ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

Investment Business

Sector Specific AML/CFT Guidance Notes

October 2019

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

Contact:
AML Unit, Enforcement Division
Financial Services Authority
PO Box 58
Finch Hill House
Bucks Road
Douglas
Isle of Man
IM99 1DT

Tel: 01624 646000
Email: aml@iomfsa.im
Website: www.iomfsa.im

Contents

1. Foreword

For the purposes of this sector specific guidance, the term "Investment Business' refers to a business conducting activity that would require a licence under Class 2 of the Regulated Activities Order 2011 (as amended in 2019)[1].

2. Introduction

The purpose of this document is to provide some guidance specifically for the investment business sector in relation to anti-money laundering and countering the financing of terrorism ("AML/CFT"). This document should be read in conjunction both with the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 ("the Code") and the main body of the AML/CFT Handbook ("the Handbook"). It should be noted that although guidance is not law, it is persuasive. Where a person follows guidance this would tend to indicate compliance with the legislative provisions, and vice versa.

This document covers unique money laundering and financing of terrorism ("ML/FT") risks that may be faced by the sector and provides further guidance in respect of approaches to customer due diligence where it may vary across between sectors.

This document is based on the following documents:

- FATF Money Laundering and Terrorist Financing in the Securities Sector[2] and
- FATF Risk-based Approach Guidance for the Securities Sector[3].

The Authority recommends that relevant persons familiarise themselves with these documents and other typology reports[4] concerning the investment business sector. Also, some case studies are included to provide context to the risks of the sector.

The Island's National Risk Assessment ("NRA") is being refreshed at the time of writing and this document will be updated in due course following the publication of the NRA findings which is anticipated to take place in late 2019.

3. Risk Guidance

The investment business industry is a broad sector and the ML/FT risks will vary for each business based on a wide range of factors such as the type of products they supply, their customers and delivery channels.

[1] https://www.iomfsa.im/media/2586/regulatedactivitiesorder2011.pdf
[2] http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf
[3] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Securities-Sector.pdf
[4] Also, see the FCA document: Understanding the Money Laundering Risks in the Capital Markets

There are a number of different business types in this sector, therefore this document covers some of the general risk factors common to the sector as a whole and then focusses on particular individual business types where necessary.

Vigilance should govern all aspects of the business' dealings with its customers, including:

- account opening;
- providing advice to a customer;
- customer instructions;
- transactions into and out of customer accounts;
- ongoing monitoring of the business relationship;
- technology / security issues if there is an online element to the business relationship; and;
- any outsourced / delegated services.

3.1 General Higher Risk Indicators

As with the basic elements of a risk assessment, discussed under Part 3 of the Handbook, the following activities may increase the risk of the relationship. Just because an activity / scenario is listed below it does not automatically make the relationship high risk, the customer's rationale / nature / purpose of the business relationship etc. should be considered in all cases.

If a business is unable to obtain a satisfactory explanation from a customer in the event of the following situations, features, or activities, or any other features which cause it concerns, it should be determined whether this is suspicious or unusual activity. As stated in paragraph 13 (Ongoing monitoring) of the Code:

In the event of unusual activity, the relevant person must:

- perform appropriate scrutiny of the activity;
- conduct enhanced due diligence ("EDD") in accordance with paragraph 15 of the Code; and
- consider whether to make a disclosure and in the event of a suspicion of ML/FT an internal disclosure must be made.

If activity is identified as suspicious, appropriate steps must be taken as set out in paragraph 15 of the Code which state the relevant person must:

- conduct enhanced due diligence, unless the relevant person believes conducting enhanced customer due diligence will tip off the customer; and
- make an internal disclosure.

Please refer to Part 7 of the Handbook for further detail of the Island's suspicious activity reporting regime.

This list of higher risk indicators is by no means exhaustive, and relevant persons should be vigilant for any transactions where suspicion may be aroused and take appropriate measures. Also please see the list of red flags included at 3.2.

