Hong Kong Institute of Certified Public Accountants 香港會計師公會

Accounting and Financial Reporting Council 會計及財務匯報局

May 2026 (revised)

Anti-Money Laundering and Counter-Terrorist Financing

Frequently asked questions on

Suspicious transaction reporting

HONG KONG INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

Anti-Money Laundering and Counter-Terrorist Financing
Frequently Asked Questions on Suspicious Transaction Reporting

Reporting suspicious transactions is important as it is a legal obligation, supports law enforcement, safeguards the integrity of Hong Kong's financial system, and reinforces the gatekeeper role of professional accountants.

The frequently asked questions ("FAQs") in this document have been prepared by the Hong Kong Institute of Certified Public Accountants ("Institute") in collaboration with the Accounting and Financial Reporting Council ("AFRC") and with the input from the Joint Financial Intelligence Unit ("JFIU")[1].

The FAQs draw the attention of members of the Institute ("members") to the obligation to report suspicious transactions, as part of the accounting profession's commitment to implementing Hong Kong's overall anti-money laundering and counter-terrorist financing ("AML/CTF") regime. Specifically, they provide information and guidance on various issues relating to the filing of suspicious transaction reports ("STRs"), including when and how members should file STRs. They also provide guidance on how to improve the quality of STRs and better tailor them to assist the JFIU and law enforcement agencies ("LEAs") in the prevention and detection of money laundering/terrorist financing ("ML/TF") activities.

This document does not constitute legal advice. In case of doubt, members should seek their own legal advice. While this document does not form part of the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing for Professional Accountants (Revised May 2023) issued by the Institute ("AML Guidelines"), members should take note of the contents and, if necessary, review their policies, procedures, and controls in the light of the contents.

[1] Joint Financial Intelligence Unit is a financial intelligence unit run jointly by the Hong Kong Police Force and the Hong Kong Customs and Excise Department.

A. Background – reporting by accountants on suspicious transactions

Since the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("AMLO") was extended in 2018 to cover designated non-financial businesses and professions ("DNFBPs"), including accounting professionals, the accounting profession has submitted only a limited number of STRs to the JFIU, which is consistent with the observations made by the Financial Action Task Force ("FATF") in its 2018/19 Mutual Evaluation of Hong Kong's AML/CTF regime[2]. This stands in contrast to other relevant DNFBPs in Hong Kong[3].

In the course of inspections of firms of certified public accountants ("practices"/"CPA firms"), the AFRC observed that practices often viewed solid, verifiable proof as necessary before filing a report, although such proof is not required under the law or relevant guidelines. An STR must be submitted if a practice forms a suspicion.

Therefore, these FAQs have been developed to provide practical guidance on what and how to report, clarify the concept of "suspicion", and support a more consistent approach to making STRs across the profession.

B. Frequently asked questions on suspicious transaction reporting

General requirements

1. Why is reporting suspicious transactions important?

As noted above, reporting suspicious transactions is a legal obligation in Hong Kong, as in many other places, and has been a requirement in Hong Kong under relevant ordinances for many years. In addition, the FATF has issued a set of Recommendations that provide a comprehensive and consistent framework of measures which jurisdictions should implement in order to combat ML/TF, as well as the financing of the proliferation of weapons of mass destruction. Jurisdictions that do not have an effective regime for combating ML/TF could be regarded as high risk, which will have implications for them and other parties doing business with them.

---

[2] The FATF, which is the international, inter-governmental body spearheading efforts to combat ML/TF, through the development and promotion of national and international policies, as well as specific measures, aimed at countering ML/TF, published the Mutual Evaluation Report on Hong Kong on 4 September 2019, generally commending Hong Kong's efforts in combating ML/TF. However, it made various references to the low number of STRs submitted by DNFBPs, e.g., "*The level of STR reporting by DNFBPs is low and is not commensurate with the risks"* (page 108) and the report suggests the need for more capacity building to encourage STR reporting by DNFBP sectors (page 108). A follow-up report was issued in 2023. The FATF has also issued other useful publications and guidance, including guidance for accountants on setting out risk categories and procedures for applying a risk-based approach to countering ML/TF.

[3] Out of the 190,636 STRs submitted in 2025, only 16 STRs (accounting for less than 0.01%) were submitted by accounting professionals. This is a significantly lower than other DNFBPs. In comparison, in the United Kingdom, out of the 866,616 Suspicious Activity Reports submitted in the period from April 2024 to March 2025, around 6,153 (0.71%) were submitted by accounting professionals. While STRs filed in other sectors, such as the trust and company service providers in Hong Kong, may have been made by professional accountants who are providing corporate and secretarial services, under the law, this is a different regulated sector from accounting professionals.

