CHARTERED SECRETARIES
特許秘書

Anti-Money Laundering and Counter-Terrorist Financing

- GUIDELINES -

The Hong Kong Institute of Chartered Secretaries

Chartered Secretaries. More than meets the eye.
特許秘書. 潛能. 超越所見.

CHARTERED SECRETARIES
特許秘書

About The Hong Kong Institute of Chartered Secretaries

More than meets the eye.

The Hong Kong Institute of Chartered Secretaries is an independent professional body with more than 5,000 members and approximately 2,500 students. It is dedicated to the promotion of its members' role in the formulation and effective implementation of good corporate governance policies in Hong Kong and throughout China as well as the development of the profession of Chartered Secretary.

The Institute is part of the Institute of Chartered Secretaries and Administrators (ICSA) of London. It was first established in 1949 as an association of Hong Kong members of ICSA. It became a branch of ICSA in 1990 before gaining local status in 1994.

The Hong Kong Institute of Chartered Secretaries

Hong Kong Office
3/F., Hong Kong Diamond Exchange Building,
8 Duddell Street,
Central, Hong Kong
Tel: (852) 2881 6177
Fax: (852) 28815050
Email: ask@hkics.org.hk
Website: www.hkics.org.hk

Beijing Representative Office
Rooms 1014-1015
10/F., Jinyu Mansion
No.129 Xuanwumen Xidajie
Xicheng District
Beijing, China P.C. 100031
Tel: (86 10) 6641 9368
Fax: (86 10) 6641 9078
Email: bro@hkics.org.hk

FOREWORD

Anti-money laundering (AML) and counter terrorist financing (CTF) are two of the major challenges facing the world today. Only by working hand-in-hand with law enforcement agencies can business be rid of the multi-billion dollar scourge of money laundering that can, and does, cost lives and destroys the livelihood of thousands of people throughout the world.

Money laundering strategies are in continual flux and no doubt this guide will need updating from time-to-time, but I believe that as Chartered Secretaries we have a duty to make sure that we are up-to-date with the latest AML/CTF procedures not only to better serve our clients and employers, but also as a matter of professional integrity.

These guidelines, published by The Hong Kong Institute of Chartered Secretaries (HKICS) are intended for use by all members, however particular attention is given to the Trust and Company Service Providers (TCSP) sector as this is an area that has recently been highlighted for attention by the Financial Action Task Force (FATF), an inter-governmental body set up to combat money laundering. The audit in 2007 of Hong Kong by the FATF and the increase in attention paid to the TCSP sector by the Hong Kong Government in relation to AML and CTF activities is testament to this view.

The increasing awareness of the role played – wittingly and unwittingly-by those working in the TCSP sector, where many Chartered Secretaries work, is one of the reasons behind HKICS' decision to publish these guidelines. By providing members with guidance on what to look for concerning money laundering and what steps they should take to avoid being party to money laundering as well as how to report suspected money laundering and terrorist financing activities, the Institute hopes it can help members play a part in deterring and/or detecting such activities.

I urge you to read and digest these guidelines which will also be available for download from the Institute's website. As professionals we must play our part and be seen to be doing so to counter money laundering and terrorist financing.

I would like to thank the Professional Services Panel and the secretariat for their input and leadership on this project as well as the members of the editorial board set up specifically to help produce these guidelines and the generous help provided by members of the Joint Financial Intelligence Unit and the Narcotics Division, Security Bureau in the writing of these guidelines. Without their help and support such a comprehensive set of guidelines would not have been possible.

Natalia Seng
President
The Hong Kong Institute of Chartered Secretaries

PREFACE

I write to extend my sincere congratulations to The Hong Kong Institute of Chartered Secretaries (HKICS) for promulgating a comprehensive set of guidelines on anti-money laundering (AML) and counter financing of terrorism (CFT).

Advances in technology have made it possible to move huge volumes of funds to virtually anywhere in the world in a matter of seconds. With globalisation of trade and business and development of complex corporate structures, our corporate services sector is being exposed to a higher risk of money laundering and terrorist financing than ever before. Business professionals such as chartered secretaries are our important partners and gatekeepers in preventing their service from being abused by criminals for money laundering and terrorist financing.

As an international financial centre and a responsible member of the global community, Hong Kong is fully committed to the fight against money laundering and terrorist financing. The Guidelines issued by HKICS provide real life and practical examples of implementing the core counter-measures formulated by the Financial Action Task Force on Money Laundering, which sets the international standards for combating money laundering and terrorist financing. The Guidelines will help equip business professionals in discharging their duties to prevent crime proceeds and terrorist funds from slipping through the gate and entering our financial system. These latest sector-specific AML/CFT guidelines underline the commitment of the corporate services sector to join hands with Government in a concerted effort to preserve the integrity and stability of our economy and business environment.

May I take this opportunity to thank the HKICS for issuing the Guidelines. I do hope that members will make full use of them, both for training and practical purposes. I look forward to further collaboration with HKICS and its members in the fight against money laundering and terrorist financing.

Ms Sally Wong, JP
Commissioner for Narcotics

Table of Contents

PART I: INTRODUCTION 5
1. Overview 5
1.1 Introduction 5
1.2 What is money laundering? 6
1.3 What is terrorist financing? 6
2. Legislation 7
2.1 The Financial Action Task Force (FATF) 7
2.2 Anti-money laundering legislation in Hong Kong 7
2.3 Legislation concerning terrorist financing in Hong Kong 10
PART II: DETAILED GUIDELINES 12
3. General Overview and Risk Assessment 12
4. Policies and Procedures to Combat Money Laundering and Terrorist Financing 13
5. Customer Due Diligence 14
5.1 General principle 14
5.2 Individuals 15
5.3 Corporations 16
5.4 Shell companies 19
5.5 Clubs, societies and charities 19
5.6 Trust and nominee accounts 19
5.7 Intermediaries 20
5.8 Politically-exposed persons 21
5.9 Non face-to-face clients 22
5.10 Powers of Attorney 23
5.11 Estates of deceased persons 23
5.12 Generally 23
6. Risk Considerations and Systems 24
6.1 Record keeping 24
6.2 Identification of suspicious transactions 25
6.3 Employee training programmes 25
PART III: REPORTING SUSPICIOUS TRANSACTIONS 26
7. Obligation to Report Suspicious Transactions/Terrorist Property 26
7.1 Introduction to Reporting Suspicious Transactions 26
7.2 Meanings of indictable offence and drug trafficking 27
7.3 Meaning of proceeds 28
7.4 Meaning of property 28
7.5 Meaning of knowledge or suspicion 29
7.6 Penalty for failing to report 29
7.7 Reporting of terrorist property 29
7.8 Meaning of terrorist property 30
7.9 Penalty for failing to report 30
8. The Joint Financial Intelligence Unit 31

PART IV: APPENDICES 33
Appendix 1: Examples of Suspicious Transactions 33
Appendix 2: Members of the FATF 34
Appendix 3: Recognised Stock Exchanges 35
Appendix 4: Common Indictable Offences 36
Theft Ordinance (Cap. 210) 36
Crimes Ordinance (Cap. 200) 37
Prevention of Bribery Ordinance (Cap. 201) 38
Gambling Ordinance (Cap. 148) 40
Companies Ordinance (Cap. 32) 41
Appendix 5: Useful Websites 43

PART 1: INTRODUCTION

1. Overview

1.1 Introduction

As Chartered Secretaries, we are professionals who are trained and expected to maintain the highest standards of corporate governance, effective operations, compliance and administration. Those expectations include a requirement that we exercise proper skill and judgment in our role as part of the international drive to combat money laundering and terrorist financing.