- where a customer is reluctant to provide normal information or provides only minimal information;
- where a customer's documentation cannot be readily verified;
- the customer is reluctant to provide the business with complete information about the nature and purpose of the relationship including anticipated account activity;
- the customer is located in a high risk jurisdiction;
- transactions involving numerous jurisdictions;
- the customer is reluctant to meet personnel from the firm in person and / or uses a "front person";
- the customer engages in frequent transactions with money service businesses;
- the customer has no discernible reason for using the businesses' services, or the businesses' location;
- the customer has a history of changing financial advisers / businesses and using a number of businesses in different jurisdictions;
- the customer's address is associated with multiple accounts that do not appear to be related;
- the customer is known to be experiencing extreme financial difficulties;
- the customer is reluctant to invest in more appropriate securities when those securities would require a more enhanced CDD procedure;
- the amount, or nature of, the investment does not seem in line with the customer's usual pattern of activity;
- the customer with a significant history with the securities business abruptly liquidates its assets to remove wealth from that jurisdiction or makes investments with very short holding periods;
- the customer enquiries about how to quickly liquidate accounts without explaining their reasons fully;
- the customer opens an account / product without any regards to loss, commissions or other costs associated with that account / product;
- the customer acts through intermediaries such as money managers or advisers in order not to have their identity registered;
- the customer exhibits unusual concern with the businesses' compliance with Government reporting requirements / AML/CFT policies and procedures;
- the customer funds deposits, withdraws or purchases financial / monetary instruments below a threshold amount to avoid certain reporting / record keeping requirements;
- wire transfers / payments are sent to, or originate from high risk jurisdictions without apparent business reason;
- the securities account is used for payments with little or no securities activities; and
- the customer's transaction pattern suddenly changes in a manner that is inconsistent with the customer's normal activities or inconsistent with the customer's profile.

3.2 Red Flags

In addition to the above higher risk indicators, there are some factors that would automatically be "red flags" in relation to that particular relationship and would therefore be suspicious activity. Appropriate steps as explained in section 3 of this document, and the Code, must therefore be taken. This list of red flags is by no means exhaustive and is as follows:

- where it is identified a customer provides false or misleading information;
- where it is identified a customer provides suspicious identification documents;
- the customer does not provide the business with relevant / accurate information about the nature and intended or ongoing purpose of the relationship, including anticipated account activity;
- the customer is secretive / evasive when asked to provide more information;
- when requested, the customer refuses to identify a legitimate source of funds or source of wealth;
- the customer refuses to provide details on beneficial owners of an account or provides information which is false, misleading or substantially incorrect;
- the customer enquires about how quickly they can end a business relationship where it is not expected;
- where the business relationship is ended unexpectedly by the customer and the customer accepts unusually high fees to terminate the relationship without question;
- the customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for;
- the customer is known to have criminal / civil / regulatory proceedings against him / her for crime, corruption, misuse of public funds or is known to associate with such persons; and
- the customer is interested in paying higher charges to keep their identity secret.

3.3 Risk factors specific to the sector

The following section of the guidance covers some of the risk factors specifically related to the provision of discretionary and advisory asset management, financial advice, stockbroking and custodians. When considering these activities there could be both retail and non-retail customers. Further guidance surrounding the risk assessments is outlined in Part 3 of the Handbook.

A number of risk assessments must be carried out by sectors as set out in the Code, including:

- business risk assessments (paragraph 5);
- customer risk assessments (paragraph 6); and
- technological risk assessments (paragraph 7).

Considering the technological risk assessment specifically, this must estimate the risk of ML/FT posed by any technological developments, such as the use of online delivery channels, to its business. An assessment should be undertaken whenever a relevant system is introduced or changed.

Investment business services are increasingly being delivered and / or supported by innovative technological solutions which reduce the administrative burden and the need for human intervention. These developments can change the ML / FT risks posed by an activity in particular due to the speed with which securities transactions can be executed and settled.

In relation to transaction monitoring systems, relevant persons should be aware of any limitations of solely using an automated system. Where transactions are complex involving multiple products and counterparties an automated system may not provide enough coverage to mitigate risks.

Examples of innovative areas include Trading Platforms, Crowdfunding and Robo Advice. By their nature online solutions are non-face-to-face and as such attract and increased ML / FT risk factors. Also, over recent years a number of automated KYC / CDD solutions have come on to the market. Such packages offer a wide variety of services, for example:

- client information upload;
- verification of customer identity;
- verification of address;
- bank account details; and
- sanctions checking.

These services can be run daily, or in some cases offer real time verification. These electronic data verification packages have become widely used given the cost and time efficiencies they provide, however when placing reliance on third parties for any aspect of KYC/CDD you should consider section 3.1.4 of the Handbook.

4. Customer due diligence

Considering the customer risk assessment, within this sector, depending on the activities you undertake, your customer could be a corporate entity including a fund, an individual or both. A customer risk assessment must be undertaken on your customer in accordance with paragraph 6 of the Code. Please see the Handbook at part 3.3 for general guidance on risk assessing a customer.

