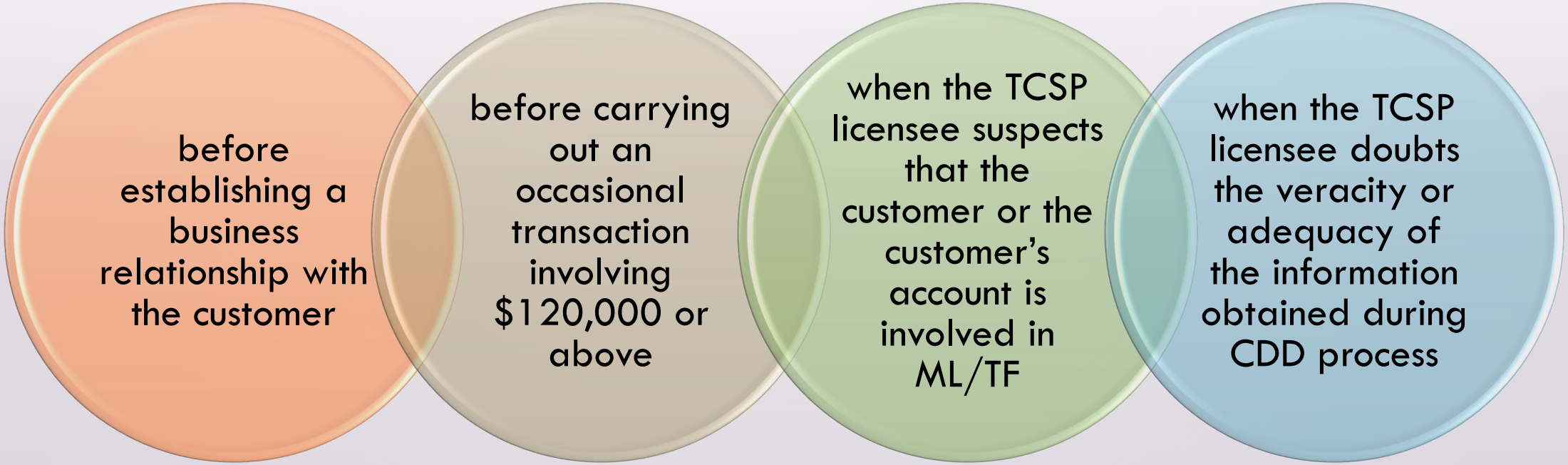
AML/CTF Requirements for TCSPs

Ms. Marie Leung
Senior Solicitor
29 October 2024

When to Carry Out CDD?

Customer due diligence ("CDD") measures must be carried out: *[s.3, Sch. 2]*



If the requirements are not complied with, the licensee **MUST NOT** establish a business relationship or carry out an occasional transaction with that customer. If a business relationship has been established, it must be terminated as soon as reasonably practicable. *[s.3(4), Sch. 2]*

What are CDD Measures?

- identifying the customer and verifying the customer's identity *[s.2(1)(a), Sch. 2]*
- identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity *[s.2(1)(b), Sch. 2]*
- obtaining information on the purpose and intended nature of the business relationship, if a business relationship is to be established *[s.2(1)(c), Sch. 2]*
- identifying the person purporting to act on behalf of the customer and taking reasonable measures to verify the person's identity and verifying the person's authority to act on behalf of the customer *[s.2(1)(d), Sch. 2]*

Appendices of Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for TCSPs ("AML/CTF Guideline")

For identification and verification of customer which is a/an:

- individual – Appendix A
- corporation – Appendix B
- partnership or unincorporated body – Appendix C
- trust – Appendix D

Case Example

Transaction : acting as the company secretary of Company X

- Who is the customer?
- Is the customer a new customer?
- Company X – Appendix B of the AML/CTF Guideline
- Section 4 of Schedule 2 to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("AMLO") – SDD applies?
- Pre-existing customers (business relationship established before 1 March 2018)?
- A person purports to act on behalf of Company X :
  - Identify the person and take reasonable measures to verify the person's identity + verify the authority

Carrying out customer due diligence measures by means of intermediaries

Section 18 of Schedule 2

(1) Subject to subsection (2), a financial institution or a DNFBP may carry out any customer due diligence measure by means of an intermediary specified in subsection (3) if—

(a) the intermediary consents in writing to be the financial institution's or the DNFBP's intermediary; and

(b) the financial institution or the DNFBP is satisfied that the intermediary will on request provide a copy of any document, or a record of any data or information, obtained by the intermediary in the course of carrying out the customer due diligence measure without delay.

(2) A financial institution or a DNFBP that carries out a customer due diligence measure by means of an intermediary remains liable under this Ordinance for a failure to carry out that customer due diligence measure.