In these guidelines, the trust and corporate services functions of a Chartered Secretary are examined in detail. The Financial Action Task Force (FATF) (see paragraph 2.1 for a description of this organisation) considers trust and company services providers to be a specific profession which is integral in the fight against money laundering and terrorist financing. The FATF defines a trust and company services provider as a person who, as a business, provides any of the following services to third parties:

- Acting as a formation agent of legal persons
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of an express trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person

In these guidelines a distinction is drawn between Chartered Secretaries who work as company secretaries within a company or group of companies and whose services are provided to that company or group, and those who work within a standalone corporate services provider which provides corporate services to a base of clients. While the risk, in terms of money laundering and terrorist financing, is quite different in respect of each of these categories, many of the fundamental risk management considerations are common to both.

Consider each type of position in more detail. Chartered Secretaries employed within a company and who provide company secretarial services for that company are more likely to be exposed to money laundering in which the company is involved (even innocently) or knows about as part of its day-to-day business and transactions. On the other hand, Chartered Secretaries who provide company secretarial services to a large base of clients are less likely to have extensive knowledge of their clients' underlying business but may be exposed to money laundering through the creation of complex corporate structures which are often used to launder crime proceeds.

1.2 What is money laundering?

Money laundering involves disguising the identity of illegally-obtained money and making it look as if it originates from a legitimate source.

There are three stages of money laundering. Any of these could contain transactions that could alert a Chartered Secretary to unlawful activity.

(a) **Placement** – the initial entry point into the financial system of funds derived from criminal activities. Banks and other financial institutions now have highly developed anti-money laundering procedures so criminals look for other ways of introducing unlawful funds into the financial system. Chartered Secretaries, like many professionals, can be targets either by handling the funds themselves or setting up bank accounts for corporate entities; these accounts are then used to front payments into the financial system. An example might be a request from a client to incorporate a company and open a bank account. While waiting for that account to be opened, the Chartered Secretary is asked to hold cash (which will be the proceeds of crime) in his or her own bank to be paid into the new account later. Identifying placement is usually the most obvious and apparent way of detecting money laundering.

(b) **Layering** – the creation of complex networks of transactions to obscure the link between the initial entry point and the end of the laundering cycle. Layering often uses complex corporate structures and trusts, perhaps involving a number of jurisdictions, and is, therefore, a stage of the process which requires particular vigilance. To continue with the above example, layering would take place when the dirty cash from the Chartered Secretary's account is paid into the new account he or she has opened for the new client and the subsequent movement of those funds through different accounts opened in the names of different companies that the Chartered Secretary has incorporated, both in Hong Kong and overseas. It is more difficult to detect layering as the inter-company transfers may be disguised to lend the transactions an air of commercial reality and probity.

(c) **Integration** – providing apparent legitimacy to illicit proceeds. After layering, integration schemes place the illicit proceeds back into the economy, making them appear to be genuine and *bona fide* business funds. Continuing with our example, imagine that the final transfer of funds is to the Chartered Secretary's account, where the money is held in escrow for the purchase of a large residential property. The sale is called off at the last minute and the Chartered Secretary returns the funds to his or her client using his or her firm's cheque. That cheque is respectable and bears no hint of the true origin of the funds and will be accepted by any mainstream bank. The funds are now clean.

1.3 What is terrorist financing?

Terrorist activities require money. One way to combat terrorism is to cut off terrorists' access to funds. Terrorist financing shot into the limelight after the events of 11 September 2001. It refers to one of the following:

- Carrying out transactions involving funds that are owned by terrorists; or
- Carrying out transactions involving funds that have been or are intended to be used for or to assist the commission of terrorist acts.

2. Legislation

2.1 The Financial Action Task Force (FATF)

The FATF was established in 1989 to lead the international fight against money laundering. This inter-governmental body develops and promotes national and international policies to tackle money laundering and terrorist financing problems. The FATF works to generate the necessary political will to bring about legislative and regulatory reforms in the areas of money laundering and terrorist financing. It has called on governments to increase oversight of, amongst others, trust and corporate services providers (see paragraph 1.1 for a definition of trust and company services providers) and to set minimum standards for company registry and administration.

The FATF has issued what is considered the cornerstone of good practice in anti-money laundering and combating the financing of terrorism (AML/CFT) in its Forty Recommendations and Nine Special Recommendations, which contain measures to combat money laundering and terrorist financing through its criminalisation, the requirement to conduct customer due diligence and record-keeping, and imposing obligations to report suspicious transactions to the authorities.

2.2 Anti-money laundering legislation in Hong Kong

Hong Kong has a legal and regulatory framework that addresses money laundering and which brings the SAR in line with the FATF's Forty Recommendations. The two principal relevant statutes are the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRPO) and the Organized and Serious Crimes Ordinance (OSCO).

Both ordinances share a common theme and provide for two distinct forms of criminal liability in terms of money laundering. The first is actually being involved in laundering money; the second is failing to report to the authorities property which you know or suspect to be representing the proceeds of crimes.

Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) (DTRPO)

Important sections of the DTRPO include:

- Under s 10(1), the Court of First Instance may make a restraint order prohibiting any person from dealing with any available property which is the proceeds of drug trafficking (this is referred to as realisable property).
- Under s 10(12), an authorised officer (i.e. a police officer, a member of the Customs and Excise Service and any other person authorised in writing by the Secretary for Justice) may give notice to a person who holds any realisable property subject to a restraint order that the person is to deliver to the authorised officer documents, copies of documents or any other information which may assist the authorised officer to determine the value of the property. In addition, s 10(14) provides that this kind of disclosure is not to be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision.
- A person who knowingly deals with any realisable property in contravention of a restraint order commits an offence under s 10(16).

Organized and Serious Crimes Ordinance (Cap. 455) (OSCO)

The OSCO was modelled on the DTRPO and extends money laundering offences to cover the proceeds of indictable offences. Indictable offences are offences of a generally more serious nature and which can or must be tried in a higher court. Appendix 4 gives a list of indictable offences and, while the list is not exhaustive, it does include the majority of indictable offences which carry financial implications that may trigger money laundering concerns. Important sections of the OSCO include:

- If there are reasonable grounds for suspecting that an organized crime has been committed and that there are reasonable grounds for suspecting that a particular person has information, or is in possession of material, likely to be relevant to the investigation, then under s 3(2) the Court may make an order authorising the Secretary for Justice to require that particular person to answer questions or furnish information to an authorised officer or to produce any material that reasonably appears to relate to any matter relevant to the investigation.
- Under s 4, the court may make an order that the person who appears to the court to be in possession or control of the material to which the application relates must produce the material to an authorised officer or give an authorised officer access to it.
- Under s 5, the Court may make an order authorising the authorised officer to enter and search premises where there are reasonable grounds for suspecting that an organized crime has been committed.

Common provisions to both DTRPO and OSCO

Being involved in money laundering

- A person commits an offence under s 25(1) of both ordinances if he or she deals with property that he or she knows or has reasonable grounds to believe represents the proceeds of drug trafficking or an indictable offence. However, s 25(2) provides that it is a defence to prove that he or she intended to disclose to an authorised officer such knowledge, suspicion or matter and there is a reasonable excuse for failing to disclose.
- Under s 25A(2) if a person who has made a disclosure referred to in s 25A(1) does any act in contravention of s 25(1) (whether before or after such disclosure), and the disclosure relates to that act, he does not commit an offence under that section if:

  (a) That disclosure is made before he does that act and he does that act with the consent of an authorized officer; or

  (b) That disclosure is made:

    (i) after he does that act;
    (ii) on his initiative; and
    (iii) as soon as it is reasonable for him to make it.

  Please refer to section 7.1 below for further discussion of the reporting requirements under s 25A of DTRPO and OSCO.

Failing to report knowledge or suspicion of money laundering

- Section 25A provides that where a person knows or suspects that any property represents or was used in connection with or is intended to be used in connection with any person's proceeds of drug trafficking or an indictable offence, he or she should disclose this knowledge or suspicion to an authorised officer as soon as it is reasonable to do so.