Part 4 of the Handbook (see the standalone part 4 of the Handbook which is in use until the main body is fully updated) sets out how to identify and verify the identity of the customer in relation to both a natural and legal person. It also provides general guidance on the timing of identification and verification of identity.

Part 4 of the Code requires that CDD procedures are undertaken in relation to a customer prior to, or during the formation of a business relationship. The customer would usually be the person seeking to form the business relationship (although it must be determined if the customer is acting on behalf of someone else). For details of particular concessions which may be relevant please see section 5 of this document and Part 6 of the Handbook.

4.1 Use of Intermediaries

Within this sector an intermediary (or a number of intermediaries) may be involved in the customer relationship. Where this is the case, it does introduce a further risk in that there can be numerous parties involved in a transaction, and it is likely these firms would have not met, or have contact with, the underlying customer. Where appropriate, relevant persons must comply with the provisions of paragraph 9 of the Code (Introduced Business). Please also see the stand alone guidance document the Authority has issued on this area.

Where an intermediary is used, a relevant person should analyse any specific risks arising from a further party being involved in the relationship. Involvement of an intermediary may vary depending on the particular products and services provided and which party is meeting the customer. It is imperative to understand the number of layers involved in the relationship and ensure enough information is held to comply with the Code and to identify any suspicious activity in relation to a relationship.

4.2 Discretionary and Advisory Asset Management

Investment management includes both discretionary and advisory management of assets and investments. It therefore includes the business undertaken by asset managers, investment advisers and investment managers in managing the customer assets.

Discretionary managers are given the power to decide upon stock selection and to undertake transactions within the portfolio according to an investment mandate from the customer.

Advisory relationships differ in that the manager does not have the authority from the customer to deal in investments on the customer's behalf. In some cases the customer will execute their own transactions using the manager's advice.

There is little distinction between the ML / FT risks associated with discretionary and advisory asset management activities. In both cases the business could handle client money and therefore the service could be susceptible to the risk of ML at all three of the stages of the traditional ML model, placement, layering and integration.

Discretionary / advisory managers must ensure they obtain the full range of customer information / verification required by the Code regardless of whether there is discretionary power given. It should be ensured that this customer information / activity is appropriately monitored on an ongoing basis as per the Code requirements.

4.2.1 Risk guidance

Specific risk factors to consider (in addition to the generic factors listed in section 3 of this document) in relation to the discretionary / advisory asset management sector may include:

- the type of customer i.e. is it an individual, fund, company or trust;
- whether there is any PEP involvement;
- whether the customer is undertaking activity inconsistent with the advice being provided;
- whether there is transfer of funds without involvement from a custodian;
- whether there are frequent and unexplained additions to the investment portfolio; and / or;
- whether there are frequent and unexplained requests for assets to be realised and the funds paid away.

4.3 Financial Advisers

Financial advisers give customers advice on their investment needs and provide assistance in selecting appropriate products. A financial adviser is typically licenced to give advice to the customer and also to arrange deals on the customer's behalf.

Generally financial advisers do not have the regulatory permissions to hold client money so there is unlikely to be involvement in the placement stage of ML. Financial advisers could however be involved in the layering and integration stages.

The vast majority of financial advice is conducted on a face to face basis which is a mitigating factor for some of the ML / FT risks faced by the business. A financial adviser must carefully consider any non face to face business and conduct appropriate CDD based on the location of the customer, or where they are conducting business activity.

Financial advisers must ensure they obtain the full range of customer information / verification required by the Code both where full advice is given and also where execution only activity is taking place. It should be ensured customer information / activity is appropriately monitored on an ongoing basis as per the Code requirements.

Financial advisers may act as eligible Introducers to other regulated businesses and therefore any relevant ML / FT risks concerned with this activity should be mitigated appropriately.

4.3.1 Risk guidance

Specific risk factors to consider (in addition to the generic factors listed in section 3 of this document) in relation to the financial advice sector may include:

- the type of customer i.e. is it an individual, company or trust;
- whether there is any PEP involvement;

- situations where the customer is reluctant to meet the financial adviser face to face if they are a local resident;
- whether the customer has been introduced and if so what is known about the introducer;
- whether the customer has had a number of different financial advisers, possibly in a number of jurisdictions; and / or:
- whether the customer is undertaking activity inconsistent with the advice being provided.

4.4 Stockbroking

Stockbroker firms hold investment business permissions which allow them to undertake a wide range of services. They can be market makers, acting as principal, or as agent when buying and selling stocks and other securities for customers. Stockbrokers are normally members of at least one stock exchange. Stockbroking is usually provided on an "execution only" basis, however can be on an advised or discretionary managed basis. Stockbrokers may also offer advisory and / or discretionary portfolio management and custodian services.

