the same bank. Which Mr. X through his father's bank account made The monthly mortgage payments a large portion of the down payment came from an unknown source (believed to be Mr. X). This was the primary residence of Mr. X. Investigative evidence showed. That Mr. X made all mortgage payments through a joint bank account held by Mr.Y and Mrs. Y and Mr. X.

Mr. X then purchased a residential property and acquired a mortgage from the same bank. Mr. X listed his income (far higher than the amount he had reported to revenue authorities) from Company A and Company B. Mr. X made the down payment and monthly payments. Over two years, Mr. X paid approximately $130,000 toward the mortgage. During this time his annual legitimate income was calculated to be less than $20,000.

Mr. X also used his brother Mr. Z as a front man (nominee) on the title to purchase an additional property investigators discovered that Mr. Z had stated an annual income of $72,000 on his mortgage application listing his employer as Mr. X although Mr. Z had never worked for his brother, and his total income for two years was less than $13,000.

Mr. X made the down payments on this property, and his tenants who were members of Mr. Xs drug trafficking enterprise paid all the monthly mortgage payments. A total of $110,000 was paid towards the property until Mr. X and his associates were arrested.

Mr. X and his father purchased a fifth property. The origin of the down payment, made by Mr. Y was unknown but believed to be the proceeds of Mr. X's drug enterprise. Mr. X made monthly payments.

The use of the real estate was one of the many methods Mr. X employed to launder the proceeds from the drug enterprise. Recorded conversations between Mr. X and his associates revealed that he felt it was a foolproof method to launder drug proceeds.

Mr. X was convicted in 2006 of drug trafficking, possession of the proceeds of crime and laundering the proceeds of crime in relation to this case.

Indicators and Methods Identified in the Scheme:

- The use of real estate was one of many methods Mr. X employed to launder the proceeds from his drug enterprise. Recorded conversations between Mr. X and his associates revealed that he felt it was a foolproof method to launder drug money.

- The only problem he faced was securing a mortgage alone, so he had to use a nominee to secure the mortgage or to co-sign on the mortgage. A problem surfaced in this investigation when various properties were sold prior to a restraining order being served. The result in a portion of the funds being secured in a lawyers trust account, which cannot be restrained. It is investigator belief that up to $500,000 was being held in this trust account.

USAID Jordan Economic Development Program
Salem Center, Sequleyah Street
Al Rabieh, Amman
Phone: +962 6 550 3050
Fax: +962 6 550 3069
Web address: **http://www.sabeq-jordan.org**