- Section 25A(3) provides that disclosure is not a breach of confidentiality as it provides that disclosure is not to be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision.
- Section 25A(4) provides that the disclosure obligation applies to employees; however they will have discharged their obligation to report if they disclose their knowledge or suspicion to the appropriate person within their workplace in accordance with the procedure established by their employers.

Tipping-off

- Section 25A(5) further provides that following disclosure to an authorised officer or to the appropriate person in accordance with the procedure established by employers, it is an offence for a person to disclose to any other person any matter which is likely to prejudice any investigation which might be conducted.

2.3 Legislation concerning terrorist financing in Hong Kong

The United Nations Security Council has passed resolutions requiring sanctions against designated terrorists and terrorist organisations. The United Nations Sanctions Ordinance (Cap. 537) gives effect to these resolutions in Hong Kong.

The FATF has also issued Nine Special Recommendations to help combat terrorist financing. Hong Kong has a legal and regulatory framework dealing with terrorist financing which brings it in line with the FATF's Nine Special Recommendations.

United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) (UNATMO)

The counter-terrorist financing provisions mirror, in large part, the counter-measures in place to combat money laundering. Offences include being involved in financing terrorism or failing to report to the authorities property which you know or suspect is terrorist property. There are tipping-off preclusions whereby disclosure to the authorities is deemed not to be a breach of confidence. Important provisions of the UNATMO include:

- Schedule 1 defines funds, which includes: cash, deposits with financial institutions, securities and debt instruments, interest, dividends, credit, rights of set-off, guarantees, letters of credit, and documents evidencing an interest in funds or financial resources.
- Section 7 states that a person shall not provide or collect funds with the intention that the funds be used or knowing that the funds will be used to commit a terrorist act, whether or not the funds are actually used in this way.

- Where a person knows or suspects that any property is terrorist property, under s 12(1), he or she must disclose to an authorised officer the information on which the knowledge or suspicion is based as soon as possible after that information comes to his or her attention. Section 12(3) then provides that a disclosure is not to be treated as a breach of any restriction upon the disclosure of information imposed by contract or by any enactment, rule of conduct or other provision.
- Following this, s 12(5) provides that where a person knows or suspects that a disclosure has been made, that person should not disclose to another person any information which is likely to prejudice any investigation which might be conducted.
- Under s 12(6), the information obtained may then be disclosed by an authorised officer for the purpose of preventing and suppressing the financing of terrorist acts to the Department of Justice, the Hong Kong Police Force, the Customs and Excise Department, the Immigration Department, and the Independent Commission Against Corruption. The authorised officer may also disclose the information to the authorities or persons responsible for investigating or preventing terrorist acts, or handling the disclosure of knowledge or suspicion that any property is terrorist property.

Please refer to section 7.7 below for further details of the reporting requirements under s 12 of UNATMO.

PART II: DETAILED GUIDELINES

3. General Overview and Risk Assessment

There is no single equation or set of rules you can use to guarantee the detection of money laundering or terrorist financing, or to guard yourself against being taken in by it. The best tactics are to apply common sense, based on a knowledge of the industry, with an enquiring mind laced with a healthy amount of commercial cynicism. Anti-money laundering and counter-terrorist financing measures are a risk-based discipline. You should develop internal systems to address your own risk profile in terms of exposure to money laundering and terrorist financing transactions.

Factors to take into account in determining your own risk profile include:

Type of client – particularly relevant for members who provide corporate services to a large client base. The type of clients you have will have an impact on your risk profile. Client factors include:

- Actual business undertaken by clients;
- Client turnover – whether your clients are long-term stable clients or short-term single transaction clients;
- Acting for clients in regions where there are high levels of fraud, corruption/bribery or terrorist activity;
- Acting for clients remotely, without meeting them face-to-face; and
- Acting for corporate clients rather than individuals.

Nature of the services provided – the nature of the work you do will have an impact on your money laundering/terrorist financing risk profile. An exceptionally common feature in layering illicit funds is the use of complex, corporate structures and trusts in a bid to obscure the source of funds and their ownership. Setting up these structures can be a core part of the services that Chartered Secretaries provide. Risk identifiers include providing services where cash payments are common (either for payment for services or services which help the movement of cash, such as opening bank accounts); payments to and from third parties; and of particular importance in Hong Kong, cross-border transactions and services. These identifiers apply equally to members providing corporate services to a wide client base, and to in-house corporate secretaries who need to consider the transactions their company is involved with or privy to.

Risk assessment is an on-going process and should be monitored continually – for ongoing client relationships and also in terms of your own risk profile as an individual or business. Risk assessment is, by its very nature, an imperfect science – risk can never be completely eliminated; you have to assess your risk position, ensure it falls within your level of risk tolerance, and implement internal controls to effectively manage that risk exposure.

4. Policies and Procedures to Combat Money Laundering and Terrorist Financing

The extent and level of internal policies and procedures aimed at combating money laundering and terrorist financing will depend on the size of your organisation, the nature and complexity of the services rendered, and your own risk profile. Internal controls will, however, share the following defining characteristics:

(1) A clear statement in writing of policies and procedures in relation to money laundering and terrorist financing which management and all employees must follow.

(2) Policies should include all of the following, which form the foundation of any adequate anti-money laundering/counter-terrorist financing system:

(a) Customer due diligence (see section 5)

(b) Record keeping (see paragraph 6.1)

(c) Identification of suspicious transactions (see paragraph 6.2)

(d) Reporting of suspicious transactions (see paragraph 7).

(3) Employee training (see paragraph 6.3).

(4) Promotion of co-operation with law enforcement authorities.

(5) Verification of compliance with internal policies and procedures.

(6) Regular review of the policies and procedures to be up to date with the law and practice.

5. Customer Due Diligence

5.1 General principle

This can be summed up in just three words: know your customer. The KYC principle, as it is commonly known, is the most essential and fundamental feature of all anti-money laundering and counter-terrorist financing systems. KYC applies to the beginning of a new relationship with a client, and also as a continuing obligation. You will be better placed to identify suspicious transactions if you know your client and understand the reasoning behind the services they want from you.

When you accept a new client, you should have internal procedures in place to properly and accurately identify the party with whom you are about to become engaged. The identification procedure should allow you to satisfy yourself, in the reasonable and objective view of a third party, of the true identity of your client and its beneficial owner. Establishing the true identity of a client requires some form of reliable verification of identity through independent evidence.

Client identification is and should be a real and active process. The perfunctory check of a fourth generation photocopy of an identity card so as to be able to tick-off a box on a file opening form is not a proper and reasonable approach to KYC. Ask for an original document; compare a photograph to the real person; look for any tampering with the document offered by the client. While you are not expected to be a forensic expert, you should not overlook obvious forgeries or questionable documentation.

When considering identification and client due diligence, the following factors may help you establish a risk profile for the client and determine the level of due diligence you perform:

Nature of the services required – if a new client wants overseas incorporated companies with opaque ownership structures in order to open bank accounts in Hong Kong, you might need to investigate further before becoming satisfied as to the *bona fides* of the arrangement. Unnecessarily complex corporate structures could tip you off to the existence of potentially questionable transactions.

Nature of the customer and their business – a new client with origins in or transacting business in countries with high degree of fraud, corruption/bribery or terrorist activity impose a high risk for your anti-money laundering profile.

Nature and source of any funds involved – money laundering and terrorist financing both involve the movement of funds and, therefore, any services which involve money and dealing with it may give rise to risk concerns. Cash transactions and clients whose business is cash-intensive (such as casinos, bars and money changers) are also risk triggers as illicit funds derived from illegal activities are invariably in the form of cash. Payments from third parties may also increase a client's risk profile if there is no apparent reason for the third party being involved.

While each case and each customer's circumstances turns on their own unique features, you should have customer acceptance policies and procedures that aim to identify the types of customers who are likely to pose a higher risk of money laundering and terrorist financing. You should also have clear internal guidelines for those who agree to accept new clients and business to determine if a new business relationship should be approved.

The suggested methodology that follows can help you satisfy yourself as to the true identity of various types of client.