Core FATF Recommendations applicable to accountants and other DNFBPs, as well as financial institutions, relate to:

- Customer due diligence ("CDD")
- Record keeping
- **Suspicious transaction reporting**

Accordingly, it is important for the reputation and standing of the profession in Hong Kong internationally and, equally importantly, to safeguard the integrity of Hong Kong's financial markets, that members working in practice and other professional firms (who are the target of the FATF Recommendations in relation to accounting professionals) fully understand their legal obligations in relation to submitting STRs and make timely reports when suspicion arises.

2. What are the relevant ordinances and key legal requirements in relation to making suspicious transaction reports?

The main ordinances to be aware of are the following:

- Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("DTROP")
- Organized and Serious Crimes Ordinance (Cap. 455) ("OSCO")
- United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("UNATMO")

In addition, the following are relevant (see also FAQ 3):

- United Nations Sanctions Ordinance (Cap. 537) ("UNSO")
- United Nations Sanctions (Democratic People's Republic of Korea) Regulation (Cap. 537AE) ("Cap. 537AE")
- United Nations Sanctions (Joint Comprehensive Plan of Action – Iran) Regulation (Cap. 537BV) ("Cap. 537BV")
- Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526) ("WMDO")

Key provisions include the following:

Under DTROP and OSCO[4], a person must make a disclosure to an authorized officer[5] as soon as it is reasonable for him/her to do so, if he/she knows or suspects that any property:

(a) in whole or in part, directly or indirectly, represents the proceeds of;

[4] Section 25A(1) of DTROP and OSCO

[5] Please refer to Part C - Glossary for the meaning of "authorized officer" and "person". In practice, STRs will generally be made to the JFIU.

(b) was used in connection with; or
(c) is intended to be used in connection with,

drug trafficking (under DTROP)/an indictable offence (under OSCO).

Further, under UNATMO[6], where a person knows or suspects that any property is terrorist property, the person must 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.

It is an offence under DTROP/OSCO and UNATMO[7], carrying a maximum penalty of three months' imprisonment and a fine of HK$50,000 (level 5[8]), to fail to make a disclosure to an authorized officer where a person has the requisite knowledge or suspicion.

It should be noted that for the statutory obligation to report to arise, it is not necessary to be able to identify or suspect:

(a) the specific nature of the offence, or even to establish that an offence has, in fact, been committed or will be committed, or
(b) the specific nature of the terrorist act for which the property was, or is intended to be, used to finance, or that a particular person is, in fact, a terrorist or a terrorist associate.

It should be noted that the terms "terrorist property" and "proceeds" are defined quite widely in Hong Kong legislation. Please refer to ***Part C – Glossary*** for details.

3. Does the requirement to report suspicious transactions apply only to suspected money laundering and terrorist financing?

No, STRs should also be made in respect of suspected breaches of UN sanctions against proliferation financing. This relates to efforts to combat the proliferation of weapons of mass destruction and UN sanctions, specifically against North Korea and Iran, and the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in FATF Recommendation 7. Relevant legislation here includes those outlined in FAQ 2, namely, UNSO, Cap. 537AE, Cap. 537BV and WMDO.

[6] Section 12(1) of UNATMO

[7] Section 25A of DTROP/OSCO and section 14(5) of UNATMO

[8] Standard levels of fines under various ordinances are specified in Schedule 8, Criminal Procedure Ordinance (Cap. 221).

See also the FATF Guidance on Counter Proliferation Financing.

4. Who must comply with the legal requirements in relation to making suspicious transaction reports?

The law on STR reporting in Hong Kong (see FAQ 2) is very broad. Under the relevant legislation, all persons, including, therefore, all practices and members working in practices, and also, for example, "responsible persons" under the Limited Partnership Fund Ordinance (Cap. 637) ("LPFO") who are accounting professionals[9], are required to report suspicious transactions.

The obligation also extends to professional firms owned or controlled by members. Regardless of the services/activities carried out by such firms/members[10] (whether audit, tax compliance/advisory services, insolvency, etc.), it is a legal obligation to perform suspicious transaction reporting. Some accountancy and trust and company service provider services that tend to be more vulnerable to money launderers include:

(a) **Financial and tax advice** – Criminals may ask for help placing assets out of reach of local authorities or setting up offshore trusts and companies for tax evasion purposes.

(b) **Bookkeeping** – Criminals may disguise transactions or delete them from records. This can include manipulating accounts receivable and accounts payable.

(c) **Creating corporations or complex legal arrangements** – Criminals may wish to create companies, trusts, and charities designed to distance themselves from criminal activity.

(d) **Wanting nominee shareholders, trustees, or directors for legal persons or complicated arrangements** – Criminals can avoid association while retaining effective control of a business.

(e) **Buying or selling properties or businesses** – Criminals may use large purchases to hide or transfer unlawful funds.

(f) **Managing funds, accounts, securities or, other assets** – This includes cash or shares transactions, foreign exchange operations, issuing or cashing cheques, and international funds transfers.

(g) **Providing a registered or correspondence address** – This helps criminals hide their true location and make their activities appear more legitimate.

