Middle East & North Africa Financial Action Task Force

Typologies Report on "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF" 2007

TABLE OF CONTENTS

Summary:

Cross-border payment and funds transfer methods have been developed, no longer being limited to the traditional methods such as cheques, payment orders, bank drafts and traveler's cheques. The introduction of new payment methods based on internet, wireless devices or private networks has been considered as one of the main global developments in the field of funds transfer and movement.

Since money launderers basically rely on the available payment methods to move and transfer funds they obtain from illegitimate sources in order to conceal or camouflage the nature of those funds, and as terrorism financers use those methods to provide and finance terrorists and terrorist organizations with legitimate or illegitimate funds in order to help them carry out terrorist acts, this calls for studying the risks associated with the innovative cross-border payment and funds transfer methods in order to identify the associated risks in terms of the extent to which these methods may be used in ML/TF.

Accordingly, MENAFATF has paid particular attention to the payment methods in order to determine the extent to which it is possible for them to be exploited in ML/TF acts, as the first typologies project to be undertaken by MENAFATF, following Lebanon's suggestion to develop a typologies project concerning "Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF", which was unanimously approved by the 2nd MENAFATF Plenary.

In cooperation with the MENAFATF Secretariat, the project leaders (Lebanon) prepared a questionnaire designed basically to identify the payment methods available in the region and assess the risks associated therewith through exploitation by money launderers or terrorist financers. The questionnaire included several cross-border payment methods by way of example. Each country was given the opportunity to add any other payment methods that might be applicable.

The Secretariat received responses to the questionnaire from some member countries, and the analysis of those responses indicated that there was only one case (mentioned in Lebanon response, case No. 1 in part IV). The shortage of cases might be due to the non-widespread new payment methods and the different levels of experience among the member countries in extracting typology cases particularly since MENAFATF and several member countries thereof are new to the subject of typologies in general. For this reason it is recommended that studies of the payment methods, both existing and emerging, continue in order to discuss the possibility of exploiting them in ML/TF, and that the results of the present study be updated.

Introduction:

Recognizing the importance of cross-border payment methods and the volume of the risks associated with them being exploited by money launderers or terrorism financers, Lebanon suggested the MENAFATF typologies project concerning ***"Existing / Emerging Cross Border Payment Methods and their vulnerabilities to ML/TF".*** The 2nd MENAFATF plenary, which was held in Lebanon in September 2005, unanimously approved the suggested project, and thereupon, the project leaders, in cooperation with the MENAFATF Secretariat, prepared a questionnaire designed to achieve the following:

1- Identifying payment methods existing in the MENA region, determining their vulnerabilities to ML/TF.

2- Examining regulatory measures taken (if any).

3- Developing a complete study to be published in the MENAFATF typologies report.

Several points were taken into consideration in preparing that questionnaire, namely:

1- Suggestion of examples of payment methods, such as informal value transfer system, cash couriers, internet payment services, digital currency services (E-Gold, E-Silver, E-Platinum or E-Palladium), stored value cards, electronic wallet, and e-cash banking (Western Union, Money Gram), allowing each country the opportunity to add any other payment methods applied therein.

2- Identifying the size of the market where the various payment methods and fund transfers are used.

3- Identifying the extent to which these methods are subject to control, supervision and licensing requirement and whether informal establishments provide such services.

4- Identifying indications that those payment methods might be used in ML/TF.

5- The extent of actual cases known to relavant authorities such as the Financial Intelligence Units or the law enforcement authorities.

The Secretariat received responses from eight member countries[1], in addition to the USA[2], concerning this questionnaire. In this regard, it is worth noting that the names and terminology used may differ from one country to another in describing the same payment method. This report uses the most widely used terminology in practice.

This report is divided into five parts: Part I presents a historical background and previous studies. Part II reviews the different types of payment methods, while Part III reviews the questionnaire data and results of analyzing the responses received from

1- Jordon, Bahrain, Saudi Arabia, Oman, Qatar, Lebanon, Yemen, and Iraq.
2- U. S. response included a case (case No. 2 in part IV).

member countries. Part IV discusses practical cases related to the payment methods, and finally, Part V is dedicated to the conclusions and recommendations.