Carrying out customer due diligence measures by means of intermediaries (Con't)

(3) The specified intermediary is—

(a) any of the following persons who is able to satisfy the financial institution or the DNFBP that they have adequate procedures in place to prevent money laundering and terrorist financing—

(i) an accounting professional;
(ii) an estate agent;
(iii) a legal professional;
(iv) a TCSP licensee;

(b) a financial institution that is an authorized institution, a licensed corporation, an authorized insurer, a licensed individual insurance agent, licensed insurance agency or licensed insurance broker company;

Carrying out customer due diligence measures by means of intermediaries (Con't)

(c) a lawyer, a notary public, an auditor, a professional accountant, a trust or company service provider or a tax advisor practising in an equivalent jurisdiction, or a trust company carrying on trust business in an equivalent jurisdiction, or a person who carries on in an equivalent jurisdiction a business similar to that carried on by an estate agent, or an institution that carries on in an equivalent jurisdiction a business similar to that carried on by an intermediary financial institution, that—

(i) is required under the law of that jurisdiction to be registered or licensed or is regulated under the law of that jurisdiction;

(ii) has measures in place to ensure compliance with requirements similar to those imposed under this Schedule; and

(iii) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities or the regulatory bodies (as may be applicable); or

(d) in the case of a financial institution, an institution that—

(i) is a related foreign financial institution in relation to the financial institution; and

(ii) satisfies the conditions in subsection (3A).

See FAQ on Customer Due Diligence

Ongoing Due Diligence Requirements

Continuously monitor the business relationship with customer *[s.5, Sch. 2]*

Reviewing from time to time documents, data and information relating to the customer obtained for the purpose of complying with Part 2 of Schedule 2 to ensure they are up-to-date and relevant;

Scrutinizing the transactions of the customer to ensure that they are consistent with the licensee's knowledge of the customer and its business, risk profile and source of funds; and

Identifying transactions that are complex, unusually large or of an unusual pattern and have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out its findings in writing.

Additional Measures or Enhanced Customer Due Diligence ("EDD")

Situations in which additional measures or EDD apply:

the customer is not physically present for identification purposes;

the customer or the beneficial owner of the customer is a politically exposed person ("PEP");

any situation specified by the Registrar of Companies in a notice given to the TCSP licensee and in any situation that by its nature may present a high risk of money laundering or terrorist financing.

- Refer to requirements set out in sections 9, 10 and 15 of Schedule 2 to the AMLO

Politically exposed person

Under Section 1 of Part 1 of Schedule 2 to the AMLO, ***politically exposed person*** means—

(a) an individual who is or has been entrusted with a prominent public function in a place outside ~~the People's Republic of China~~ Hong Kong and— *(Amended 15 of 2022 s. 33)*

(i) includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official; but

(ii) does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i);

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a), or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a);

Politically exposed person (Con't)

Under Section 1 of Part 1 of Schedule 2 to the AMLO, ***former politically exposed person*** means—

(a) an individual who, being a politically exposed person, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong;

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a), or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a). *(Added 15 of 2022 s. 33)*

Politically exposed person (Con't)

Special requirements when customer is politically exposed person under Section 10 of Schedule 2

(3) **Subsections (1) and (2) do not apply** in relation to a customer or a beneficial owner of a customer of a financial institution or a DNFBP if the financial institution or the DNFBP is satisfied that—

(a) the customer or the beneficial owner of the customer is a former politically exposed person; and

(b) the former politically exposed person does not present a high risk of money laundering or terrorist financing based on an appropriate risk assessment. *(Added 15 of 2022 s. 33)*

Politically exposed person (Con't)

Duty to continuously monitor business relationships under section 5 of Schedule 2

(3) If – (b) a customer, or a beneficial owner of a customer, of a financial institution or a DNFBP is known to the financial institution or the DNFBP, from publicly known information or information in the financial institution's or the DNFBP's possession, to be a politically exposed person,

the financial institution or the DNFBP must, in monitoring the business relationship with the customer under this section, take additional measures to compensate for any risk of money laundering or terrorist financing that may be caused by the fact that the customer or beneficial owner is a customer or beneficial owner falling within paragraph (b).

(5) **Subsection (3)(b) does not apply** in relation to a customer, or a beneficial owner of a customer, of a financial institution or a DNFBP if the financial institution or the DNFBP is satisfied that—

(a) the customer or the beneficial owner of the customer is a former politically exposed person; and

(b) the former politically exposed person does not present a high risk of money laundering or terrorist financing based on an appropriate risk assessment. *(Added 15 of 2022 s. 33)*

Customer not physically present for identification purposes

- Special requirements under section 9(1) of Schedule 2 to the AMLO
- Enhanced ongoing monitoring under section 5(3)(a) of Schedule 2 to the AMLO
- See FAQ on Customer Due Diligence

Recognized digital identification system

Special requirements when customer is not physically present for identification purposes under section 9 of Schedule 2