[9] Under section 33(1) of the LPFO, the general partner in a limited partnership fund must appoint a person (who may be the general partner or another person) as a responsible person to carry out the measures set out in Schedule 2 of the AMLO. Under section 33(2) of the LPFO, a responsible person may be an accounting professional.

[10] It should be noted that the requirement of suspicious transaction reporting applies universally to all persons, including individuals and entities engaged in activities prescribed in section 5A of AMLO or subsection 600.2 of the AML Guidelines.

Suspicious transaction indicators and meaning of "suspicion"

5. Where can I find more information on suspicious transaction indicators?

The JFIU has listed some examples of suspicious transaction indicators on its website. Additional indicators can be found in Appendix D of the AML Guidelines, while some more specific examples can be found in Part F of this document.

In some circumstances, transactions involving high-risk jurisdictions, especially where this is outside of expectations in relation to a particular client, could be an indicator. More information on high-risk jurisdictions can be found in Part E of this document.

6. What counts as "suspicion"?

The dictionary defines "suspicion" as implying a belief or opinion based upon facts or circumstances that do not constitute proof. Case law and other sources indicate that suspicion is more than speculation, but less than proof or knowledge. While suspicion is personal and subjective, it will generally be built upon some objective foundation and should not be based simply on bias or prejudice. Once a person has formed a suspicion, there is a duty to report.

From a practice's perspective, where, for example, a transaction or a series of transactions of a client is not consistent with the knowledge of the client, or is unusual, such as a pattern that has no apparent economic or lawful purpose, the practice should take appropriate steps to further examine the transactions and identify if there is any suspicion.

Please refer to the JFIU's website for details on "**How to identify a Suspicion?**".

What and how to report

7. What are the procedures to report suspicious transactions?

Members, or the appropriate person within practices (for example, the Money Laundering Reporting Officer ("MLRO") designated by practices for AML/CTF purposes) should submit STRs to the JFIU.

The JFIU has upgraded its Suspicious Transaction Report and Management System (STREAMS) to STREAMS 2, which was launched on 2 February 2026. **CPA firms and other entities regulated for AML/CTF are no longer able to submit STRs via email, fax, or post. All STRs must be submitted electronically through STREAMS 2**. Three submission options are available:

- Submit an STR via XML Submission (an electronic certificate (e-cert) is required);
- Upload a completed STR in the prescribed PDF format in STREAMS 2 (e-cert

is required); and
- Complete an STR web-form directly in STREAMS 2 (e-cert is not required).

User account registration

A STREAMS 2 user account can be opened by completing the application form and returning it to the JFIU (jfiu@police.gov.hk).

For enquiries, reporting entities/persons can contact the JFIU by telephone (852) 2866 3366 or by email to jfiu@police.gov.hk.

Please refer to the JFIU's website for more information on:

- When to submit an STR?
- How to submit an STR?
- What to report in an STR?

8. What are the appropriate formats and contents of a suspicious transaction report?

Format of STRs

While practices and other professional firms may have their own formats for internal reporting, STRs should have a structured format and contain all relevant information, based on the following "SAFE" principles:

(a) **S**tructure the content systematically (for easier comprehension);

(b) **A**void providing non-editable transaction records to the JFIU, as far as possible;

(c) **F**ocus on the main subject and be concise; and

(d) **E**nsure appropriate use of file attachments.

While it is recognized that practices may not always be able to identify the exact nature of any underlying crime, they should report or select the most likely category of crime on a "best efforts" basis.

Structure of STRs

STRs should contain sufficient information to assist the JFIU in understanding the background for analysis and investigation. While the information required for each STR will vary, it is important to ensure that sufficient information, as is reasonably available, is provided and that the mandatory fields, e.g., account number and balance, are completed, on a "best efforts" basis.

Providing the basic background information on the client is only the first step. A summary should also be provided, explaining the grounds for, and analysis of, the knowledge or suspicion, e.g., which suspicious indicators or red flags are present.

Suspicion should be supported by further information on relevant conduct or activities. STRs should not be made purely on the basis of a client's business being high risk, without the presence of requisite knowledge or suspicion, and supporting details of any unusual activities.

Avoid providing non-editable transaction records

Practices should provide transaction records, if any, that are comprehensible, with an explanation of any abbreviations used, and in an editable format, where possible, to facilitate the JFIU's further processing and analysis.

Focus on the main subject and be concise

STRs should be precise and concise with sufficient information to establish suspicion and facilitate follow-up enquiries. Events should be described in logical, chronological order, avoiding acronyms and jargon where possible. Where a service/technical aspect of the practice's engagement is being reported, it is suggested that a brief synopsis of the service/engagement be provided.

Entities involved in different layers of suspected fraud and ML, where known, should be included to give a fuller picture of the potential criminal activity. Where entities are only remotely associated with the subject of an STR, practices should assess their relevance and consider whether they should be included or covered in separate STRs.