Part I: Historical Background and Previous Studies:

The payment methods and the extent of their possible exploitation in ML/TF has been the focus of the FATF attention since it started preparing and publishing the typologies reports. Most of FATF reports contained parts on this subject, particularly the following reports:

1. FATF Typologies Report on ML, June 1996

The report contained:

- A study on cash smuggling either through physical smuggling of money or cash instruments, or via shipping.
- A reference to the fact that modern electronic payment methods pose a new challenge in the field of AML, particularly through the introduction of the so-called "Smart Cards".

The report recommended that, despite the absence of an evidence of the exploitation of those electronic payment methods for criminal purposes, FATF should take the initiative by working with the concerned parties in order to identify the threats represented by those products and lay down appropriate security controls to prevent money launderers from actually exploiting those e-banking products.

2. FATF Typologies Report on ML, February 1997

This report discussed:

- "Alternative Payment Methods" and pointed out that there was a continuous and increasing activity in cross-border cash smuggling, which enables money launderers to move cash easily to neighboring countries through the land borders.

- The "Hawala System" which, as reported by many countries, is a money transfer system outside the formal banking system widely used within ethnic groups of African and Asian origins, this system includes transferring money outside the banking sector.

The report stated that it was difficult, at the time, to find out whether the APMs were large enough to be used by money launderers, given the fact that these methods were widely used for legitimate purposes, and that it was difficult to identify those who provide this service.

3. FATF Typologies Report on ML, February 1998

This report mainly focused on modern payment methods, concluding generally that modern payment systems developed gradually and spread widely, and despite the absence of cases of money laundering in this sector, the report discussed the risks that those new products might pose through their exploitation in ML. The fact that no ML cases through the use of modern payment methods were discovered may indicate the weakness and inability of the means necessary for detection or that modern payment methods do not pose any money laundering risks.

The report contained several cases related to different subjects such as physical cross border movement of cash (Case No. 3 in Part IV of the report).

4. FATF Typologies Report on ML, February 1999

This report was a continuation of the previous report with regard to studying E-Wallets, the "Hawala system" and Internet-based banking transactions. The practical cases included a case of funds transfer (Case No. 4 in Part IV).

5. FATF Typologies Report on ML, February 2000

- The reports included reference to the significant role that alternative remittance system appear to play in support of ML, and that a typical aspect of such systems was that they were based on ethnic, cultural or historical factors. The ARSs operate outside the domestic financial systems that are subject to control.

- The spread of these systems was due to the increasing number of immigrants and to the fact that this system was safe to a certain extent and less-costing, in addition to the fact that the anonymity of users. These features attracted persons to use the system in both legitimate and illegitimate activities.

- "Hawala System" was generally preferred because it was cheaper than effecting money transfers through the banking system, in addition to the fact that it is a 24-hour service available everyday of the year. It was based on trust and did not require the use of many documents.

The report recommended the continued study of the ARS and its relationship to ML. It stated that each system should be examined individually in order to develop a clear understanding of its role, method of operation and potential threats with regard to ML. The report said that this should take the form of rules that should be observed at the global level in order to prevent the use of these systems in illegitimate activities.

6. FATF Typologies Report on ML, 2003-2004

As of 2002, FATF typologies reports started to focus increasingly on terrorism and terrorist financing. Several related subjects, such as non-profit organizations and wire transfers were discussed.

The report of 2003-2004 contained several practical cases including a case of exploiting wire transfers in the financing of terrorism (Case No. 5).

7. FATF Typologies Report on ML, June 2005

The report contained the following:

- The ARSs were used to transfer money from one location to another outside the banking channels. In using ARSs, criminals tended to employ more sophisticated means in order to avoid detection and reach their goals. The report also discussed the factors that encouraged them to use these systems.

- The report referred to the difficulty of detecting the exploitation of these systems in terrorist financing because the financing may be made from legitimate sources. However the best ways of combating such financing lied in the implementation of the AML policies in terms of following the procedure of identifying customers and reporting suspicious transactions.

- The high-risk category of these systems included, cash courier, shop-front registered ARS, and covert ARS while the national and multinational franchised ARS were classified as medium-risk.

- Several indicators that may help banks, regulatory authorities and law enforcement bodies detect the use of such systems in ML and/or FT.

- A number of cases, including one involving informal remittance systems (Case 6).

