In this part, suspicious activity indicators and case examples specific to individual sectors are presented. You may learn more about money laundering and terrorist financing risks specific to your sector by going through the information provided. Though the information is sector specific, you are recommended to go through the case studies of the other three sectors as well. That will certainly enhance your understanding of money laundering and terrorist financing. Please note that the suspicious activity indicators listed are not exhaustive. Suspicious transactions usually involve a number of indicators. In making assessment, businesses should not rely on this alone and should consider all pertinent information.

3.1 Remittance Agents and Money Changers

Remittance agents and money changers (RAMC) face a significant money laundering threat. They offer a range of services, which are attractive to criminals:

(a) money exchange services which can be used to buy or sell foreign currencies, as well as consolidating small denomination bank notes into larger ones;

(b) exchanging financial instruments such as travellers cheques, Euro cheques, money orders and personal cheques; and

(c) telegraphic transfer facilities.

Criminals like to use RAMC as vehicles for money laundering and channelling funds to terrorists because they are not as stringently regulated as traditional financial institutions. RAMC's internal control systems are usually less equipped to guard against money laundering. This weakness is compounded by the fact that most of their customers are occasional ones, which makes it more difficult for RAMC to "know their customers", and thus makes them even more vulnerable.

3.1.1 Suspicious Activity Indicators

3.1.1.1 General

(a) Remittances in excess of the "norm" of the customer having regard to his financial situation, income level, usual transaction scale, etc. without good reasons;

(b) Escalating levels of remittance activity of an individual customer above what is expected from original "Know Your Customer" assessments:

(i) pattern of transactions has changed since the business relationship was established;

(ii) the transaction is different from the normal business of this customer; and

(iii) the size and frequency of the transactions are not consistent with the normal activities of the customer;

(c) Personal remittances sent to destinations that do not have an apparent family or business link;

(d) Remittances made outside migrant remittance corridors - e.g. Asian foreign domestic helpers remitting funds to South America;

(e) Reluctance of customer to give an explanation for remittance;

(f) Personal funds sent at a time not associated with salary payments; and

(g) Requests for a large remittance but settling for smaller amounts to avoid requirement to produce proof of identity.

3.1.1.2 New Customers

(a) Difficulties are encountered when checking the customer's identity/the customer is reluctant to provide details of his/her identity;

(b) There is no genuine reason for the customer using the services of a remittance agent;

(c) The customer wants to carry out a transaction using a large amount of cash;

(d) The cash the customer using is used notes and/or in small denominations;

(e) The customer requests currency in large denomination notes;

(f) The customer will not disclose the source of the cash (in particular where transactions involve international transfers or foreign currency);

(g) The explanation for the transaction is unreasonable having regard to the amount involved; and

(h) The customer has made an unusual request for collection or delivery.

3.1.2 Below are four case examples for illustration.

Case Example 1: Remittance Agents Used to Pay Costs of Drug Trafficking

A drug syndicate regularly recruited female couriers and sent them to a drug-producing country on package holidays. Frequently, the couriers would have to extend their stay whilst awaiting delivery of the drugs. The drug syndicate would therefore use a remittance agent to send funds to the couriers to pay for the living expenses whilst awaiting delivery of the drugs.

The drug syndicate used false names to pay cash to remittance agents at a level not requiring production of proof of identity. The couriers collected the money, which was sent to them usually in names different from their true names.

Key Message

Detection by the remittance agent requires an understanding of the role of the destination country in drug trafficking and questioning the remitting customer about the purpose of the transaction.

Law enforcement relies on good record keeping by the remittance agent to show the use of false identities in the prosecution of such cases. Access to records at both ends of the transaction is essential.

Case Example 2: Remittance Agent Utilizing an Unwitting Correspondent Agent in a Fraud

A European remittance agent had a correspondent relationship with a remittance agent in Asia. The Asian agent settled payments for remittances originating from the European agent, and asked the European agent to pool the reimbursements and direct them in large payments to some third parties in Asia. The reimbursements were in fact paid to exporters who had overstated their exports. The receipt of funds from Europe was used to validate their claim for tax rebates for overstated/nonexistent business deals.

In this case, the European remittance agent unwittingly used the money paid in settlement to finance a fraud. This also obscured the audit trail.

Key Message

This example illustrates the need for remittance agents to be cautious when entering into correspondent relationship and transactions with agents in jurisdictions with weaker regulatory regimes.

Case Example 3: Remittance Agent's Failure to Report a Suspicious Transaction

A registered remittance agent was requested by an occasional walk-in customer to receive an inward foreign currency remittance in Australian dollars equivalent to HK$5 million for onward transfer to China in Renminbi.

The inward remittance was received and upon confirmation of receipt, the customer changed his instruction, requesting to withdraw the proceeds of the transfer in Hong Kong dollars. The remittance agent complied with the revised instruction and paid the customer HK$5 million in cash.

Two days after the transaction was completed, the bank advised the remittance agent that the originating bank in Australia had requested the funds to be restrained, alleging that the transaction was fraudulent. However, the remittance agent did not make a STR.

The matter was subsequently investigated and the transfer was confirmed to be the proceeds of a fraud.

Key Message

Despite the circumstances of the transaction and subsequently being placed on notice as to the questionable nature of the transfer, the agent failed to make a STR. As soon as the agent had grounds to suspect that the transaction might be illegitimate, he should have made a STR.

Case Example 4: Remittance Agent Involved in Missing Trader Intra-Community Fraud (MTIC Fraud)

MTIC fraud is common in EU member countries. It is started by a trader buying goods from a country within EU free of Value Added Tax (VAT). The trader then sells the goods at VAT-inclusive prices to customers, and finally absconds without paying the VAT. Very often, the goods would continue to move through a chain of transactions and will eventually be exported to another country, e.g. a Middle East or Asian country. The goods may end up at where they originated and are ready to go around again. It is not uncommon to find the same goods going round and round five or six times in just a few months.

MTIC fraud typically involves fund transfers amongst companies in EU, Middle East and Asia, including Hong Kong; and is associated with companies that trade in computer parts, mobile phones, and other relatively high valued and easily transportable technological items. The banking community in EU countries has identified and disrupted the financial activities associated with this type of fraud. MTIC fraud syndicates have therefore switched to using remittance agents to transfer funds. The transactions will appear normal to the remittance agents at both ends of the transactions, unless they are aware of the fraud profile.

Knowing and understanding the nature of business performed by the remitter will generally reveal that the size of transactions cannot be supported by the purported commercial activities as MTIC fraud related remittance transactions are typically large and frequent. The remittance agents remitting and receiving the money should be able to detect this type of fraud by examining the business details behind the transactions.

Key Message

For large and frequent remittances, both the ordering and receiving remittance agents need to ascertain whether there is any suspicious circumstance. They should compare details of the originator and the ultimate beneficiary to determine whether the transaction makes any business sense.