Where a network of relationships or accounts has been identified, practices should report the network in the same STR, as far as reasonably practicable. To help the JFIU and LEAs conduct analyses and investigations more efficiently, practices should include sufficient information and may include a linked chart to illustrate the connections among the subjects, organizations, and/or accounts.

Where enquiries have been made with clients to clarify or gather more information, the results (i.e., brief details of those enquiries) may also be relevant. However, when making such enquiries with the clients, practices should also be mindful of the risk of tipping off, as referred to in FAQ 14.

The sources of funds for the transactions, the client's source of wealth, and connected accounts or relationships are often key information that supports suspicion and should be included in the STR.

Appropriate use of file attachments

Narrative information should be entered in the relevant field under "suspicious

indicator" in the STR proforma. This information is sometimes included in file attachments to the STRs, which makes prompt assessment by the JFIU more difficult. Attachments[11] should only be used to supplement the information provided in the narratives. For instance, where a network of suspicious relationships is reported, practices could attach a diagram to help illustrate the connections among the parties.

Further details of information to be included in STRs can be found in ***Part G – Topics to be covered in a suspicious transaction report*** of this document.

9. Can a suspicious transaction report relate to an overseas offence or suspected offence?

Yes, section 25 of DTROP/OSCO states:

In this section and section 25A, references to an indictable offence include a reference to conduct which would constitute an indictable offence if it had occurred in Hong Kong.

However, if there is no nexus to Hong Kong and, for example, a member identifies a suspicious transaction that has no connection to Hong Kong while working in, or visiting, an overseas office, in principle, this may be reportable to the local equivalent of the JFIU, rather than the JFIU, depending upon the AML/CTF requirements in that jurisdiction.

Other matters relating to suspicious transaction reports

10. Would making a suspicious transaction report be considered a breach of any restriction on disclosure of information?

No, a disclosure made in good faith to JFIU will not be treated as a breach of any contract, enactment, rule of conduct, or other provision restricting disclosure of information, and will not render the person making the disclosure liable in damages for any loss arising out of the disclosure. This is made clear in DTROP/OSCO and UNATMO[12].

In addition, while reporting suspicion is a legal requirement, in and of itself, it may also minimize the risk of breaching section 25 of DTROP/OSCO, on dealing with property known or believed to represent proceeds of indictable offence, or section 8A of UNATMO, on dealing with certain property knowing that, or being reckless as to whether, the property is terrorist property or related otherwise to terrorists/terrorist associates, which are very serious offences.

[11] Where attachments are used, they should be named in a way that reflects the nature of the document in order to assist the JFIU's investigation.

[12] Section 25A of DTROP/ OSCO and section 12 of UNATMO

11. Is it always necessary to report directly to the Joint Financial Intelligence Unit?

Not necessarily, in the case of employees. Under DTROP/OSCO and UNATMO, once employees have reported their suspicions to an appropriate person (for example, the MLRO) in accordance with the procedure established by their employers for the making of such disclosures, they have fully satisfied their statutory obligation[13].

In other words, it is sufficient for an employee to make a report to a person designated by the practice as the MLRO, to receive reports from staff. The MLRO is responsible for making the decision on whether or not to file an STR to the JFIU. In order to be able to fulfil the role adequately, the MLRO should be a person of sufficient seniority and authority within the organization (see also subsection 610.4 of the AML Guidelines).

12. Is the identity of the person filing a suspicious transaction report protected?

The identity of the person filing an STR is kept strictly confidential. Access to the disclosed information is restricted to financial investigating officers within the LEAs. DTROP/OSCO and UNATMO[14] impose tight restrictions on revealing the identity of the person making the report. The LEAs have indicated that they consider maintaining the integrity of the relationship established between LEAs and the financial and non-financial sectors to be of paramount importance.

13. Should a person who has made a suspicious transaction report to the Joint Financial Intelligence Unit, or an internal report to a Money Laundering Reporting Officer, expect to receive feedback on follow-up action taken?

While there is no hard and fast rule, and for employers, this may depend on the internal procedures set out by the employers, in principle, it would be good practice for the MLRO to update employees who have made internal STRs that follow-up action has been taken (although not necessarily to confirm that an STR has, or has not, been made to the JFIU, where that is the case, in order to minimize the risk of any subsequent tipping off) or at least to acknowledge receipt of the internal report and indicate that it will be followed up. This would help to demonstrate that employees' efforts to relay their knowledge or suspicions to the management of the employer are being taken seriously.

The JFIU will acknowledge receipt of an STR made by an entity under section 25A of DTROP/OSCO, and section 12 of the UNATMO. If there is no need for imminent action, e.g., the issue of a restraint order on an account, consent will usually be given for an account to be operated under the provisions of section 25A(2)(a) of DTROP/OSCO, and section 12(2B)(a) of the UNATMO. If, on the other hand, a practice is aware that a restraint has been put on a client's account, it should take appropriate action and seek legal advice where necessary.