The report concluded that the most effective way to detect undeclared transactions made through ARSs was to detect the settlement transactions made by these entities, for as soon as these systems carry out the settlement operations, the performance by the banks of the money laundering control operations in terms of identifying the customers and reporting suspicious transactions would tremendously help in such detection. The fact that settlement operations take place at an international level underlines the importance of the exchange of information among the regulatory authorities, FIUs and LEAs in order to prevent the criminal groups from using those ARSs for ML/TF.

8. FATF Typologies Report on ML, October 2006

- The report contained a study on the various types of payment methods, both traditional and nontraditional, including pre-paid cards, e-wallets and internet-based payment services.

- The overall results indicated that it was not easy to identify modern payment methods at a global level. However, it was possible to identify them at the level of individual countries through a questionnaire.

- The report identified several risk factors associated with payment methods and suggested means to reduce those risks.

The report recommended that the work team do the following in the future:

1) ***Provide guidelines to the countries concerning preventive measures that can be taken in order to limit the risks of using modern payment methods in ML and/or FT.***

2) ***Update this study with developments to the payment systems in addition to the typologies, and analysis of the risks two years later.***

3) ***Suggestions concerning what are involved in modern payment systems in order to examine them over the two-year period.***

Part II: Different Types of Payment Methods:

Payment methods vary from one country to another depending on several factors. The most important of these factors are the economic environment of the country, the degree of customers' banking awareness, the extent of technological advancement in the country and the applicable legislations, laws, and the regulations imposed by the regulatory authorities on the entities that provide these services. Payment methods are divided into two types:

A- Traditional Payment Methods

These are the generally recognized payment methods such as cheques, payment orders, bank drafts, traveler's cheques and money transfer services provided by the banks and other intermediaries or non-banking institutions. FATF has laid down a definition of the money remittance system as ***"the financial system which accepts cash, cheques and any other cash instrument or any value store at one location for payment of the equivalent amount in cash or in any other form to a beneficiary in another location"***.

B- Non-Traditional Payment Methods

The non-traditional cross border payment methods and cross-border fund transfers include the following:

1) Informal Value Transfer System:

This is an informal system for the transfer of funds whereby money remittance services are provided outside the official payment system channels. This system has different names such as the "Hawala Dar", the "Hundi" system and others.