5.2 Individuals

The identity of an individual includes their name (in English and Chinese), address, physical appearance, employment, date of birth, etc. Positive identification can be obtained from official government-issued documents such as passports and identity cards. Hong Kong residents' main source of identification is their Hong Kong identity card; passport is generally sufficient for non-residents. Proof of address in the form of bank statements or utility bills can also add comfort in determining an individual's identity.

If you have any question about the validity or genuineness of someone's identification document, you should contact the Immigration Department Hotline at 2824 1551 (for Hong Kong identity cards) or the local consular office (for overseas identity documentation).

You can also consider carrying out a search on the Securities and Futures Commission (SFC) website to see if the SFC has taken action against the individual. The website provides the latest enforcement news and details the reasons for any enforcement action, and the consequences of the action.

Specific name search: www.sfc.hk/sfcPressRelease/jsp/EN/NameSearch.jsp
Latest enforcement news: www.sfc.hk/sfcPressRelease/EN/sfcAllPressReleaseServlet

The Hong Kong Monetary Authority (HKMA) occasionally provides updates on the Lists of Names for Suspicious Account Reporting, which is issued and updated by the US Government. The most recent updates can be found on the HKMA Guidelines and Circulars link at www.info.gov.hk/hkma/eng/guide/index.htm.

5.3 Corporations

A company's identity consists of its name, registered office, constitution, management and shareholders. Companies, although they are separate legal entities, cannot give instructions themselves but act through agents. As well as satisfying yourself as to the identity of the company, you should also satisfy yourself as to the identity of the person giving you the instructions – and their authority to do so.

Where the corporate customer concerned is any one of the following:

(1) A financial institution authorised and regulated by the HKMA or the SFC in respect of its business in Hong Kong, or a subsidiary of such an institution;

(2) A financial institution not authorised to carry on business in Hong Kong, but which is incorporated in a country which is a member of the FATF (See Appendix 2) and which is regulated by bodies carrying out equivalent functions to those mentioned in (1);

(3) Listed on the Stock Exchange of Hong Kong, or is a subsidiary of such a company;

(4) Listed on a stock market recognised by the SFC (see Appendix 3); or,

(5) A non-listed company, whose principal shareholders and the directors (including the managing director) are already known to you;

then you can simplify the due diligence process and obtain the following information from public services:

(1) Certificate of incorporation and business registration certificate;

(2) Memorandum and articles of association;

(3) Resolution of the board of directors to enter into or undertake the transaction for which your services are required or form part; and

(4) A search at the Companies Registry or similar overseas body.

If you have a corporate customer other than those listed above, you should also be satisfied about the identity of all of the following persons:

(1) Principal beneficial shareholders;

(2) The directors (including the managing director); and

(3) Any person from whom you are to take instructions.

You may also consider reading the company's latest audited accounts to satisfy yourself as to the *bona fides* of the client, its financial situation and its sources of income.

Where a listed company is effectively controlled by an individual or a small group of individuals, you should also verify the identity of these individual(s).

Where the direct customer is a non-listed company which has a number of layers of companies in its ownership structure, you should verify the identity of the individuals who are the ultimate principal beneficial owners of the direct customer. A complex ownership structure without an apparent purpose is, in itself, a risk factor.

Where a corporate customer is known to have nominee shareholders, you should look for satisfactory evidence of the identity of the beneficial owners. Companies with capital in the form of bearer shares pose an increased risk of money laundering and terrorist financing as these shares obscure the identity of the beneficial owners; you will need to take an appropriate and proportionate approach to due diligence.

As with individuals, you can also consider carrying out a search on the SFC website to see if the SFC has taken action against the company.

Specific name search: www.sfc.hk/sfcPressRelease/jsp/EN/NameSearch.jsp
Latest enforcement news: www.sfc.hk/sfcPressRelease/EN/sfcAllPressReleaseServlet

5.4 Shell companies

Shell companies are legal entities with no business substance but through which financial transactions may be conducted. A legitimate business may have sound commercial reasons for the lack of transparency that accompanies the formation and operation of shell companies, but this poor transparency can also allow these companies to disguise their ownership and purpose. Shell companies are common tools for money laundering and other financial crimes, primarily because it is easy and cheap to set up and operate them.

You should obtain satisfactory evidence of the identity of the beneficial owners and directors as well as an understanding of the rationale for using a shell company.

5.5 Clubs, societies and charities

Where the customer is a club, society or a charity, you need to be satisfied that the organisation's purpose is legitimate, as are the people controlling it and its source of income and/or donations. This can be done by examining the organisation's constitution or by making an actual visit to the organisation and asking appropriate questions of those representing it. The Inland Revenue Department has a list of registered charities in Hong Kong (see www.ird.gov.hk/eng/tax/ach_index.htm) which may help you establish a charity's *bona fides*.

5.6 Trust and nominee accounts

A trust is not a separate legal entity. A trust formed when the original owner transfers something of value to a trustee, who manages and controls the assets for the benefit of the owner or for other beneficiaries. A trust can be a legitimate way of protecting property and assets for specific individuals or purposes, but it can also be used to conceal the true beneficial owner of proceeds of criminal acts, or used as part of a money laundering scheme to complicate funds flows.

You should be suspicious of a customer who undertakes a transaction on behalf of another person without sufficient identification of the trust or nominee capacity, and you should make further inquiries as to the underlying principals and the nature of the trust and its purpose.

A copy of the trust deed will give you a good understanding of the trust and identities of the trustees, the settlor and beneficiaries.

5.7 Intermediaries

Customers are sometimes introduced by intermediaries such as law firms, accountants or others. Chartered Secretaries may rely on the intermediaries to perform customer due diligence, though you have the ultimate responsibility to carry out proper and proportionate due diligence and satisfy yourself of the identity of the client and the nature and purpose of the services required of you.

Before relying on an intermediary, as a Chartered Secretary you should be satisfied of all of the following:

(1) That the intermediary's customer due diligence procedures are as stringent as your own;

(2) That the intermediary's customer due diligence systems are reliable; and

(3) That you will be permitted to verify the intermediary's customer due diligence at any stage.

As a Chartered Secretary you ought to be able to rely on intermediaries which are incorporated in, or operating from, a member jurisdiction of the FATF (see Appendix 2) and which are:

(1) Regulated by the HKMA, the SFC or the Insurance Authority; or

(2) Regulated by an authority that performs functions equivalent to these authorities; or

(3) If not so regulated, are able to demonstrate that they have adequate procedures to prevent money laundering.

As a Chartered Secretary you should review the intermediaries regularly to ensure that they continue to be reliable intermediaries as, ultimately, they are responsible for their own due diligence.

5.8 Politically-exposed persons

There may be a significantly increased risk in entering into business relationships with individuals holding important public positions or with persons or companies clearly related to these individuals. Politically-exposed individuals are those who have been entrusted with prominent public functions, such as heads of state or government, senior politicians, senior government officials, judicial or military officials, senior executives of public organisations and senior political party officials. The concern here is that these individuals may abuse their public powers for their own illicit enrichment through bribes, etc.

You should consider all the following risk factors when conducting a business relationship with politically-exposed persons:

(1) The country where they are from, taking into account their position(s);

(2) Any unexplained sources of wealth or income;

(3) Expected receipts of large sums from governmental bodies or state-owned entities;

(4) Any sources of wealth described as commission earned on government contracts;

(5) Requests by them to associate any form of secrecy with a transaction; and

(6) Use of accounts at a government-owned bank or use of government accounts as the source of funds in a transaction.

5.9 Non face-to-face clients

Unless a reliable intermediary (see above) has already conducted a face-to-face interview with a customer as part of its customer due diligence procedure, you should always try to conduct a face-to-face interview with a new customer.