[13] Section 25A(4) of DTROP/OSCO and section 12(4) of UNATMO

[14] Section 26 of DTROP/OSCO, and section 12 of UNATMO

A practice should conduct an appropriate review of a business relationship upon the filing of an STR to the JFIU, irrespective of any subsequent feedback provided by the JFIU, and apply appropriate risk mitigating measures. Filing a report with the JFIU and continuing to operate the relationship without any further consideration of the risks and the imposition of appropriate controls to mitigate the risks identified would be inappropriate. Generally, the issue should be escalated to the practice's senior management to determine how to handle the relationship concerned, to mitigate any potential legal or reputational risks posed by the relationship, in line with the practice's business objectives, and its capacity to mitigate the risks identified.

Once an STR number is assigned, it represents that the JFIU has acknowledged the STR. The practice would be able to check the consent status in the system.

Practices should be aware that making an STR does not remove the need to report further suspicious transactions in respect of the same client. Further suspicious transactions, whether of the same nature or different from the previous suspicion, should continue to be reported by members to the MLRO, who should make further reports to the JFIU if appropriate.

Tipping off and training

14. What is "tipping off" and what are the potential consequences of tipping off?

"Tipping off" is where a person, knowing or suspecting that a disclosure (i.e., an STR) has been made to the JFIU, or, internally, to a compliance officer, such as an MLRO, discloses to another person any matter that is likely to prejudice an investigation that might be conducted as a result.

It does not matter whether that person knows or believes an investigation has actually started, he/she needs to consider the consequences that disclosing information could prejudice a future investigation. "Any matter" could include:

- Information that establishes that an STR has been made, or that a requirement to submit an STR has been triggered;
- A report made or prepared for the purposes of meeting STR obligations, including any copies; or
- Any document purporting to set out information contained in an STR.

"Prejudicing an investigation" means doing something that could negatively affect an investigation. You do not need to know that a disclosure will negatively affect an investigation. Whether a disclosure would be likely to prejudice an investigation will often depend on a combination of:

- *What* information is disclosed;
- *To whom* the information is disclosed;
- *How* the disclosure is made; and

- *When* the disclosure is made.

Tipping off is a criminal offence under section 25A of DTROP/OSCO and section 12 of UNATMO, carrying a maximum penalty, on conviction upon indictment, of three years' imprisonment and a fine of $500,000 (or imprisonment of one year and a fine of $100,000 (level 6), upon summary conviction).

Disclosures of information to other LEAs will also not generally breach the tipping off offence. However, it would be advisable to alert them if an STR has already been made to the JFIU. These LEAs include the police and agencies that have investigative functions, such as the:

- Department of Justice
- Hong Kong Police Force
- Independent Commission Against Corruption
- Hong Kong Customs and Excise Department
- Immigration Department

Reducing the risk of tipping off

Tipping off can occur if practices and professional firms do not have suitable controls in their business to prevent tipping off. This includes when sharing information within a reporting group or with a third party.

Under subsection 640.1 of the AML Guidelines, practices must ensure that they have in place internal controls to prevent any partner, director, or employee from committing the offence of "tipping off" a client, or any other person who is the subject of the report.

15. Should employees receive training in relation to making suspicious transaction reports?

Yes, under section 670 of the AML Guidelines, practices should provide staff training that covers, among other things, the practice's obligation to report suspicious transactions (subsection 670.1.5), and information on the offence of tipping off, for relevant employees (subsection 670.1.6), to ensure that they understand the offence and how to reduce the risk of falling foul of it. For further information, see sections 610, 640, and 670 of the AML Guidelines.

C. Glossary

“Authorized officer” means:

(a) a police officer;
(b) a member of the Customs and Excise Service established by section 3 of the Customs and Excise Service Ordinance (Cap. 342);
(c) a member of the Immigration Service established by section 3 of the Immigration Service Ordinance (Cap. 331); or
(d) an officer of the Independent Commission Against Corruption established by section 3 of the Independent Commission Against Corruption Ordinance (Cap. 204).

“Client” includes:

a prospective client

“Dealing” includes:

(a) receiving or acquiring the property;
(b) concealing or disguising the property (whether by concealing or disguising its nature, source, location, disposition, movement, or ownership or any rights with respect to it or otherwise);
(c) disposing of or converting the property;
(d) bringing into, or removing the property from Hong Kong; and
(e) using the property to borrow money, or as security (whether by way of charge, mortgage or pledge or otherwise)

“Indictable offence” is:

an offence that is tried on indictment and includes an offence that may be tried either summarily or on indictment (Please refer to ***Part D - Examples of indictable offences*** for details).

“Law enforcement agencies” refers mainly to:

the authorities designated to investigate ML/TF offences in Hong Kong. The primary investigative authorities are the Hong Kong Police Force and the Customs and Excise Department. In the event that ML/TF offences are facilitated by corruption, the Independent Commission Against Corruption will investigate such cases (see also the definition of “authorized officer”, above)

“Person” is defined to:

include any public body and any body of persons, corporate or unincorporated, and the definition applies notwithstanding that the word “person” occurs in a provision creating or relating to an offence or for the recovery of any fine or compensation, under the Interpretation and General Clauses Ordinance (Cap. 1).