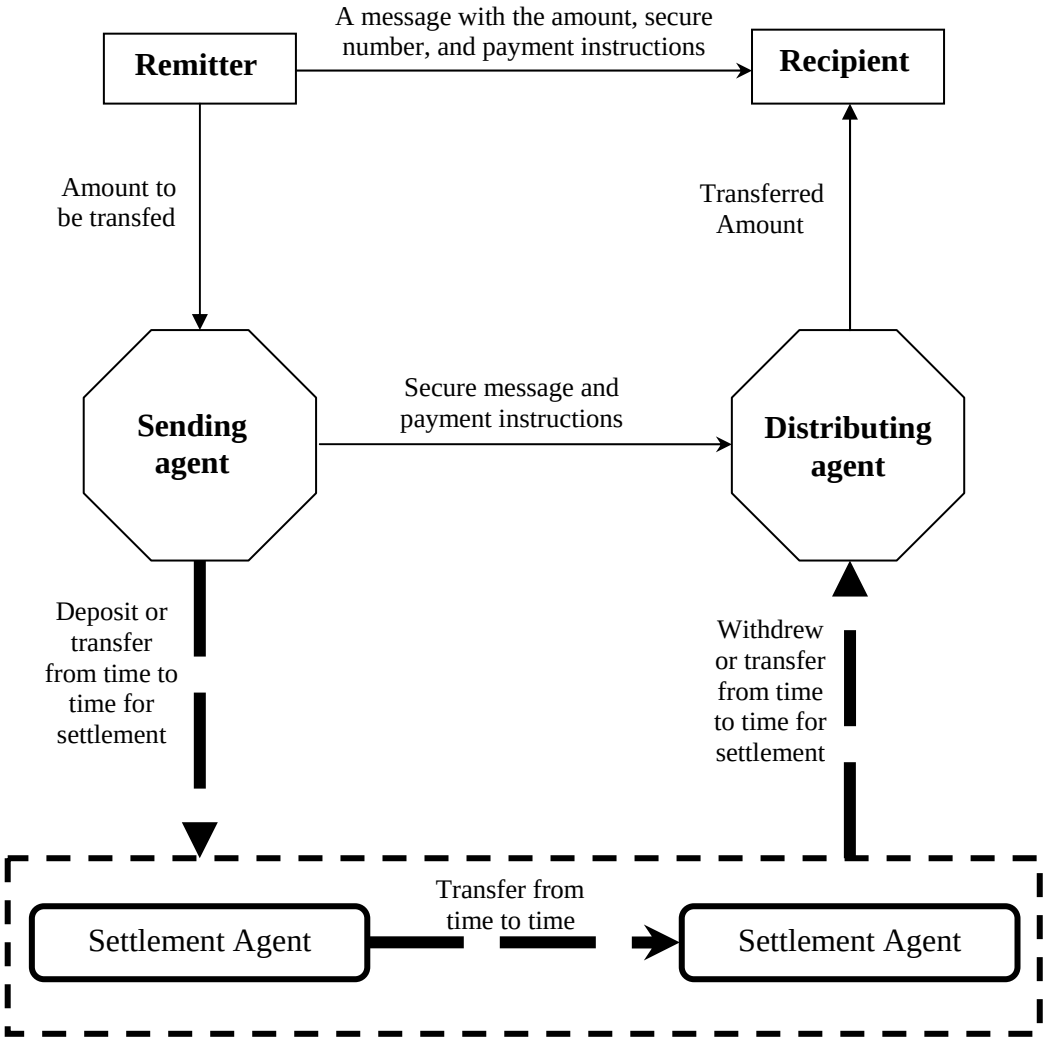
The best practices working paper[3] concerning the subject of the "Hawala" issued by MENAFATF states that this system does not require identification of the remitters, that the funds are transferred through an informal network and typically there is no physical or electronic transfer funds every time a remittance is made, for settlement takes place periodically between the remitter's intermediary and his counterpart in the beneficiary's country (the receiving intermediary), through intermediaries that usually are banks.

This system is based on three main elements: secrecy, performance of the transactions upon verbal instructions and mutual trust among the parties in this system, which are:

- **The remitter**, who is the person who requests the transfer of a certain amount to a recipient in another country.
- **The sending agent**, who receives the money to be transferred in consideration for a commission agreed upon.
- **The distributing agent**, who delivers the remitted amount to the recipient.
- **The recipient** who is the person who receives the remitted amount.

3- Best practice working paper issued by MENAFATF, December 2005.

The following figure[4] shows the relationship among these parties and the mechanism of this system:



2) <u>Cash Couriers:</u>

This involves the physical movement of cash and bearer negotiable instruments from one country to another. This process typically takes place through material transportation by a natural individual or moving by shipping.

FATF Special Recommendation IX on the physical cross-border movement of cash, which was added by FATF in October 2003 to the 8 Special Recommendations on terrorist financing, states that countries should apply such standards which will enable them to detect the physical movement of cash and bearer negotiable instruments, including the use of any declaration/disclosure system for such funds, and that competent bodies should have the legal authority that enables them to seize and freeze such funds or bearer instruments that they suspect are linked to terrorist financing or

4- FATF Typologies report on ML, June 2005, P. 9.

money laundering, or those that are not declared or disclosed properly, and they should impose deterring proportionate and effective sanctions against offenders.

The interpretative note to the recommendation specified two systems for implementation: the Declaration System whereby all persons who are in possession of money or bearer negotiable instruments exceeding a certain amount to declare such possession to the competent authorities. The second system is the Disclosure System, whereby all persons who are in possession of money or bearer negotiable instruments to disclose such possession to the competent authority when they are asked to do so.

3) Online payment services:

On-line payment services enable individuals to transfer funds or to buy items through the internet. Despite the limited availability of such services in several countries, it seems that a system called PayPal is the most widely used internet-based payment method.

This system enables users to send and receive funds through their email address. The person who wishes to use this system should first subscribe in the system in order to be able to receive and send funds by entering the email address of the recipient and the amount that he wishes to send or receive. The debit is charged to a credit card.

4) Digital Currency Services (e-gold, e-silver, e-platinum, and e-palladium):

E-Gold is a digital gold currency and an electronic payment system operated by E-Gold Co. Ltd, allowing users to invest in gold and precious metals.

