公 司 註 冊 處
COMPANIES REGISTRY

Part 2

Anti-Money Laundering and Counter-Financing of Terrorism Requirements for Licensed Money Lenders

Ms. Yandy LAM
Solicitor
Companies Registry
11 Nov 2025

LEGISLATION AND GUIDELINE

Guideline on Anti-Money Laundering and Counter-Financing of Terrorism ("AML/CFT") (For Licensed Money Lenders) ("AML Guideline")

- Last revised in March 2025
- Promulgated by reference to the requirements set out in Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) ("**AMLO**") *[para. 1.1 of the AML Guideline]*
- Guidance to licensees and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas so as to meet the relevant AML/CFT statutory and regulatory requirements *[para. 1.4 of the AML Guideline]*
- Non-compliance may *cast doubt* on whether the licensee is *fit and proper* to carry on business as a money lender and whether its officers are *fit and proper* to be associated with the business of money-lending *[para. 1.16 of the AML Guideline]*

Other legislation relating to money laundering and terrorist financing ("ML/TF"), financial sanctions and financing of proliferation of weapons of mass destruction

- Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
- Organized and Serious Crimes Ordinance (Cap. 455)
- United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
- United Nations Sanctions Ordinance (Cap. 537)
- Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)

CUSTOMER DUE DILIGENCE (1) – CDD MEASURES

CDD Measures *[para. 4.1.3 of the AML Guideline]*

- identify the customer and verifying the customer's identity
- Identify and take reasonable measures to verify the beneficial owner's identity
- obtain information on the purpose and intended nature of the business relationship (if any) established with the licensee
- if a person purports to act on behalf of the customer: identify the person and take reasonable measures to verify the person's identity and verify the person's authority to act on behalf of the customer

CUSTOMER DUE DILIGENCE (2) - WHEN TO CARRY OUT CDD

When to carry out CDD? *[para. 4.2 of the AML Guideline]*

- before establishing a business relationship with the customer;
- before carrying out an occasional transaction involving HK$120,000 or above;
- when the licensee suspects that the customer or the customer's account is involved in ML/TF; or
- when the licensee doubts the veracity or adequacy of any information previously obtained during the CDD process.

If the requirements are not complied with, the licensee **SHOULD NOT** establish a business relationship or carry out any occasional transaction with that customer. If a business relationship has been established, it should be terminated as soon as reasonably practicable. *[para. 4.13.1 of the AML Guideline]*

CUSTOMER DUE DILIGENCE (3)
– IDENTIFICATION AND VERIFICATION OF IDENTITY - CUSTOMER

For identification and verification of a customer which is a:

- natural person
  – para. 4.3.2 to 4.3.5 (formerly Appendix A) of the AML Guideline
- legal person (including a partnership or an unincorporated body)
  – para. 4.3.6 to 4.3.9 (formerly Appendices B & C) of the AML Guideline
- trust or other similar legal arrangement
  – para. 4.3.10 to 4.3.12 (formerly Appendix D) of the AML Guideline

ADDITIONAL MEASURES / ENHANCED DUE DILIGENCE ("EDD")

Situations in which additional measures / EDD apply include:

- Situations presenting a high ML/TF risk or a situation specified by the Registrar in a notice in writing given to the licensee *[paras. 4.9.1 to 4.9.6]*
- Politically exposed persons (PEPs) *[paras. 4.9.7 to 4.9.27]*
- Customer not physically present for identification purposes *[paras. 4.10.1 to 4.10.5]*

HIGH ML/TF RISKS

A licensee should apply EDD measures in relation to a business relationship or transaction to mitigate and manage the high ML/TF risks in *[para. 4.9.1 of the AML Guideline]*:

(a) a situation that by its nature may present a high ML/TF risk taking into account the potentially higher risk factors set out in paragraph 4.9.5 (see next slide); or

(b) a situation specified by the Registrar in a notice in writing given to the licensee.

EXAMPLES OF POTENTIALLY HIGHER RISK FACTORS

(a) **customer** risk factor:
- (i) business relationship is conducted in unusual circumstances;
- (ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;
- (iii) companies that have nominee shareholders/ directors, bearer shares or bearer share warrants;
- (iv) cash intensive business; or
- (v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex

(b) **product, service, transaction or delivery channel** risk factors:
- (i) anonymous transactions (which may involve cash); or
- (ii) frequent payments received from unknown or unassociated third parties

(c) **country** risk factors:
- (i) countries or jurisdictions not having effective AML/CFT Systems;
- (ii) countries or jurisdictions having a significant level of corruption or other criminal activity;
- (iii) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or
- (iv) countries, jurisdictions or geographical areas providing funding or support for terrorist activities, or that have designated terrorist organisations operation

EXAMPLES OF EDD MEASURES

(a) obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner

(b) obtaining additional information on the intended nature of the business relationship

(c) obtaining information on the source of wealth of the customer

(d) obtaining information on the source of funds of the customer

(e) obtaining information on the reasons for intended or performed transactions

(f) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards

[para. 4.9.6 of the AML Guideline]

ENHANCED CUSTOMER DUE DILIGENCE – POLITICALLY EXPOSED PERSON (1)

Definition 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 Hong Kong and—
  (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).

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).