“Proceeds” include:

(a) payments or other rewards received at any time in connection with the commission of that offence;
(b) property derived or realized, directly or indirectly, from any of the payments or other rewards; and
(c) pecuniary advantage obtained in connection with the commission of that offence

“Terrorist property” is:

(a) the property of a terrorist or terrorist associate; or
(b) any other property consisting of funds that:
    (i) is intended to be used to finance or otherwise assist the commission of a terrorist act; or
    (ii) was used to finance or otherwise assist the commission of a terrorist act.

D. Examples of indictable offences

Ordinance	Offence	Section
Cap.32, Companies (Winding up and Miscellaneous Provisions) Ordinance	Offences by officers of companies in liquidation Falsification of books Responsibility of directors for fraudulent trading Criminal liability for misstatements in prospectus For other offences, reference can be made to Schedule 12 of the Ordinance	s271 s272 s275 s342F -
Cap.622, Companies Ordinance	Officer recklessly or knowingly making false statements, etc., to auditors	s413
Cap.112, Inland Revenue Ordinance	Fraud, etc., with intent to evade or assist any other person to evade tax	s82
Cap.134, Dangerous Drugs Ordinance	Trafficking in a dangerous drug, or offering to traffic in a dangerous drug or in a substance believed to be a dangerous drug, or doing/ offering to do acts for this purpose Manufacturing a dangerous drug or doing/offering to do an act preparatory to, or for the purpose of, manufacturing a dangerous drug	s4 s6
Cap.210, Theft Ordinance	Theft Fraud False accounting	s9 s16A s19
Cap.405, DTROP	Reference can be made to Schedule 1 of the Ordinance	-
Cap. 455, OSCO	Reference can be made to Schedules 1 and 2 of the Ordinance	-
Cap. 526, WMDO	Prohibition on providing services in relation to weapons of mass destruction	s4

Cap.571, Securities and Futures Ordinance	Offence of insider dealing	s291
	Offence of disclosure of information about prohibited transactions	s297
	Offence of disclosure of false or misleading information inducing transactions	s298

E. Consideration of high-risk jurisdictions

When assessing whether a country presents higher ML/TF risk, it is useful to start with recognized international benchmarks, in particular, countries subject to international sanctions, as well as the FATF's lists of high-risk and monitored jurisdictions.

Sanctioned jurisdictions

Information about UN-sanctioned jurisdictions can be found in different locations, including:

- The Institute's website, and the websites of different Hong Kong AML/CTF regulators, including the Hong Kong Monetary Authority, the Securities and Futures Commission, and the Companies Registry;
- The website of the Commerce and Economic Development Bureau of the Hong Kong SAR Government; and
- The United Nations Security Council website.

Whatever the source used, it should be checked regularly for updates.

As regards sanctions applied by individual jurisdictions, or regional groups, like the European Union, while they may be regarded as "unilateral" sanctions, these lists may also be indicative of higher-risk jurisdictions. These lists include:

- Office of Foreign Assets Control in the United States
- European Union sanctions list

FATF high-risk and monitored jurisdictions

A good starting point is the FATF webpages on high-risk and other monitored jurisdictions. See also paragraphs 620.12.27 - 620.12.30 of the AML Guidelines. As regards jurisdictions under increased monitoring, the FATF explains:

Jurisdictions under increased monitoring are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the "grey list".

The FATF and FATF-style regional bodies continue to work with the jurisdictions below as they report on the progress achieved in addressing their strategic deficiencies. The FATF calls on these jurisdictions to complete their action plans expeditiously and within the agreed timeframes. The FATF welcomes their commitment and will closely monitor their progress. The FATF does not call for the

application of enhanced due diligence measures to be applied to these jurisdictions. The FATF Standards do not envisage de-risking, or cutting-off entire classes of customers, but call for the application of a risk-based approach. Therefore, the FATF encourages its members and all jurisdictions to take into account the information about such jurisdictions on the FATF website in their risk analysis.

It should be noted that the situation is not static and jurisdictions may be added to, or removed, from the list of high-risk jurisdictions and those subject to increased monitoring. It is important, therefore, to check for any updates before taking specific action in relation to jurisdictions that are potentially high risk.

F. Examples of potential suspicious transactions

Further examples requiring consideration of filing STRs are provided below.