If this is not practical, you should consider adopting the following measures:

(1) Ask that the customer's identity documents be certified by a suitable certifier such as:

(a) An embassy, consulate or high commissioner of the country of issue of the identity document;

(b) A member of the judiciary, a senior civil servant, a serving police or a customers officer in a jurisdiction that is an FATF member (see Appendix 2) or an equivalent jurisdiction;

(c) A lawyer, notary public, actuary, accountant in a jurisdiction that is an FATF member (see Appendix 2) or an equivalent jurisdiction or a member of the HKICS; or

(d) A director, officer or manager of a regulated financial institution incorporated in, or operating from, a jurisdiction that is an FATF member (see Appendix 2) or an equivalent jurisdiction;

(2) Require that additional documents be supplied on top of those required for face-to-face customers (whichever documents you consider best addresses any risk concern identified);

(3) Independent contact with the customer by you;

(4) Update the customer's information more regularly; or

(5) If necessary, refuse a business relationship with the customer unless a face-to-face interview is conducted.

5.10 Powers of Attorney

You should satisfy yourself that any power of attorney under which a person purports to act on behalf of another is a genuine power and that the attorney is the person so authorised.

5.11 Estates of deceased persons

You should satisfy yourself that, if someone claims to be acting on behalf of the estate of a deceased person, that that party is properly entitled to so act. You should scrutinise the testamentary or probate documentation from which the authority arises (grant of probate, letters of administration, etc).

5.12 Generally

There is no exhaustive list as to what constitute reasonable and proper enquiries to make in terms of due diligence. As a Chartered Secretary you should therefore consider asking for any other material that you consider appropriate in specific circumstances, such as reference letters from a client's bankers, lawyers or accountants, commercial databases, and the like. You should maintain continued due diligence throughout your relationship with a client and ensure all engagement letters are drafted in such a way as to allow your corporate services firms to terminate the relationship should a money laundering/terrorist financial issue arise.

6. Risk Considerations and Systems

6.1 Record keeping

The DTRPO and the OSCO entitle the Court to examine all relevant past transactions to assess whether a defendant has benefited from drug trafficking and/or other indictable offences.

Subject to any other statutory requirements, a company or professional firm should keep the following records for at least six years after the end of the business relationship (or after the conclusion of any investigation carried out by the authorities into the client):

(1) Records on the risk profile of each customer;

(2) Data obtained from the customer due diligence process;

(3) Copies of official identification documents;

(4) All necessary records on both domestic and international transactions sufficient to permit reconstruction of individual transactions;

(5) The client engagement letter and service contract; and

(6) Financial documentation relating to the client and transaction.

Documents may be retained in the following formats:

(1) Original documents;

(2) Hard copies;

(3) On microfiche; or

(4) In computerised form.

6.2 Identification of suspicious transactions

Given the different business sectors that Chartered Secretaries may be involved in, it is difficult to provide an exhaustive list of what is or is not a suspicious transaction. Appendix 1 provides examples of some general warning signs including both general concerns and issues specific to the services carried out by Chartered Secretaries, and is based on real examples. Identifying any warning signs listed there should prompt you to make further investigations.

The activity alone won't tell you whether a particular act is related to money laundering or terrorist financing. You will have to examine it in the context of other factors.

6.3 Employee training programmes

Money laundering and terrorist financing is an ever-changing world as criminals deploy more and more diverse and ingenious means to obscure the source of ill-gotten gains. A company or a professional firm need to develop ongoing employee training to ensure that its employees are aware of the following:

- If they become suspicious of a particular customer or transaction, they must report the matter immediately and should know who they should report to.
- They do not have to be certain, only suspicious, that the transaction relates to criminal activity.
- If they do not report their suspicions, they may be committing a criminal offence and/or be liable to disciplinary action for gross misconduct.
- They should not inform the customer of their suspicion.
- Unless instructed otherwise, they should continue to deal with the customer in the normal way.

Training should at least take place on a sufficiently regular basis. The focus for new staff, front-line staff and compliance staff should be different to accommodate their different roles. Generally, the training should include:

- Ways to identify signs of money laundering and terrorist financing that arise during the course of the employees' duties (see Appendix 1);
- Steps to be taken once the risk is identified;
- Their roles in the company's compliance efforts;
- The company's records maintenance policy;
- The disciplinary consequences for non-compliance with the DTRPO, the OSCO and the UNATMO (summaries of which can be found in section 2 of these Guidelines).

You should also advise employees to read the relevant sections of the DTRPO, the OSCO and the UNATMO.

7. Obligation to Report Suspicious Transactions/Terrorist Property

7.1 Introduction to reporting suspicious transactions

The primary role of effective AML/CFT financing guidelines is to identify suspicious transactions and, having done so, make a report to the authorities so that they can investigate and bring an end to whatever unlawful activity has sparked your suspicion.

The obligation to report money laundering activities is laid down in s 25A(1) of both the OSCO and the DTRPO, which are largely identical.

Section 25A(1) of the OSCO/DTRPO states that:

> Where a person knows or suspects that any property-
>
> (a) in whole or in part directly or indirectly represents any person's proceeds of;
>
> (b) was used in connection with; or
>
> (c) is intended to be used in connection with,
>
> an indictable offence/drug trafficking, he shall as soon as it is reasonable for him to do so disclose that knowledge or suspicion, together with any matter on which that knowledge or suspicion is based, to an authorized officer.

The authorised officer referred to in these provisions means any police officer, any member of the Customs and Excise Department (see section 8 below). Note, however, that in practice, reports are made to the Joint Financial Intelligence Unit (JFIU), which is jointly operated by the Hong Kong Police and the Hong Kong Customs and Excise Department. Full details on making a report on a suspicious transaction can be found at the JFIU website www.jfiu.gov.hk

Under s 25A(1) of the OSCO and the DTRPO, the requirement to report **does not** depend upon who committed the indictable offence/drug trafficking, or whether there is a relationship between the suspected money launderer and the person making the report (although there would usually be one). What is relevant is whether the person knows or suspects that any property wholly or partly, directly or indirectly, represents any person's proceeds of an indictable offence/drug trafficking, or was, or is, intended to be, used in connection with, an indictable offence/drug trafficking. If the answer is affirmative, he must as soon as it is reasonable for him to do so, disclose that knowledge or suspicion and any matter on which it is based to an authorised officer.

It is recommended that the following steps be taken to assess whether a transaction is suspicious and whether any report should be made under s 25A (1):

- Screen the information available (including information obtained from CDD and subsequent activities of the client) to see if there are any suspicious activity indicator(s);
- Ask the client appropriate questions to obtain further information;
- Review all the information that you have to decide whether the apparently suspicious activity is to be expected; and
- Evaluate the profile of the client against the past and/or proposed activities.

If the evaluation results in activities being considered suspicious, you should make a report to JFIU (through your compliance officer if there is one so appointed).

7.2 Meaning of indictable offence and drug trafficking

(a) Indictable offence

Indictable offences are offences of a generally more serious nature, and which can usually be tried in a higher court.

It is important to note that s 25(4) stipulates that references to an indictable offence in s 25A of the OSCO include a reference to **conduct** which would constitute an indictable offence **if it had occurred in Hong Kong**. A non-exhaustive list of the more common indictable offences which generate financial proceeds that may trigger money laundering considerations is set out in Appendix 4.

(Note: There is no need to identify the indictable offence in making report under s 25A of the DTRPO and OSCO. As long as there is suspicion that the property represents crime proceeds, a report should be made.)

(b) Drug trafficking

Drug trafficking is defined in the DTRPO to mean doing or being concerned in, **whether in Hong Kong or elsewhere**, any act constituting a "drug trafficking offence[1]. Schedule 1 of the DTRPO contains a list of drug trafficking offences, and it includes trafficking in a dangerous drug (as defined in the Dangerous Drugs Ordinance (Cap. 134)), supplying a dangerous drug to or for unauthorised persons, manufacturing dangerous drugs, and similar activities.

[1] Section 2(1)(a) of the DTRPO.

