Understanding the details of financial crime: the new MENAFATF *Typologies Report*

Since its creation more than ten years ago, MENAFATF has grown in stature and sophistication to become the leading voice in the fight against financial crime in the Middle East.

One of MENAFATF's most successful initiatives has been the publication of its biennial *Typologies Report*, detailing case studies and patterns of crime that have been detected by Financial Investigation Units throughout the Middle East. *Arab Banker*'s editor, Andrew Cunningham, explains the importance of the *Typologies Report* and summarises some of the case studies that it presents.

All banks in the Middle East agree on the importance of fighting financial crime. It is not just the financial penalties imposed by regulators, or the financial cost of the crimes themselves, or the reputational risks that have pushed the issue of financial crime to the top of senior managements' agendas. Major international banks are cutting correspondent banking relationships with institutions that are perceived to have insufficient controls.

SUMMARIES OF SOME OF THE EXAMPLES OF THE CASE STUDIES IN THE MENAFATF REPORT

Corruption that facilitates money laundering/terrorist financing

The suspect deposited three cheques for LD 4 million into his bank account, but he had never made deposits of this kind before and there had been no account movement in the previous two years. The branch manager at the bank referred the case to the local Financial Investigation Unit (FIU) which recognised that the source of the funds paid into the account had been identified as a suspect ('W') in a previous transaction. Suspicious elements in this transaction included: over-invoicing, use of shell-companies, 'structuring' of cash deposits, and the fact that W was a suspect in a previous transaction.

Laundering the proceeds of corruption

A bank regulator became suspicious while conducting an inspection of a bank under its control and, specifically, while studying the accounts of one of the bank's customers. The customer held several accounts and most of the movements through the accounts comprised large cash deposits that were inconsistent with the nature of his business. Furthermore, the customer did not use banking products other than cash deposits and transfers. The customer transferred his salary into the accounts but the accounts showed no movements reflecting personal expenses. Areas of suspicion included: holding several accounts in one name, depositing large amounts of cash that were inconsistent with the nature of the business, and focussing on cash deposits without the use of any other banking instruments.

Use of offshore banks, international commercial companies and offshore trusts

An FIU received a suspicious transaction report about Company A that was receiving large amounts of money by transfer from Country B, and then promptly transferring them to several other countries, some of which were classed as tax havens. The FIU discovered that the transfers from Country B were being made monthly by a public company and that the recipients in the tax havens were shell companies. It was noticed that one particular company in one of the tax havens ('C') received the majority of the money. The FIU discovered that Company A was receiving the proceeds of bribes arising from a contract under which the public company in Country B would supply military equipment to a government authority in Country C. It was further discovered that the company in C that received most of the funds was owned by the brother of the person who had concluded the contract with the arms supplier in Country B.

Trade Based Money Laundering (TBML)

A customer arranged a letter of credit for €2.4 million from his bank to finance the import of machines from abroad. He then submitted shipment documents to the bank in order to complete the transfer of funds. The bank discovered that the merchandise had not arrived – the customer claimed that the merchandise had broken down in a port before its arrival. Further investigation by the bank established that the documents presented by the customer were false. The customer's objective had been to enable the transfer of funds out of the bank and into a bank in another country. Suspicious elements in this case included: submitting false documents, and claiming that the ship carrying the merchandise had broken down in a port before its arrival.

Underground banking/alternative remittance systems/hawala

A bank reported that a local individual was gathering funds from different people of his nationality and then making deposits and internal transfers in his own accounts. He would then make deposits and internal transfers into the accounts of several

Another point of agreement is that everyone within a bank has to play a role in identifying and rooting out financial crime. To be effective, the fight against financial crime cannot be viewed as a 'Compliance' matter, a 'Legal' matter, or simply consigned to the Operational Risk department. Front-line staff – tellers in the branches, telephonists in the call centre, and the technicians monitoring internet banking systems – have to know what to look for and when to sound the alarm.

Of course, a customer who regularly deposits large amounts of cash will always arouse suspicion. But financial criminals are usually more subtle than to do something so obvious. (Though one of the biggest challenges in the Middle East is that cash is still widely used for legitimate purposes as a result of underdeveloped banking systems.)

So what are the signs that a transaction might be part of a criminal action? What should staff on the front line look out for? Those are the questions that the MENAFATF *Typologies Report* tries to answer.