Client Risk	
Example 1	A client or its beneficial owner(s) that becomes subject to new sanctions should be treated as a significant risk indicator. **Illustrative Example:** After a client relationship has been established or continued, the client or its beneficial owner(s) may become subject to UN sanctions. Even if they become subject to sanctions imposed by specific jurisdictions or regional groups (e.g., the United States or the European Union) that are not directly applicable in Hong Kong, such a development could still be an indicator of suspicious activity that warrants further assessment and reporting when considered together with the client's transactions or activities, where appropriate.
Example 2	A client appears to be acting on behalf of somebody else's instruction or behaves evasively/defensively during questioning. **Illustrative Example:** A client intends to establish a business relationship with your firm but is unable or unwilling to answer certain basic questions about his own company (e.g., history, scale of operations, nature of the business of the counterparts). The absence of knowledge about his own business might suggest that he is not the ultimate owner or controller of the company.
Example 3	A client assigns his family or close associates as nominee shareholders or directors without any apparent legal, economic or rational reason. **Illustrative Example:** A client refuses to explain the sudden change of shareholders or directors to be their family or close associates, which could raise consideration about the underlying intent of this arrangement.

Example 4	Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic, or other legitimate reason. **Illustrative Example:** A client intends to buy an entity which is failing in business at an exceptionally high price. The absence of a rational economic or business reason raises concerns about the legitimacy and the underlying intent of this acquisition.
Example 5	A client appears to be using a personal account for business purposes, or vice versa. **Illustrative Example:** All business income and expenses should be transacted exclusively through corporate bank accounts. A substantial volume of business payments or business-related transactions processed via a client's personal bank account may indicate an increased risk of tax evasion. In such cases, further inquiry is warranted to understand the rationale for using personal accounts and to assess whether the circumstances give rise to a suspicion that should be reported.
Example 6	A client has no employees, which is abnormal for the type of business. **Illustrative Example:** A company operating in Hong Kong with numerous transactions and an exceptionally large turnover, but with no employment record (e.g., as revealed by tax filings/Mandatory Provident Fund records). The absence of staff at a company of such scale might be a red flag that it is merely a shell or front company.
Transaction/Service Risk	
Example 7	Suspicious activity based on transaction patterns, e.g., "U-turn" transactions or apparently fictitious revenue. **Illustrative Example:** Funds are being transferred between the client and its suppliers without any evidence of the actual delivery of goods or services. In some cases, these payments are later followed by refunds from the suppliers, resulting in transaction cycles that lack a clear economic rationale.

	Such patterns raise serious concerns regarding the legitimacy of the transactions and suggest possible misuse for money laundering or layering schemes. Additional red flags that further heighten suspicion include: • Fund transfers occurring immediately before the end of a month or fiscal year, potentially to manipulate financial statements or obscure the true nature of the transactions. • Suppliers and customers sharing the same or nearby business addresses, which may indicate collusion or the existence of fictitious entities. • Unusual transaction volumes or frequencies that do not align with the client's typical business activities. • Absence of adequate supporting documentation or the presence of inconsistencies in invoices and shipping documents. • Absence of supporting evidence for certain material revenue recognized in the financial statements. • Over or under invoicing of goods/services. • Multiple invoicing of the same goods/services. • False description of goods/services (e.g., inconsistent entries on bills of lading).
Example 8	Transactions that have no apparent legitimate purpose or commercial rationale — such as unnecessary or circuitous routing of funds or other assets to or from third parties, or through third-party accounts. **Illustrative Example:** A client engages in a series of complex financial arrangements that lack genuine commercial substance. For instance, the client may issue and repurchase its own financial instruments shortly after they were issued, or may purchase financial instruments through an intermediary in a back-to-back transaction. Such arrangements serve to obscure the true relationships among the parties involved and may disguise beneficial ownership, financial exposure, or the actual flow of funds. These practices raise serious concerns regarding both the legitimacy of the transactions and the potential intent to evade regulatory scrutiny or facilitate money laundering.

Example 9	Payment for goods/services is mostly in cash, through other forms of value (e.g., cryptocurrency), or via unusual means of payment (e.g., precious metals or stones), making it difficult to trace. **Illustrative Example:** A client engages in cash-intensive business, e.g., dealers in precious metals and stones, and the transactions are disproportionate to his business scale or far exceed the projected activity at the beginning of the relationship. The transactions raise concerns regarding the ultimate source and legitimacy of the funds.
Example 10	Creation of complicated ownership structures, including cross-jurisdictional structures, without legitimate or rational reason. **Illustrative Example:** A client requests to set up an overseas company/trust with a complicated ownership structure. Such an arrangement might be a red flag to obscure the true relationships among the parties involved and may have the effect of disguising beneficial ownership, financial exposure, or the actual flow of funds.
Geographic Risk	
Example 11	Clients or beneficial owners linked to jurisdictions with significant weaknesses in their AML/CTF regimes. **Illustrative Example:** A company operating in Hong Kong was recently sold to an individual residing in Myanmar, a jurisdiction designated as high-risk for ML/TF. The absence of a clear, legitimate connection between the new owner and the company's established business activities raises concerns about the legitimacy and the underlying intent of this acquisition.
Example 12	Clients or beneficial owners transact with entities based in high-risk jurisdictions as determined by the FATF or known to be corporate tax havens. **Illustrative Example:** Receiving funds or sending funds to entities in high-risk jurisdictions when there is no apparent connection between the country and the client, and the client is unable to provide justifiable supporting