Typically, an account is opened for the user at the company to enable him to transfer currency into E-Gold. In return, the user pays by various means such as cheques, cash, wire transfers, bank drafts or other means.

The user may claim his balance of E-Gold in the form of gold bullions or have it converted into banknotes or remitted to a bank account. He can also transfer the balance of the E-Gold account to a debit card without the need to know the name of the holder of that card. This will make it possible to use the card to withdraw the corresponding amount through an ATM.

5) Stored Value Cards:

The stored value cards contain a pre-paid cash value stored on a magnetic strip or electronic chip embedded in the card, thereby enabling users to effect financial transactions. They are also called pre-paid cards or smart cards.

Stored value cards are typically linked to an account that is opened and provided with funds for a certain amount. This kind of cards enables the use of the prepaid cash by the card holder. Although there are many kinds of stored-value cards used in various ways, they all operate according to a system that is identical to that of debit cards that

are ultimately linked to a bank account. The card may be issued and the bank account may be opened at a banking or non-banking institution.

Stored value cards are of two kinds:

5-1 Closed System Cards

These cards are issued for specific purposes and may be called "non-reloadable cards". These cards cannot be re-loaded when their value is used up, nor can their value be increased once they have been issued.

This kind of cards may be used for paying small amounts for commodities and services that can be purchased through the internet. The cards can be purchased for cash or through any payment methods. They are available in various pre-set amounts (below a set ceiling). Users may the cover layer which hides the secret number in order to enter the code that specifies the pre-paid value. Upon paying for goods and services purchased through the internet, the user should enter the secret number of the card thereby gaining access to the prepaid amount stored on the Server of the issuing company. This will enable the deduction of the amount due from the actual card balance.

5-2 Open System Cards

These are re-loadable cards that can be used within a wide range of locations and for a larger number of purposes. They can be used locally and internationally, and may be subject to restrictions limiting its use within a specific geographical area. These include Visa Card and Master Card which allow their holders to use them as debit cards to purchase goods or to withdraw cash through ATMs.

Users may claim the value of the cards by cashing out the balance through ATMs or by turning to the primary service provider for claiming the card balance.

6) Electronic Wallet:

This is an electronically stored value on a device similar to a card, and may sometimes be called a "Smart Card". It has a magnetic strip on which the account data are stored. This type of payment method allows the holder to deal with them as if holding money but in a different.

With certain kinds of e-wallets, value may be transferred from one card to another directly or to another person or retail outlet without the need for such transaction to pass through an intermediary account.

In view of the fact that the funds are stored on the "wallet", there is no need to make a direct communication or identify the holder because the purpose of this kind of payment method (the e-wallet) is to use as a substitute for cash in day to day transactions. They are used to make small disbursements such as in public transportations means or at vending machines.

7) E-cash banking (Western Union, Money Gram):

This kind of transactions include such operations as the transfer or receipt of funds through licensed institutions such as money transfer services (e.g. Western Union and Money Gram) that are licensed to deal in money by electronic means on behalf of their customers, whether on a regular or occasional basis, for certain fees.

Part III: Analysis of Countries Responses to the Questionnaire

This part covers the data included in the questionnaire, the responses received from member countries, the analysis of such data, and the key findings of the study. The responses received indicate that the payment methods used differ from one country to another.

It is found that in certain countries, like Yemen, payment methods are limited to cheques only, while in other countries, such as Iraq, payment methods include the SWIFT system, bank drafts, traveler's cheques and credit cards. Payment methods in Bahrain include the transfers via licensed services, such as Western Union (through two agents licensed by the Central Bank of Bahrain) in addition to stored-value cards. In Qatar, there are credit, debit, and pre-paid cards, while in Oman we found a variety of payment methods including SWIFT, telex transfers, credit cards, e-cash and instant remittance by using such international systems as Western Union and Money Gram.

In Lebanon, payment methods include e-cash banking (the receipt/transmission of electronic money by banks and other Licensed Money Transmitting Businesses), Visa Card, Master Card, American Express Card, and SWIFT. It was also found that Saudi Arabia and Jordan have the largest variety of payment systems; Saudi Arabia has credit cards, smart cards, electronic remittances, speed cash and an instant payment system called SPAN which includes credit cards, prepaid cards, ATM's, points of sale and SWIFT.