The report identifies 17 types of transactions, all relating to money laundering or terrorist financing (ML/TF). Examples include: Trade Based Money Laundering; Human Trafficking and Smuggling; Precious Purchases such as antiquities; racehorses and cars; and Using Shell Companies.

By analysing the case studies, MENAFATF is also able to identify the most common techniques and tools used by criminals to implement their crimes. Most obviously, it is banks that are by far the most misused institutions. Nearly three-quarters of all case studies submitted to MENAFATF involved the use of banks, whereas exchange companies were used in only 14% of cases. (The remainder involved the use of 'border regions'.) Bank transfers were the financial instrument used most frequently, closely followed by cash deposits. Forged documents or financial instruments were the most frequently used techniques to effect a crime, with overseas funds transfers the second most frequent. As for indications that a crime was taking place, the existence of forged documents was, unsurprisingly, the most frequently cited, but the second most frequent were examples of 'disproportionate value' (where funds or cash being employed are inconsistent with the transaction they are supposedly financing), repetitive transactions and transactions whose size is inconsistent with the usual account movements. ■

MENAFATF

MENAFATF was created in November 2004 as an 'FATF Style Regional Body' (FSRB). FATF is the 'Financial Action Task Force' that was created in 1989 by the G-7. It has published recommendations on how to counter money laundering, terrorist financing and proliferation. It has 36 members, one of which is the GCC. Saudi Arabia has observer status. MENAFATF has 19 members, including all Arab countries and the State of Palestine.

In francophone countries, MENAFATF is known as GAFIMOAN, the acronym of its name in French: Groupe d'Action Financière du Moyen-Orient et de l'Afrique du nord.

companies. The amounts the suspect was collecting on a monthly basis ranged from SR150,000–200,000 which was inconsistent with the nature of the suspect's business. The internal transfers were also inconsistent with the suspect's business. Under investigation, the suspect was unable to prove the legitimacy of the transactions or the source of funds (either incoming or outgoing from his account).

Use of new payment systems

A company opened owned a bank account and signed up for electronic banking. The company sold cards through its website that provided cardholders with various benefits (medical assistance, car rentals, car breakdown services, etc). The bank suspected that, in practice, the company was selling fictitious cards and that its true purpose was to provide a conduit through which money that had been fraudulently acquired could be transferred to beneficiaries, while disguising the true identities of the beneficiaries. The bank's suspicions appeared to be confirmed by the following points: the company issued a very large number of different types of cards, the company appeared on Mastercard's list of suspicious operations, and the company withdrew money from the bank in cash.

Human trafficking and smuggling

The suspect was self-employed and received internal transfers into his bank account from regions bordering his own country. He also made cash deposits varying from LD50,000 to LD200,000. He then distributed funds out of his account through internal transfers and through cheques that he deposited himself for the benefit of another person ('B') in the same bank. The bank became suspicious because: the account was being used to receive and distribute money that originated in high-risk areas bordering the account holder's country into accounts of natural and legal persons that had no relationship with those border regions and B's account was categorised as a 'government employee' account, but the amounts received were inconsistent with that. For example, in the first seven months of 2013, the account showed a debit balance of LD42,465 million and a credit balance of LD42,524 million.

Using shell companies

A suspect ('A') opened two bank accounts at Bank 'S'. The first account was personal and the second was in the name of a company. Three months after the accounts were opened, the company account received a transfer of TD134,000 issued from a public treasury account under the title 'VAT Recovery'. Suspect A transferred the full amount to the personal account and then used most of it to buy two plots of land. The remainder he withdrew in cash. Around the same time, Suspect 'B' created a Company and opened an account at Bank S. Three months later, B's company received a transfer for TD276,985 issued by the same public treasury account. Suspect 'B' withdrew the full amount in cash straight away.

Financial transfers/using bank accounts abroad

The suspect received large and repeated amounts of money from abroad and each time gave the same explanation for the transfer (family obligations). After reviewing the transactions, the FIU discovered that many of the transactions were clustered together over short time periods and that these transfers were originated by only three people. The FIU was suspicious of the way the transfers were structured/timed and the repeated use of transfers for a single purpose. It asked the FIU in the country issuing the transfers for information about the three individuals.