7.3 Meaning of proceeds

Under s 2(6) of the OSCO, a person's proceeds from an offence are: (i) any payments or other rewards received by him at any time in connection with the commission of that offence; (ii) any property derived or realised, directly or indirectly, by him from any of the payments or other rewards; and (iii) any pecuniary advantage obtained in connection with the commission of that offence.

Similarly, for the purposes of the DTRPO, a person's proceeds from drug trafficking are: (i) any payments or other rewards received by him at any time in connection with drug trafficking carried on by him or another; (ii) any property derived or realised, directly or indirectly, by him from any of the payments or other rewards; and (iii) any pecuniary advantage obtained in connection with drug trafficking carried on by him or another[2].

The ambit of these provisions is in fact wider than it may seem. This is because under s 2(9) of the OSCO and s 2(5) of the DTRPO, references to property received "in connection with" an offence or drug trafficking include a reference to property received in such connection **and** in "**some other connection**". It seems that these provisions aim to cover situations where the crime itself does not directly generate profit yet some sort of benefit or gain is indirectly derived.

7.4 Meaning of property

The next task is to identify what property is properly considered to be representative of, whether directly or indirectly and whether wholly or in part, the proceeds of the relevant offence. Under the OSCO and the DTRPO, property is defined to include immovable property, such as land and buildings, and movable property such as money, goods, interests and profit arising out of an interest in land and the like[3]. Note, also, that both ordinances apply to property situated in Hong Kong **or elsewhere**[4].

There is therefore room for the property which has been identified as representative of the proceeds of a particular crime to be in a different form and location from that of the original criminal proceeds. For instance, where proceeds are received in cash in Mexico, the property representing the proceeds, or any part of it, could be invested in a car in Hong Kong. While this example is simple and straightforward, there will inevitably be cases where the link between the proceeds and the property is not so clear, and a certain degree of investigation and tracing must be performed in order to ascertain a sufficient connection.

---

2 Section 4(1)(a) of the DTRPO.

3 Section 2(1) of the OSCO and the DTRPO.

4 Section 2(4) of the OSCO and S 2(3) of the DTRPO.

7.5 Meaning of knowledge or suspicion

These terms are not defined in the OSCO or the DTRPO. While what constitutes knowledge should be relatively clear, suspicion is harder to conclusively define; however it should arise from some **factual foundation** which, upon consideration, gives rise to an apprehension that a person might possibly have laundered illegal proceeds. Mere speculation is insufficient.

It must be emphasised here that what triggers the reporting obligation is the subjective knowledge or suspicion of an individual vis-à-vis the elements mentioned in the paragraphs above, and you should focus on this knowledge or suspicion. For the obligation to be triggered, it need not be proved, nor need there be concrete evidence, that a crime has in fact been committed. If you are in any doubt about whether your suspicion is enough to trigger a reporting obligation, prudence dictates either making a report or consulting the JFIU (via the 'contact us' page of the JFIU website, www.jfiu.gov.hk). You should also take care in documenting your decision-making process in case you are later required to justify adopting a non-suspicion position.

7.6 Penalty for failing to report

A person who fails to make a report when there is an obligation under s 25A(1) commits an offence and is liable to a maximum penalty of three months' imprisonment and a fine of $50,000.

7.7 Reporting of terrorist property

The UNATMO also provides for reporting obligations. Section 12(1) of the UNATMO states that:

> Where a person knows or suspects that any property is terrorist property, then the person shall disclose to an authorized officer the information or other matter-
>
> (a) on which the knowledge or suspicion is based; and
> (b) as soon as is practicable after that information or other matter comes to the person's attention.

As with the OSCO/DTRPO, a person who knows or suspects that any property is terrorist property shall disclose such information to an authorised officer. For the meaning of authorised officer and knowledge/suspicion, refer to paragraphs 7.1 and 7.5 a discussion of these terms under the OSCO/DTRPO.

7.8 Meaning of terrorist property

Terrorist property means the property of a terrorist or terrorist associate or any other property consisting of funds that is intended to be used (or was used) to finance or otherwise assist the commission of a terrorist act.

Section 2 of the UNATMO defines a "terrorist act" as follows:

(a) Subject to paragraph (b), means the use or threat of action where-

(i) The action is carried out with the intention of, or the threat is made with the intention of using action that would have the effect of-

(A) causing serious violence against a person;

(B) causing serious damage to property;

(C) endangering a person's life, other than that of the person committing the action;

(D) creating a serious risk to the health or safety of the public or a section of the public;

(E) seriously interfering with or seriously disrupting an electronic system; or

(F) seriously interfering with or seriously disrupting an essential service, facility or system, whether public or private; and

(ii) The use or threat is-

(A) intended to compel the Government or to intimidate the public or a section of the public; and

(B) made for the purpose of advancing a political, religious or ideological cause;

(b) In the case of paragraph (a)(i)(D), (E) or (F), does not include the use or threat of action in the course of any advocacy, protest, dissent or industrial action.

7.9 Penalty for failing to report

A person who fails to make a report when there is an obligation under s 12(1) commits an offence and is liable to a maximum penalty of three months' imprisonment and a fine of $50,000.

8. The Joint Financial Intelligence Unit

The Joint Financial Intelligence Unit (JFIU) was set up to receive reports about suspicious financial activity and suspicion reports relating to terrorist property made under the provisions of the DTRPO, the OSCO and the UNATMO. The JFIU is staffed by members of the Hong Kong Police Force and the Hong Kong Customs & Excise Department. The JFIU does not actually investigate suspicious transactions itself. Its role is to receive, analyse and store suspicious transactions reports and to disseminate them to the appropriate investigative unit, typically the Narcotics Bureau, the Organized Crime & Triad Bureau, the Commercial Crime Bureau of the Hong Kong Police Force, the Hong Kong Customs & Excise Department, ICAC, IRD, SFC, etc.

A company or professional firm should appoint a designated compliance officer to be responsible for accepting internal reports and for reporting to the JFIU where necessary in accordance with the DTRPO, the OSCO and the UNATMO.

Compliance officers should keep a register of:

(1) All reports made to them by employees; and

(2) All reports made to the JFIU.

Compliance officers should report suspicious transactions to the JFIU as soon as it is reasonable for them to do so. A Chartered Secretary working for a company or a professional firm should refrain from carrying out any suspicious transactions until the JFIU has been informed and consents to the company or the professional firm carrying out the transactions. Where it is not practicable to refrain from carrying out the transactions or if this would make it difficult to pursue the beneficiaries of the suspicious transactions, you may carry out the transactions and notify the JFIU as soon as it is reasonable to do so.

The JFIU has a number of different suggested proforma suspicious transaction report forms on its website. One that can be used in general circumstances can be found at www.jfiu.gov.hk/download_files/b5/C-7-HKP.doc (for Chinese Version) and at www.jfiu.gov.hk/download_files/eng/E-7-HKP.doc (for English version).

Access to information disclosed to the JFIU is restricted to (officers of the JFIU). In the event of a prosecution and the information disclosed is required to be used as evidence, production orders will be obtained to produce the materials to court.

Section 26 of both the DTRPO and the OSCO places strict restrictions on revealing the identity of the person making disclosure under s 25A (in fact, tipping a person off that a report has been made in respect of them carries a more severe sentence than failing to report a suspicious transaction). If it is known or suspected that a report has already been made to the JFIU, you should ensure that the customer does not become aware that his or her name has been brought to the attention of the law enforcement agencies. Tipping a person off as to the making of a report is a criminal offence carrying a penalty of up to $500,000 and three years' imprisonment.

Section 12(5) of the UNATMO also provides that a person shall not disclose to another person information or any other matter which is likely to prejudice any investigation following the disclosure. Any contravention of s 12(5) is a criminal offence which carries, on conviction or indictment, a fine and three years' imprisonment or, on a summary conviction, a year's imprisonment and a fine of $100,000.