(2) **Subsection (1) does not apply** in relation to a customer of a financial institution or a DNFBP if the financial institution or the DNFBP has carried out the measure referred to in section 2(1)(a) or (ab) of this Schedule in relation to the customer on the basis of data or information provided by a recognized digital identification system. *(Added 15 of 2022 s. 33)*

Recognized digital identification system (Con't)

Duty to continuously monitor business relationships under section 5 of Schedule 2

(3) If - (a) a customer of a financial institution or a DNFBP has not been physically present for identification purposes,
the financial institution or the DNFBP must, in monitoring the business relationship with the customer under this section, take additional measures to compensate for any risk of money laundering or terrorist financing that may be caused by the fact that the customer is a customer falling within paragraph (a).

(4) **Subsection (3)(a) does not apply** in relation to a customer of a financial institution or a DNFBP if the financial institution or the DNFBP has carried out the measure referred to in section 2(1)(a) or (ab) of this Schedule in relation to the customer on the basis of data or information provided by a recognized digital identification system. *(Added 15 of 2022 s. 33)*

Recognized digital identification system (Con't)

Under Section 1 of Part 1 of Schedule 2 to the AMLO, ***recognized digital identification system*** means—

> in relation to a financial institution or a DNFBP who is a TCSP licensee or a Category B PMS registrant, a digital identification system that is a reliable and independent source that is recognized by the relevant authority

FAQ on DIS : The Registrar recognizes iAM Smart, developed and operated by the HKSAR Government, as a digital identification system that can be used for identity verification of natural persons.

Recognized digital identification system (Con't)

Section 2 of Schedule 2

(1) The following measures are customer due diligence measures applicable to a financial institution or a DNFBP—

(a) for a financial institution, or a DNFBP who is a TCSP licensee or a Category B PMS registrant, identifying the customer and verifying the customer's identity on the basis of documents, data or information provided by—

(i) a governmental body;

(ii) the relevant authority or any other relevant authority;

(iii) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority or any other relevant authority;

(iiia) a recognized digital identification system; or *(Added 15 of 2022 s. 33)*

(iv) any other reliable and independent source that is recognized by the relevant authority;

Record-Keeping Requirements

Records to be kept *[s. 20, Sch. 2]*

In relation to a **transaction**

- the original or a copy of the documents, and a record of the data and information should be kept **for at least 5 years after the completion of the transaction**.

In relation to a **customer**

- the original or a copy of the CDD documents, record of the data and information and files relating to the customer's account and business correspondence with the customer and any beneficial owner of the customer should be kept **throughout the continuance of the business relationship with the customer and for a period of at least 5 years after the end of the business relationship**.

Record-Keeping Requirements (Con't)

Duty to keep records under section 20 of Schedule 2

(1) A financial institution or a DNFBP must—

(b) in relation to each customer, keep—

(i) the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of the customer or any beneficial owner of the customer in accordance with Part 2 of this Schedule; and

(ii) the original or a copy of the files relating to the customer's account and business correspondence with the customer and any beneficial owner of the customer.

(3A) Records required to be kept under subsection (1)(b) for an occasional transaction that is carried out in any of the circumstances set out in section 3(1)(b), (1A) and (1B) of this Schedule must be kept for a period of at least 5 years beginning on the date on which the occasional transaction is completed. *(Added 15 of 2022 s. 33)*

Financial Sanction and Counter-Terrorist Financing

- It is an offence under the relevant Regulations of the **United Nations Sanctions Ordinance, Cap. 537** for any person to make economic assets available to or deal with economic assets of individuals or entitles designated by the United Nations Security Council; or those acting on behalf of, or at the direction of, or owned or controlled by such individuals or entities.
- **The United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575 ("UNATMO")** criminalizes the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates.

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

- Section 7 prohibits a person from providing or collecting any property for use to commit terrorist acts.
- Section 8 prohibits a person from making any property or financial (or related) services available to or for the benefit of a person; or collect property or solicit financial (or related) services for the benefit of a person knowing that, or being reckless as to whether, such person is a terrorist or terrorist associate.
- Section 8A prohibits a person from dealing with any property, knowing that, or being reckless as to whether, the property is (a) a specified terrorist property, (b) owned or controlled by a specified terrorist or terrorist associate, or (c) held on behalf of, or at the direction of, a specified terrorist or terrorist associate.

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

- Section 11L prohibits a person from providing or collecting property with the intention or knowing that the property will be used, in whole or in part, to finance the travel of a person between states for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts, or the provision or receiving of terrorist training (whether or not the property is actually so used).
- TCSP licensees are reminded not to have any business relationship with any sanctioned individuals or entities, or any terrorist or terrorist associate as defined under the UNATMO.
- Chapter 8 of the AML/CTF Guideline.