"Execution Only" arrangements refer to where the business is not required to assess the suitability of any transaction for the customer. It purely carries out transactions on the instructions of the customer. A business undertaking execution only business is still required to fully comply with the Code therefore they must ensure they obtain the full range of customer information / verification required by the Code. Stockbrokers must ensure this customer information / activity is appropriately monitored on an ongoing basis.

As stockbrokers hold client money it is a sector that could be used at all three stages of the traditional three stages of money laundering model, placement, layering or integration.

Where customer instructions are taken on a non face to face basis this could increase the risk of the service being used for ML / FT. This should be carefully considered and appropriate CDD obtained based on the location of the customer. Also, as per section 4 of this document the number of intermediaries that may be involved should be considered.

4.4.1 Risk guidance

Specific risk factors to consider (in addition to the generic factors listed in section 3 of this document) in relation to the stockbrokers sector may include:

- the type of customer i.e. is it an individual, company or trust;
- whether there is any PEP involvement;
- consideration whether execution only business is being undertaken and no advice is being provided, if so it may be difficult to fully understand the customer's background and therefore it could be difficult to identify suspicious activity;
- whether the customer is reluctant to meet the stockbroker face to face if they are a local resident;

- whether the customer has had, or has, a number of different stockbrokers, possibly in a number of jurisdictions therefore making it difficult to build up a picture of their background;
- whether there are sudden and unexplained additions to, or transfers from, the customer's investment portfolio;
- whether the customer appears indifferent to the profit or loss generated by trading activities; and
- whether the customer transfers, and asks the investment business to dispose of, assets which were not acquired through that business, since transfers of assets off market may provide a vehicle for the ML.

4.5 Custodians

Custodians are financial institutions that hold customers' securities and other investments for safekeeping so as to minimise the risk of their theft or loss. A custodian can hold securities and other assets in electronic or physical form.

Custodians would typically hold client money therefore it is a sector that could be used at all three stages of the traditional three stages of money laundering model, placement, layering or integration.

The vast majority of customer instructions would tend to be received on a non face to face basis which could increase the risk of the service being used for ML/FT. This should be carefully considered and appropriate CDD obtained based on the location of the customer. Also, as per section 4 of this document the number of intermediaries that may be involved should be considered.

4.5.1 Risk guidance

Specific risk factors to consider (in addition to the generic factors listed in section 3 of this document) in relation to the custodian sector may include:

- the type of customer i.e. is it an individual, company or trust;
- whether there is any PEP involvement;
- whether the customer is reluctant to meet the custodian face to face if they are a local resident; and;
- situations where the custodian is utilised by other investment businesses in respect of their customers, in these cases it should be ensured that both the custodian and the investment business concerned have complied with the necessary Code requirements.

5. Simplified customer due diligence measures

The following sets out further detail regarding concessions that may be applicable to the sector.

5.1 Where the customer is a collective investment scheme

Where a relevant person enters a relationship with a customer it should undertake appropriate CDD in line with the requirements of the Code. In particular, an area that must be focussed on is paragraph 12(2)(b) of the Code which requires a relevant person to determine if the customer is acting on behalf of another person and identify, and take reasonable measures to verify the identity of that person.

However, if certain conditions are met, paragraph 21(2) of the Code provides a concession to the aforementioned Code requirement at paragraph 12(2)(b). This concession may be used where a relevant business' customer is a collective investment scheme (except exempt schemes), or an equivalent arrangement in a jurisdiction in List C (Appendix C) of the Handbook and if the manager or administrator of the scheme is a regulated person or a person acting in the course of external regulated business carrying on equivalent regulated activity in a List C jurisdiction.

Therefore, if these conditions are met, the relevant person does not have to comply with paragraph 13(2)(c) and it can treat the collective investment scheme as its customer, meaning it does not have to identify and verify the ID of the underlying investors in the scheme. The remaining provisions of the Code such as the requirement to conduct a risk assessment, ongoing monitoring provisions etc. continue to apply.

As stated in paragraph 21(4) of the Code, if there is suspicious activity as defined in paragraph 3 of the Code, the concession no longer applies and EDD must be considered in line with paragraph 15 of the Code and an internal disclosure made. If there is an unusual activity such as the transaction appearing unusually large or complex, the business should undertake EDD in line with paragraph 15 of the Code and consider whether the use of the concession remains appropriate.