PART IV: APPENDICES

Appendix 1: Examples of Suspicious Transactions

Some types of customer behaviour that might point to suspicious transactions:

- When acting as a nominee shareholder, being instructed to approve loans from the company to its directors frequently and/or for sums which are large compared to the size of the company.
- Being requested to use your own bank account to hold the proceeds of a declared dividend and then being instructed to distribute those funds to various shareholders who are unknown to you and for whom you do not act.
- When acting for an overseas client, being asked to hold funds pending their setting up a Hong Kong account of their own.
- Being asked to act in an escrow capacity in respect of funds you do not know the provenance of.
- Source of the funds is unclear or not consistent with the customer's apparent standing.
- Customer proposes payment by cash when that type of business transaction would normally be handled by other payment instruments.
- Customer proposes payment by a cheque drawn from an account other than the company account.
- Early termination of a transaction, especially at a loss.
- Customer refuses to provide an explanation of financial activity or provides an explanation assessed to be untrue.
- Delay in providing information for verification.
- Customer provides an address that is overseas or 'care of' another party.
- Customer uses an account whose name is similar to another established business entity or charity organisation.
- Customer attempts to use an account under a false name.
- A transaction involving an undisclosed party.
- Customer transfers the benefit of the transaction to an apparently unrelated third party.
- Unusual use of an intermediary in the course of a transaction.
- Customer's identity is difficult to verify.
- Customer wishes to set up companies or trusts with no apparent commercial or other purpose.
- Customer suddenly shows an unexpected improvement in financial position, without apparent commercial justification.
- Customer purchases goods or services at prices significantly above or below the market price.
- Unexplainable clearing or negotiation of third party cheques and their deposits in foreign bank accounts.
- Transfers between bank accounts of related entities or charities for no apparent reasons.
- Customer uses multiple accounts to collect funds that are then transferred to the same foreign beneficiaries.

Appendix 2: Members of the FATF

Since the list of FATF members is constantly changing, you should refer to the FATF website for the latest updates: www.fatf-gafi.org/

The FATF' s members as of 18 January 2008 are:

- Argentina
- Australia
- Austria
- Belgium
- Brazil
- Canada
- China
- Denmark
- European Commission
- Finland
- France
- Germany
- Greece
- Gulf Co-operation Council
- Hong Kong, China
- Iceland
- Ireland
- Italy
- Japan
- Kingdom of the Netherlands*
- Luxembourg
- Mexico
- New Zealand
- Norway
- Portugal
- Russian Federation
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom
- United States
- India (observer status)
- Republic of Korea (observer status)

* *the Kingdom of the Netherlands: the Netherlands, the Netherlands Antilles and Aruba*

Appendix 3: Recognised Stock Exchanges

Stock exchanges recognised by the Securities and Futures Ordinance (Cap. 571):

- American Stock Exchange
- Australian Stock Exchange
- Bolsa de Madrid
- Borsa Italiana S.p.A.
- Bourse de Montreal Inc.
- Copenhagen Stock Exchange
- Deutsche Borse AG
- Euronext Amsterdam
- Euronext Brussels
- Euronext Paris
- Helsinki Exchanges
- Japanese Association of Securities Dealers Automated Quotations
- Korea Stock Exchange
- Kuala Lumpur Stock Exchange
- London Stock Exchange
- Luxembourg Stock Exchange
- Nagoya Stock Exchange
- National Association of Securities Dealers Automated Quotations
- New York Stock Exchange
- New Zealand Stock Exchange
- Osaka Securities Exchange
- Oslo Bors
- Philippine Stock Exchange Inc.
- Singapore Exchange Securities Trading Limited
- The Stock Exchange of Hong Kong Limited
- Stock Exchange of Thailand
- Stockholmsborsen
- SWX Swiss Exchange
- Tokyo Stock Exchange
- Toronto Stock Exchange
- Wiener Borse AG

Appendix 4: Common Indictable Offences

Theft Ordinance (Cap. 210)

Section number	Offence
9	Theft: A person who dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.
10	Robbery: a person who steals, and immediately before or at the time of doing so, uses force on any person or puts any person in fear of being then and there subjected to force.
16A	Fraud: A person by deceit and with intent to defraud induces another person to commit an act or make an omission which results in either in benefit to any person other than the second-mentioned person or in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person.
17	A person who by deception dishonestly obtains property belonging to another with the intention of permanently depriving the other of it.
18	A person by deception dishonestly obtains a pecuniary advantage, meaning that he is granted by a bank a credit facility or credit arrangement, an improvement to the terms of a credit facility or credit arrangement, or a credit to an account.
21	A company director or an officer of a company publishes or concurs in publishing a false written statement with intent to deceive members or creditors.
22	A person who dishonestly destroys or conceals or procures the execution of any valuable security, any will or other testamentary document or document filed or deposited in court or a government department.
23	Blackmail: a person makes an unwarranted demand with menace with a view to gain for himself or another or with intent to cause loss to another.
24	A person handles stolen goods by dishonestly receiving the goods or undertaking or assisting in their retention, removal, disposal or realisation.

Crimes Ordinance (Cap. 200)

Section number	Offence
24	A person threatens another person with injury to his or her property, or to a third person's property, or to a deceased person's estate, with intent to alarm the person so threatened or any other person or to cause them to do an act which they are not legally bound to do or to cause them to refrain from doing an act which they are legally entitled.
71	A person making false instruments with the intention that s/he or someone will use it to induce somebody to accept it as genuine.
72	A person copying a false instrument that s/he knows to be false with the intention that s/he or someone will use it to induce somebody to accept it as genuine.
73	A person using a false instrument that s/he knows to be false with the intention that s/he or someone will use it to induce somebody to accept it as genuine.
74	A person using a copy of a false instrument that s/he knows to be false with the intention that s/he or someone will use it to induce somebody to accept it as genuine.
75	A person has in custody or under his/her control a false instrument that s/he knows to be false with the intention that s/he or someone will use it to induce somebody to accept it as genuine.
76	A person making or possessing equipment for making a false instrument that s/he knows to be false with the intention that s/he or someone will use it to induce somebody to accept it as genuine.
84	A person (e.g. principal, broker or agent) who wilfully inserts, in a contract, agreement or token of sale and purchase for the sale of share, stock or other interest in the capital stock of any bank or company, a false entry in relation to the numbers by which they are distinguished on the registers or books of the company or the names other than those of the persons in whose name the shares, stock or interest stand as registered proprietors.
85	A person, with intent to defraud, makes a false entry or alters words or figures in any books of account kept at any bank in Hong Kong or by a company or society established by charter.
86	A person (a clerk or servant of any bank in Hong Kong or any company or society established by charter), with intent to defraud, makes out or delivers any dividend warrant, or warrant for payment of any interest or money for a greater or less amount than the amount to which the person on whose behalf such warrant is made out is entitled.

Prevention of Bribery Ordinance (Cap. 201)

Section number	Offence
3	A government officer solicits or accepts any advantage without the general or special permission of the Chief Executive.
4	A person without lawful authority offers an advantage to a public servant as an inducement or reward for the public servant's: (a) performing or abstaining from performing, or having performed or abstained from performing, any act in his capacity as a public servant; (b) expediting, delaying, hindering or preventing, or having expedited, delayed, hindered or prevented, the performance of an act, whether by that public servant or by any other public servant in his or that other public servant's capacity as a public servant; or (c) assisting, favouring, hindering or delaying, or having assisted, favoured, hindered or delayed, any person in the transaction of any business with a public body. A public servant without lawful authority solicits or accepts such an advantage.
5	A person without lawful authority offers an advantage to a public servant as an inducement to or reward for the public servant's giving assistance or using influence in: (a) the promotion, execution, or procuring of any contract with a public body for the performance of any work, the providing of any service, the doing of any thing or the supplying of any article, material or substance, or any subcontract to perform any work, provide any service, do any thing or supply any article, material or substance required to be performed, provided, done or supplied under any contract with a public body; or (b) the payment of the price, consideration or other moneys stipulated or otherwise provided for in any such contract or subcontract as aforesaid. A public servant without lawful authority solicits or accepts such an advantage.