	documents for the transaction, raises concerns about the legitimacy of the transactions.
Example 13	The client is paying or receiving unusual consultant fees to/from offshore companies. **Illustrative Example:** During an audit, the client asserted that the cash payments were remuneration for being a consultant on an overseas project, but was unable/evasive in providing proof of the business agreement. Such transactions raise concerns about their legitimacy.
Delivery Channel Risk	
Example 14	Client requests provision of services with no face-to-face interaction. **Illustrative Example:** Client refuses to attend the office of your firm or insists on nominating another representative when being requested for further enquiry/supporting documents. Such refusal of face-to-face interaction raises concerns about the client's true identity or the ultimate beneficiary.

G. Topics to be covered in a suspicious transaction report

The following topics should be covered, where available, at the time of completing the STR:

(i) Reporting Party

- Where it is known that the client has been the subject of a previous STR, or involved in any known investigation of any LEA, include the previous STR reference/LEA reference/search warrant/court order number, etc. (if known) to enable the JFIU to identify the appropriate investigation team

(ii) Individual

- Include all the known personal particulars of the client, including the full legal name, all the known passports/identification documents, addresses, emails, phone numbers, etc.
- Specify the role of the client in the STR (e.g., suspect, transaction counterpart, victim, etc.)

(iii) Company/Organization

- Include registration number, jurisdiction of incorporation, addresses, and related persons, etc.
- Specify the role of the company/organization in the STR

(iv) Account

- Include any known bank account/cryptocurrency wallet details, including the opening and closing date, account balance, and related persons/companies (if known)

(v) Transaction

- Include the period and amount of the suspicious transaction

(vi) Suspected crimes and suspicious indicators

- Check the applicable box(es) of the “suspected crime” type
- Check the applicable box(es) for the “suspicious indicator”

(vii) Narrative about suspicious transactions

- Check the applicable box(es) on “triggering factors” for the suspicion

- Complete information on the background of the client and a summary of the business relationship:

For individuals

  - Full name
  - Date of birth or age
  - Nationality
  - Occupation or employment
  - Income or other relevant information relating to the source of wealth and/or funds
  - Family background, if known (e.g., wife/husband of the client also maintained a business relationship with the firm, or being a politically exposed person)
  - Any other relevant information that relates to net worth

For companies/Organizations

  - Full name and business nature
  - Date and place of incorporation
  - Details of connected parties (e.g., beneficial owners, directors, shareholders)
  - Summary of the known financial situation of the entity

Summary of the business relationship

  - The business nature of the practice/professional firm
  - Anticipated level and nature of the activity to be undertaken through the relationship
  - Purpose and intended nature of the business as stated by the client

Details of investigation/Transaction analysis

  - Specification of reviewing period
  - Financial transactions – When the suspicion relates to a financial transaction, include details of the beneficiary/remitter of funds, bank account details, date and type of transaction (e.g., cheque, cash, etc.), previous transaction pattern (if known, e.g., dormant), and reason for the transactions to be suspicious
  - Services provided – provide details of the services being provided /requested to be provided that triggered the suspicion (e.g. audit, setting up of trust/company, etc.) and include the date and details of the activity and parties involved
  - Identify the suspected benefit from the criminal conduct/suspicious transaction and the estimated amount, where applicable

- Result of CDD enquiry and internal investigation[15] in relation to adverse news from open source or other suspicious activities
- Provision of hyperlinks to the relevant open-source information

Conclusions/Action taken/Way forward

- Provide a summary of the narrative
- Indicate follow-up action to be taken (e.g., further review, report to any competent authority, etc.)

[15] The background and process of the CDD enquiry and internal investigation generally need not be included, unless the information is useful in relation to the basis for suspicion.

H. Other useful resources

(a) Institute's AML webpage

(b) AML Guidelines

(c) JFIU's website on suspicious transaction reports and typologies

(d) Narcotics Division, Security Bureau's website on AML / CTF

(e) FATF's website for international guidance and statements

(f) FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures

(g) FATF Guidance for Risk-Based Approach for the Accounting Profession

Useful references from other jurisdictions:

Australia

(a) AUSTRAC - Suspicious matter reports (Reform)

(b) AUSTRAC - Risk insights and indicators of suspicious activity for accountants

(c) AUSTRAC - Tipping Off

Canada

(a) FINTRAC's compliance guidance - Reporting suspicious transactions to FINTRAC

(b) What to consider when submitting a suspicious transaction report issued by the Government of Canada?

Guernsey

(a) Guidance on Combatting Proliferation and Proliferation Financing

The United Kingdom

(a) UK Financial Intelligence Unit - Suspicious Activity Reports annual report

(b) ICAEW Suspicious Activity Reporting (SAR) Guidance