5.2 Exemption in relation to certain insurance products

Some financial advisers are able avail themselves of the exemption of section 9 of the Insurance Intermediaries (General Business) Regulations 1999. These particular financial advisers may also be eligible to make use of certain CDD concessions contained in paragraph 20 of the Code if particular insurance products are sold. It should be noted that although these concessions dis-apply CDD (part 4) in certain circumstances, other parts of the Code, including the obligation to undertake a customer risk assessment (part 3) continue to apply in all instances.

It is at the relevant person's discretion whether the insurance CDD concessions (paragraph 20) are utilised, however, for customers that are provided other investment business services the CDD requirements contained in part 4 of the Code continue to apply, therefore the concession would not be applicable. If relevant person is considering using any of these CDD concessions we would suggest contacting the Authority to discuss further.

6. Case Studies

The case studies below are real life examples of risks that have crystallised causing losses and / or sanctions (civil and criminal) against the funds /investment business sector. These examples are based on the FATF report: Money Laundering and Terrorist financing in the Securities Sector October 2009[5].

For further typologies please see the Annex to the FCA document: Understanding the Money Laundering Risks in the Capital Markets[6]

6.1. Laundering by acquisition of a publicly traded shell company

The Financial Intelligence Unit ("FIU") received a suspicious transaction report ("STR") from a bank regarding D, a man in his twenties with a student account. The STR stated that D bought a controlling interest in public shell company X and then proceeded to open a bank account in the name of that company. A few days later, the account received a deposit of approximately US2.5 million.

In addition to company X, D was also the sole owner of a private company, Y. D used company Y to purchase a controlling interest in company X through the Over the Countermarket. Part of the US$2.5 million that was credited to company X was derived from a company Y account. Company Y received large deposits from several private accounts managed by criminal entities involved in drug trafficking. In one case the funds were transferred from the person known to be involved in criminal activity through a money service business account to the account of company X to further distance the source of the funds. The new controlling owners appointed new directors, including family members.

Shortly after the US$2.5 million was transferred to the account of company X, it was transferred back to the money service business account. Some of the money was transferred as a loan to company W, which was associated with the same criminal organisation that originally transferred funds to Company Y.

D and his family were well-known to the FIU for having acquired public shell companies in the past for money laundering purposes, including committing other predicate offences. They were also suspected of fraudulently influencing the movement of the stock share prices of

[5] http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf
[6] https://www.fca.org.uk/publication/thematic-reviews/tr19-004.pdf

companies owned by them, performing circular transfers of funds, and fraudulently removing funds from the companies.

High risk indicators from this case included:

- the use of a publically traded shell company;
- transferring funds through several accounts;
- using a money service business to transfer funds; and
- withdrawing the funds shortly after the acquisition by means of loans.

6.2. Securities transfers

The Tax Administration and the Fiscal Intelligence and Investigation Service has discovered methodologies involving the allocation of securities as a means to effect tax fraud. These activities involved the use of false documents, in violation of tax and criminal laws. To date, 14 cases have been detected, involving six different financial institutions. Seven cases have been investigated in greater depth. The key role played by the facilitating financial institutions in these cases was examined by the Dutch Central Bank and The Netherlands Authority for the Financial Markets.

The cases investigated have in common the misuse of a normal and legitimate service provided by banks, broker-dealers and other institutions licensed to trade in securities: the ability to transfer securities held electronically.

The misuse in the Dutch cases was triggered by a difference in the way capital gains and losses were treated for the income and corporate tax purposes. In short, capital losses are not deductible for income tax purposes, but are included in the tax base for corporate tax.

In these cases, individuals transferred securities between their personal portfolio and a corporate securities portfolio over which they had control. Depending on what was necessary in the specific case, securities were transferred in either direction. In the case of a loss that occurred in the personal portfolio, the relevant securities were transferred to the corporate stock portfolio and vice versa.

The attractive feature of the misuse of the securities-transfer service is its lack of transparency. In a transfer there is no mandatory current account relationship. As is the case with regular sale and purchase instructions, payment for securities transferred can be arranged by other means, such as cash payments. As a consequence, bank statements do not have to show that a share transfer has taken place. In the different cases that were investigated, transfers of securities were communicated to the client by separate statements that were not consecutively numbered and that did not have any connection with the year-end bank reconciliation. All cases investigated resulted in administrative or criminal sections.