In Jordan, payment methods include a large number of systems such as payment cards (Visa Electron), credit cards (Visa/Master Card), Electron Prepaid Card, Visa Charge Card, Visa Revolving, e-wallet and e-cash (Western Union and Money Gram).

Despite the wide diversity of payment methods from one country to another, the analysis of countries responses to the questionnaire indicates that the volume of this market is not big.

Some countries gave examples of how certain payment methods are vulnerable to ML/TF, such as:

1- Prepaid cards issued without verification of customer identification, which may result in absence of any book keeping about card holders.

2- Payment cards can be used by individuals other than the original card holders who may withdraw funds through ATMs in different currencies and various countries, possibly to finance a terrorist act, group or organization.

3- Cards in general are to carry ship, mail and transport from one place to another

Countries responses revealed the existence of only one case mentioned in Lebanon's response (part IV).

Some countries suggested the adoption of certain procedures in an attempt to prevent the use of various payment methods by money launderers or terrorist financers. These include:

- To verify the identity of the card holder.
- On-site visits undertaken by regulatory authorities to assess the extent of FIs compliance with AML/CFT laws and regulations.
- Maintain and update local legislations and regulations in accordance with international standards.
- Building a consolidated data base of suspicious cases reported to the FIU in order for it to identify trends, indicators, and methods used in each case, thereby helping to prevent future occurrence of similar cases.
- To establish regulations and programs to monitor transaction and withdrawals made through payment cards thereby helping to identify unusual transactions.
- To set limits for stored value cards to prevent their use in ML/TF activities.

Part IV: Practical Cases

The received responses to the questionnaire contained only one case from SIC (Lebanon FIU), concerning a money remittance business (MRB) that had been the victim of a fraud scheme. The details of this case are as following:

Case No. 1 (Lebanon): Money Transfer

The SIC received a letter from a local law enforcement agency seeking its assistance in a case subject of an on-going investigation by the Interpol in connection with a money remittance business (MRB) that had been the victim of a fraud scheme perpetrated by one of its customers (Mr. Crook).

Mr. Crook, using false identification and other fraudulent means, had successfully managed to transfer a lump sum of money presumably from his personal bank account into the account of MRB, who subsequently transferred the funds into the account of Mr. Crook's accomplice (Mr. Crimino) opened with a local bank with false identification, in preparation for the scheme.

Following an internal audit examination of its own accounts, the foreign bank realized that the transfer into the MRB account was carried out by fraudulent means, and subsequently debited the said account and returned the money that collateralized the transaction to the original account. The MRB, through its lawyer, filed a lawsuit against both Mr. Crook and Mr. Crimino, claiming that it had been subject of a fraud.

Consequently, the SIC asked all banks and financial institutions operating in Lebanon to provide it with information about potential accounts held by Mr. Crimino. Following banks and financial institutions replies, the SIC conducted an investigation into the accounts of Mr. Crimino, which revealed the withdrawal of the original amount through two large cash withdrawals, one bank check, and repetitive small ATM withdrawals (totaling 40% of the original amount) over a period of one month, aiming at disguising the audit trail and ownership of the funds, and hence preventing any effective inquiry by the competent authorities.

As a result, the SIC lifted the banking secrecy off Mr. Crimino bank accounts and forwarded its investigation report to the General Prosecutor and the Interpol.

Case No. 2 (US Case):

According to a U. S. law enforcement agency, six individuals indicted in a fraud scheme in March 2004 used a digital precious metals exchange service to transfer some $50 million from 26,000 investors.

Six men who ran one of the largest online centers for trafficking in stolen credit and bank card numbers and identity information pleaded guilty in federal court. The U. S. Attorney for New Jersey says the plea is the last step in pulling the plug on the notorious "Shadowcrew.com" website. The one-stop online marketplace operated by the defendants was taken down in October 2004 by the U. S. Secret Service, closing an illicit business that trafficked in at least 1.5 million stolen credit and bank card numbers that resulted in losses in excess of $4 million. The illicit funds were laundered through digital precious metals accounts.