Section number	Offence
6	A person without lawful authority offers any advantage to any other person as an inducement to the withdrawal of a tender or the refraining from the making of a tender for any contract with a public body for the performance of any work, the providing of any service, the doing of any thing or the supplying of any article, material or substance. A person without lawful authority solicits or accepts such an advantage.
7	A person without lawful authority offers an advantage to any other person as an inducement to that other person's refraining or having refrained from bidding at any auction conducted by or on behalf of any public body. Any person without lawful authority solicits or accepts such an advantage.
8	A person without lawful authority, while having dealings of any kind with the government through any department, office or establishment of the government, offers an advantage to a government officer employed in that department, office or establishment of the government. A person without lawful authority, while having dealings of any kind with any other public body, offers an advantage to any public servant employed by that public body.
9	An agent who without lawful authority solicits or accepts an advantage as an inducement to doing or forbearing to do, or having done or forborne to do, any act in relation to his principal's affairs or business; or showing or forbearing to show, or having shown or forborne to show, favour or disfavour to any person in relation to his principal's affairs or business. A person without lawful authority offers an advantage to an agent as an inducement to do the above. An agent who, with intent to deceive his principal, uses any receipt, account or other document in respect of which the principal is interested, and which contains any statement which is false or erroneous or defective in any material particular and which to his knowledge is intended to mislead the principal.
10	A person who, being or having been a prescribed officer, maintains a standard of living above that which is commensurate with his present or past official emoluments, or is in control of pecuniary resources or property disproportionate to his present or past official emoluments unless he gives a satisfactory explanation to the court as to how he was able to maintain such a standard of living or how such pecuniary resources or property came under his control.

Gambling Ordinance (Cap. 148)

Section number	Offence
5	A person operates, manages or assists in the operation or management of a gambling establishment.
7	A person engages in bookmaking or holds out in any manner that he solicits, receives, negotiates or settles bets by way of trade or business.
9	A person who promotes, organises, conducts or manages, or otherwise has control of, an unlawful lottery.
15	An owner, tenant, occupier or person in charge of any premises or place knowingly permits or offers the premises or place to be kept or used as a gambling establishment.
16(a)	A person wins from another person any money or other property by fraud, misleading device or false practice.
16(b)	A person fraudulently by deception persuades, incites or induces another person to take part in gambling or a lottery.
16A	A person knowingly operates, manages or otherwise has control of or assists in the operation, management or other control of any premises or place where bookmaking or betting with a bookmaker is promoted or facilitated.
16D	An owner, tenant, occupier or person in charge of any premises or place knowingly permits or offers such premises or place to be used as premises or place mentioned in s 16A(1), or lets or agrees to let any premises or place with the knowledge that such premises or place is to be used as premises or place mentioned in section 16A(1).
16E	A person, for the purposes of dissemination or distribution in Hong Kong to the public or a section of the public, broadcasts forecasts, hints, odds or tip relating to guessing or foretelling the result of, or contingency regarding any horse, pony or dog race at any time within 12 hours before the conduct of that race.

Companies Ordinance (Cap. 32)

Section number	Offence
49G(6)	Default by company's officer in registering return disclosing purchase by company of own shares.
157J(3)	Company entering into a transaction or arrangement contrary to section 157H (i.e. loans to directors or to a company in which a director holds a controlling interest).
271(1)	An officer: (a) does not to the best of his knowledge and belief fully and truly discover to the liquidator all the property of the company, and how and to whom and for what consideration and when the company disposed of any part of it, except such part as has been disposed of in the ordinary way of the business of the company; or (b) does not deliver up to the liquidator all property of the company as is in his custody or under his control, and which he is required by law to deliver up; or (c) does not deliver up to the liquidator all books and papers in his custody or under his control belonging to the company and which he is required by law to deliver up; or (d) within 12 months next before the commencement of the winding up or at any time thereafter conceals any part of the property of the company to the value of $100 or upwards, or conceals any debt due to or from the company; or (e) within 12 months next before the commencement of the winding up or at any time thereafter fraudulently removes any part of the property of the company to the value of $100 or upwards; or (f) makes any material omission in any statement relating to the affairs of the company; or (g) knowing or believing that a false debt has been proved by any person under the winding up, fails for the period of a month to inform the liquidator; or (h) after the commencement of the winding up prevents the production of any book or paper affecting or relating to the property or affairs of the company; or (i) within 12 months next before the commencement of the winding up or at any time thereafter, conceals, destroys, mutilates, or falsifies any book or paper affecting or relating to the property or affairs of the company; or (j) within 12 months next before the commencement of the winding up or at any time thereafter makes any false entry in any book or paper affecting or relating to the property or affairs of the company; or

Section number	Offence
	(k) within 12 months next before the commencement of the winding up or at any time thereafter fraudulently parts with, alters, or makes any omission in any document affecting or relating to the property or affairs of the company; or (l) after the commencement of the winding up or at any meeting of the creditors of the company within 12 months next before the commencement of the winding up attempts to account for any part of the property of the company by fictitious losses or expenses; or (m) within 12 months next before the commencement of the winding up or at any time thereafter pawns, pledges, or disposes of any property of the company which has been obtained on credit and has not been paid for, unless such pawning, pledging, or disposing is in the ordinary way of the business of the company; or (n) is guilty of any false representation or other fraud for the purpose of obtaining the consent of the creditors of the company or any of them to an agreement with reference to the affairs of the company or to the winding up.
272	Officer falsifying books.
273	Officer acting with intent to defraud creditors by giving or concealing property of company in liquidation.
275(3)	Person being a party to carrying on the business of a company with intent to defraud creditors.
342F(1)	Authorising the issue, circulation or distribution in Hong Kong of a prospectus relating to shares in or debentures of an overseas company containing an untrue statement.

Appendix 5: Useful Websites

Websites referred to in this guideline:

- **Securities and Futures Commission (SFC)**
  www.sfc.hk
- **Hong Kong Monetary Authority (HKMA)**
  www.info.gov.hk/hkma/eng/guide/index.htm
- **Inland Revenue Department (IRD)**
  www.ird.gov.hk/eng/tax/ach_index.htm
- **Joint Financial Intelligence Unit (JFIU)**
  www.jfiu.gov.hk
- **Financial Action Task Force (FATF)**
  www.fatf-gafi.org

Other useful websites:

- **Department of Justice Bilingual Laws Information System (BLIS)**
  www.legislation.gov.hk/eng/index.htm
- **Narcotics Division, Security Bureau**
  www.nd.gov.hk
- **Hong Kong Police**
  www.info.gov.hk/police
- **Hong Kong Customs and Excise Department**
  www.customs.gov.hk
- **Independent Commission Against Corruption (ICAC)**
  www.icac.org.hk
- **Office of the Commissioner of Insurance (OCI)**
  www.oci.gov.hk
- **Estate Agents Authority (EAA)**
  www.eaa.org.hk/welcome.htm
- **United Nations Security Council (UN)**
  www.un.org/Docs/sc

These guidelines are intended to assist members of the HKICS in complying with their obligations under the legislation concerning anti-money laundering and counter-terrorist financing in Hong Kong. These guidelines are not a definitive guide nor are they intended to replace seeking legal advice in particular circumstances.

The Hong Kong Institute of Chartered Secretaries

Hong Kong Office
3/F., Hong Kong Diamond Exchange Building,
8 Duddell Street,
Central, Hong Kong
Tel: (852) 2881 6177
Fax: (852) 28815050
Email: ask@hkics.org.hk
Website: www.hkics.org.hk

Beijing Representative Office
Rooms 1014-1015
10/F., Jinyu Mansion
No.129 Xuanwumen Xidajie
Xicheng District
Beijing, China P.C. 100031
Tel: (86 10) 6641 9368
Fax: (86 10) 6641 9078
Email: bro@hkics.org.hk