Counter-Financing of Proliferation of Weapons of Mass Destruction ("PF")

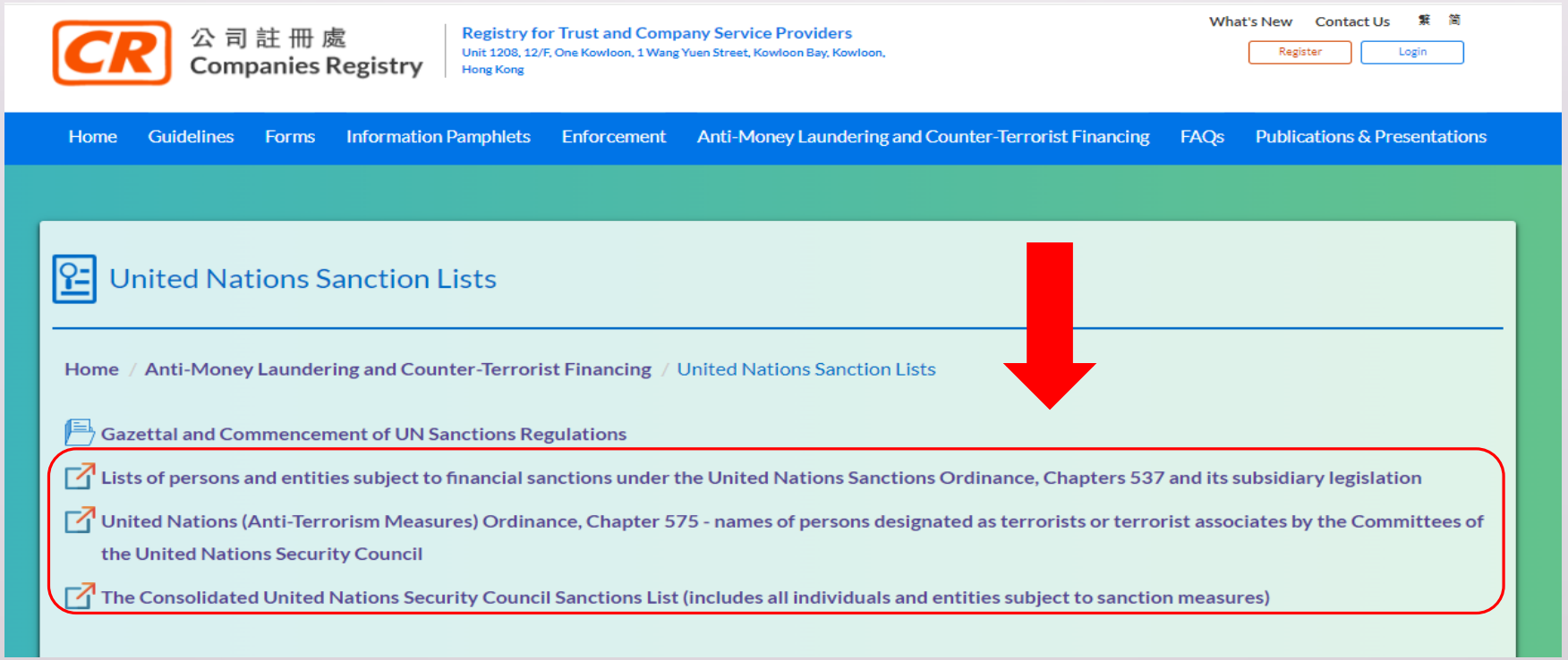
United Nations Sanctions (Democratic People's Republic of Korea) Regulation, Cap. 537AE

Under section 4 of **the Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526**, it is an offence for a person to provide any services where he/she believes or suspects, on reasonable grounds, that those services may be connected to weapon of mass destruction proliferation.

Persons and Entities subject to Sanctions and Terrorists or Terrorist Associates

- TCSP licensees should ensure that they should have an appropriate system to conduct name checks against the relevant list(s) for screening purposes and that the list(s) is/are up-to-date.
- Licensees should conduct screening customers against current lists of terrorist and sanction designations at the establishment of the relationship, and thereafter, as soon as practicable after the new lists of terrorist and sanction designations are published, licensees have to screen their entire client base against the new lists.

- Lists of sanctioned persons and entities and list of names of persons designated as terrorists or terrorist associates specified under the UNATMO are available at the website of the Companies Registry's Trust and Company Service Providers Licensing Regime (www.tcsp.cr.gov.hk).



Reporting Suspicious Transactions

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

Organized and Serious Crimes Ordinance, Cap. 455

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

- In cases of suspicions of money laundering, TF, PF or sanctions violations, report should be made to the Joint Financial Intelligence Unit ("JFIU")
- Chapter 7 of the AML/CTF Guideline
  - TCSP licensees must establish and maintain a record of all ML/TF reports made to the MLRO and all suspicious transaction reports made to the JFIU.

The End