According to the shortage of cases we have selected the following cases relative to payment methods, from FATF typologies reports. This is to enrich the study, and widen member countries experiences in this field. Some of these cases are:

Case No. 3: Cross Border Cash

Facts:

Three suspicious transaction reports were received relating to a number of transactions which were carried out at Bank in country A whereby large amounts of money were deposited into accounts and then withdrawn shortly afterwards as cash. The first report was received in August 1994, concerning an account held by Mr. X. Upon initial investigation, the subjects of the reports (X, Y and Z) were not known in police databases as being connected to criminal activity. However further investigation showed that X had imported more than 3 tons of hashish into country A over a 9 year period. Y had assisted him on one occasion, whilst Z had assisted in laundering the money.

Most of the money was transported by Z as cash from country A to country B where X and Z held 16 accounts at different banks, or to country C, where they held 25 accounts. The receipts from the bank in country A for the withdrawn money were used as documentation to prove the legal origin of the money, when the money was deposited into banks in country B.

Results

X and Y were arrested, prosecuted and convicted for drug trafficking offences and received sentences of six and two years imprisonment respectively. A confiscation order for the equivalent of US$ 6 million was made against X. Z was convicted of drug money laundering involving US$ 1.3 million, and was sentenced to one year nine months imprisonment.

Lessons

1. Financial institutions should not accept proof of deposit to a bank account as being equivalent to proof of a legitimate origin.

2. Carrying illegal proceeds as cash across national borders remains an important method of money laundering.

Case No. 4: Money Transfers

Facts

In July 1997, the police arrested Mr. X the leader of a drug trafficking group in country A. The subsequent investigation revealed that X had remitted part of his illegal proceeds abroad. A total of USD 450,000 was remitted via three banks to an account on behalf of suspect X's older brother Y. Transfers were made on five occasions during the months between April and June 1998 in amounts ranging from USD 50,000 to USD 150,000).

Another individual, suspect Z, actually remitted the funds and later returned to country A. On each occasion, Z took the funds in cash to the bank, exchanged them for dollars, and then had the funds transferred. Each of the transactions took about one hour to conduct, and the stated purpose for the remittances was to cover 'living expenses'.

Results

Suspect X was convicted for violating provisions of the anti-narcotics trafficking law, and the anti-money laundering law.

Lessons

This case is a good example of a case derived not just from suspicious transaction reporting but also as a follow-up to traditional investigative activity.

Case No. 5: Wire Transfers

An investigation in country A of company Z, which thought to be involved in the smuggling and distribution of pseudoephedrine, revealed that employees of the company were sending a large number of negotiable cheques to company B (to be cashed). Additional evidence revealed that the target business of company B was acting as an unlicensed money remitter.

Based on the above information, search was conducted about the Company Z and analysis of the documents and bank records. As a result of the search indicated that the suspects had wire transferred money to a terrorist group.

Later that year the investigators engaged in a series of co-ordinated searches. Three subjects were arrested and approximately USD 60,000 in cash and cheques were seized. Additionally, a bank account was identified containing approximately USD 130,000. The subjects are currently awaiting trial.

Case No. 6: Alternative Transfer Systems

An investigation was started by the police of Mr. X, who was the manager and the principal shareholder of company C, which is located in country A. This company works in the field of selling prepaid phone cards, food products, airplane tickets and above all, provided short term credits, money exchange services, cheque cashing and money transfers to country B's illegal immigrants in country A. the largest activity for company C is international transfers (approximately 85 % of its turnover).

Mr. X organized a system that allowed money transfers between country A and country B where he had bank accounts and capital. He arranged for family members in country B to deliver these transfers to the beneficiaries. The remitters deposited the money directly into Mr. X's account in country A either with in local currency or in USD. The increasing amounts of the money transfers from country A to country B forced Mr. X to use cash couriers.

In order to ensure the security of cash transfers, Mr. X started to use, at the beginning of 1999, a company specializing in international remittances. The company E, based abroad, held a bank account in bank F in country A, and similar companies G, H and I, were later used.

Company E's transfer orders were directly completed by the client on a company E dispatch note. Then, Mr. X sent it by fax to the company E. The investigators discovered that the transfer orders were also sent by e-mail. Mr. X deposited cash into the account opened by company E in bank F. Mr. X generally required his clients to divide their transactions into smaller amounts whenever they were above USD 3 000.