What was surprising in the cases investigated was:

- the number of cases detected;
- the similarity of modus operandi;
- the relative ease in which employees of financial institutions were persuaded to co-operate in the scheme;
- the fact that the cases took place at different players in the financial sector; and
- the involvement of accountants and tax advisors.

High risk indicators from this case included:

- transactions without an apparent economic rationale;
- use of false documentation; and
- ante-dating of documents.

6.3. Structuring of cash deposits

D became the subject of a STR submitted to the FIU that detailed activity involving the structuring of cash deposits into an account.

A "contract for difference" (CFD) is a type of derivative where an agreement is made to exchange the difference in value of a particular security (or other financial instrument) between the time at which a contract is opened and the time at which it is closed. In this particular investigation, the profits were deposited in a major Australian bank.

D used false identification documents, including a false citizenship certificate and driver's licence, to open a trading account over the internet. The individual became the subject of an STR because of the structuring of cash deposits into an account. The STR highlighted that over an eight-day period, approximately AUD$ 400,000 was deposited into the account in amounts. An investigation into this resulted in criminal restraining orders being placed on the individual's assets.

High risk indicators from this case included:

- multiple same day transactions;
- use of false documentation; and
- structuring of case deposits.

6.4. Rapid purchase and sale of shares

A bank reported that large wire transfers ordered from a securities dealer were received into a business account administered by Person A. Once received, money was used to purchase

bank drafts, and cheques were issued payable to various individuals and entities. The purpose of the transfers between the securities dealer and the bank is not known, since the individual has refused to respond to questions asked by the bank's anti-money laundering section.
It was suspected, however, that the client was "dumping" in the market a large number of shares purchased earlier (evidenced by previous wire transfers sent to the securities dealer) once they reached a certain value.

The securities dealer that sent the wire transfers also reported the following on Person B:

- listed investment advisor: Person A;
- was the signing authority of 24 accounts held by two corporations located in two Central American countries. The review of the accounts activity revealed movement of funds from one account to another;
- was purchasing shares of specific companies, selling them a short time later and wiring the proceeds to bank accounts held by the corporations at financial institutions located in Central America and the Caribbean; and also to a bank account administered by Person A; and
- never held stocks long enough to take advantage of future dividend distributions.

Another securities dealer reported that an individual, whose investment adviser was also Person A, purchased a large number of shares and sold them a short time later with no economic gain. When purchasing the stocks, the client never used wire transfers but rather cheques drawn on an account held in a financial institution located in a foreign country. The transactions always involved one particular company.

The case relates to eight individuals and two corporations involved in a stock manipulation scheme:

- Person A was the investment adviser of a group of 7 individuals;
- Person B was listed as the signing officer of two corporations;
- the two corporations had addresses in two different Central American countries but also held bank accounts in other Caribbean locations.

According to information posted in a market regulator's website:

- Person A was the main subject of a stock manipulation investigation;
- one person of the group was under investigation for banking fraud in an Asian country; the fraud cost investors close to CAN$100 million (awaiting extradition).

Person A appeared to be providing information on when to purchase and sell stocks of specific firms to the rest of the group. The investors did not hold the stocks enough to take advantage of dividend distributions. Proceeds of stocks sold were:

- wired to bank accounts held overseas;
- used to purchase banks drafts or to issue cheques payable to individuals and entities (it was suspected that the beneficiaries were nominees).

Analysis of the financial transactions of the remaining individuals of the group revealed constant purchases and sales of securities whose proceeds were deposited in bank accounts

followed by issuance of cheques or bank drafts payable to individuals and entities. Some transactions involved penny stocks and stocks traded on the pink sheets (which are less regulated, and therefore more easily manipulated).
High risk indicators from this case included:

- buying and selling of securities with no discernible purchase in circumstances that appear unusual; and
- use of multiple accounts at a single securities dealer for no apparent reason.

6.5. Employee of a securities intermediary assisting a PEP to launder money

D, an investment representative at a large broker-dealer, helped a PEP from a foreign jurisdiction launder over US$10 million that the PEP received from drug traffickers. The PEP received these illicit assets as payment for allowing drug shipments to safely pass through his jurisdiction. D helped the PEP establish numerous brokerage accounts at her firm in the name of various foreign shell companies and then deposited the illicit assets into these accounts. Weeks before the PEP was to lose prosecution immunity, D assisted the PEP in wire transferring the illicit assets out of the brokerage account and into a foreign account. D then set up a fictitious account for the PEP and wire transferred all of the assets back to her firm.

High risk indicators from this case included:

- wide spread news regarding investigation of the PEP; and;
- foreign wire transfers.