The fact that company C was primarily an illegal transfer business became evident through the study of dispatch notes. From 4 September 1999 to 30 September 1999, intercepted faxes indicated some 3,600 transfers to country B, approximately EUR 2 million. These operations involved 1,300 recipients in 78 cities in country B and 900 bank accounts in 40 different banks.

As of March 2000, the investigators saw a dramatic increase, in the number and volume, of transfers made by company C. If the company made the transfer without middleman, it received a 5 % commission of the amount of the transfer. When the cash went through companies E, G, H or I, Mr. X shared the commission. The use of these companies presented the advantage of minimizing the risk of loss or the risk of confiscation.

Mr. X was sentenced to 3 years imprisonment (including 2 years of suspended sentence) in 2004. Other members of the system also received jail sentences.

Part V: Conclusion and Recommendations.

Countries' responses to the questionnaire indicate the presence of few emerging payment methods in the MENA region.

The responses also indicate that all institutions providing these services are licensed, regulated, and supervised.

The shortage of cases may be attributed to the following causes:

1- The limited spread of new payment methods.
2- The different levels of experience among member countries in extracting typologies particularly since MENAFATF and several member countries thereof are new to the subject of typologies in general.

In view of the small number of responses received and the absence of sanitized cases, it is difficult to reach a conclusion reflecting the situation in the MENA region concerning the vulnerability of the payment methods to ML/TF. For this reason, we recommend the following:

1- To continue studying the cross border payment methods (existing and emerging) and their vulnerability to money laundering and/or terrorist financing, and update the results of this study.

2- To urge all countries which have not responded yet to the questionnaire to respond thereto after they complete the study of their own systems, for the purpose of reaching an overall assessment of payment methods associated risks in the region as a whole.

3- To expand the selection of typologies cases beyond incidents in which suspects have been convicted, including cases pending before courts, suspicious transaction reports containing strong indicators of ML/TF, as well as those under investigation or referred to investigation.

Annex: MENAFATF Payment Methods Questionnaire.

Country or State:		
Name of the organization:		
Contact Person:		
Contact details	Phone #:	E-mail address:
Date:		

1. What is the name of the Payment Method? (Existing or emerging)
2. How long has it been available in your jurisdiction?
3. Please provide detailed description of the payment method
4. What is the estimated number of Domestic Service Providers? (Please include statistics for the last 3 years)

5. What is the estimated number of account holders (users) who are using this payment method? (Please include statistics for the last 3 years)
6. Are there any ceiling limits on the transaction(s) executed through the payment method described above (i.e. amount transferred, uploaded, stored, etc..)? If yes, what is the ceiling limit?
7. Is there any evidence of ML/TF vulnerabilities associated with the payment method described above? If yes, please provide some examples.
8. Is the payment method subject to local laws and regulations? If yes, please provide illustration of the national requirements (in terms of CDD, record keeping, reporting suspicious transactions and others) imposed on payment service providers in relation to the payment method described above. Also please give reference to the relevant legal provision

9. Is the payment method described above subject to any supervision by a competent authority? If yes, please provide details.
10. Is the payment method described above subject to reporting obligation to a national agency with a public database? If yes, what is the applicable threshold amount?
11. Please provide some examples of sanitized cases involving the use of payment method as conduits for ML/TF
12. Does the local regulation stipulate sanctions against non-compliant service providers? If yes, please provide reference to the relevant legal provision.
13. In the presence of a regulatory regime applied to the payment method described above, are you aware of any illegal operator(s) in your jurisdiction?

14. If the answer to question 13 is yes, was the operator subject to any legal action by imprisonment, fine or by either penalty?
15. In case the payment method described above is not subject to local regulation, do you plan to issue a new regulation setting minimum standards to be observed by concerned service providers?
16. Based on cases investigated, were you able to establish a trend of indicators associated with the payment method described above.
17. If the answer to question 16 is yes, are you providing the financial sector with a list of indicators on the recent trends and techniques associated with the use of the payment method described above to help them identify and report suspicious transactions?
18. If such list exists, is it being updated regularly and is it published on your website?

19. Does your local law and regulation allow you to share information on trends and indicators with any regional or international FIU? If yes, please give reference to the relevant legal provision.
20. What measures do you recommend to minimize or limit misuse of the payment method described above?