ENHANCED CUSTOMER DUE DILIGENCE – POLITICALLY EXPOSED PERSON (2)

Definitions of different types of PEPs in the AML Guideline

(a) A non-Hong Kong PEP *[para. 4.9.7 of the AML Guideline]*
(b) A former non-Hong Kong PEP *[para. 4.9.12 of the AML Guideline]*
(c) A Hong Kong PEP *[para. 4.9.14 of the AML Guideline]*
(d) An international organization PEP *[para. 4.9.15 of the AML Guideline]*

EDD Measures for non-Hong Kong PEPs

[see paras. 4.9.10 and 4.9.11 of the AML Guideline]

EDD Measures for Hong Kong PEPs and international organization PEPs

[see para. 4.9.18 of the AML Guideline]

ENHANCED CUSTOMER DUE DILIGENCE – POLITICALLY EXPOSED PERSON (3)

Treatment of former PEPs *[paras. 4.9.13 and 4.9.19 of the AML Guideline]*

- Risk-based approach

- Licensee may **decide NOT TO** apply / continue to apply the **EDD measures** *(*para. 4.9.10 of the AML Guideline) **and enhanced monitoring measures** (para. 4.9.11 of the AML Guideline) to a customer who is / whose beneficial owner is

  - (i) **a former PEP**; and

  - (ii) the former PEP **does not present a high risk of ML/TF** based on appropriate assessment

ADDITIONAL MEASURES – CUSTOMER NOT PHYSICALLY PRESENT FOR IDENTIFICATION PURPOSES

If a customer has not been physically present for identification purposes, at least ONE of the following additional measures must be carried out *[para. 4.10.1 of the AML Guideline]* **:**

- further verifying the customer's identity on the basis of documents, data or information referred to in para. 4.3.1 of the AML Guideline but not previously used for the purposes of verification of the customer's identity;
- taking supplementary measures to verify information relating to the customer that has been obtained by the licensee; or
- ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with an authorized institution, or an institution that (i) is incorporated or established in an equivalent jurisdiction; (ii) carries on a business similar to that carried on by an authorized institution; (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO; and (iv) is supervised for compliance with those requirements by authorities in that jurisdiction that perform functions similar to those of the Hong Kong Monetary Authority.

HOWEVER, if a licensee has verified the identity of the customer on the basis of data or information provided by a digital identification system that is a reliable and independent source that is recognized by the Registrar of Money Lenders (see para. 4.3.1 of the AML Guideline)**, the licensee is not required to carry out any additional measures set out above.** *[para. 4.10.2 of the AML Guideline]*

CARRYING OUT CUSTOMER DUE DILIGENCE MEASURES BY MEANS OF INTERMEDIARIES (1)

A licensee may rely upon an intermediary to perform any part of the CDD measures. **HOWEVER**, the ultimate responsibility for ensuring that CDD requirements are met remains with the licensee *[para. 4.11.1 of the AML Guideline].*

When relying on an intermediary, a licensee should *[para. 4.11.3 of the AML Guideline]*:

(a) obtain written confirmation from the intermediary that the intermediary agrees to act as the licensee's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2 to the AMLO; and

(b) be 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 CDD measures without delay.

CARRYING OUT CUSTOMER DUE DILIGENCE MEASURES BY MEANS OF INTERMEDIARIES (2)

Intermediaries in Hong Kong *[para. 4.11.8 of the AML Guideline]*

A. Financial Institutions

- an authorized institution
- a licensed corporation
- an authorized insurer
- a licensed individual insurance agent
- a licensed insurance agency
- a licensed insurance broker company

B. Professional Intermediaries

(provided that such intermediaries satisfy the licensee that they have adequate procedures in place to prevent ML/TF and are required to comply with the requirements set out in Schedule 2 to the AMLO with respect to customers)

- an accounting professional
- an estate agent
- a legal professional
- a trust or company service provider (TCSP) licensee

ONGOING DUE DILIGENCE REQUIREMENTS (1)

A licensee should continuously monitor the business relationship with a customer in two aspects: *[para. 5.1 of the AML Guideline]*

Ongoing CDD:
reviewing from time to time documents, data and information relating to the customer obtained for the purpose of complying with CDD requirements to ensure they are up-to-date and relevant;

Transaction monitoring:
(i) 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

Transaction monitoring:
(ii) identifying transactions that are complex, unusually large in amount 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.

ONGOING DUE DILIGENCE REQUIREMENTS (2)

Licensees should *[paras. 5.2 and 5.3 of the AML Guideline]*:

- Undertake reviews of existing CDD records of customers on a regular basis and/or upon trigger events

- Develop clear policies and procedures, especially on the frequency of periodic review or what constitutes a trigger event

High ML/TF risk customers should be subject to a minimum of an annual review, or more frequent reviews if deemed necessary, to ensure the CDD information retained remains up-to-date and relevant

TRANSACTION MONITORING

Licensees should:

- establish and maintain adequate systems and processes to monitor transactions *[para. 5.4]*
- regularly review the adequacy and effectiveness of their transaction monitoring systems and processes *[para. 5.8]*
- conduct transaction monitoring following the risk-based approach - the extent of monitoring should be commensurate with the ML/TF risk profile of a customer *[para. 5.9]*
- properly document the findings and outcomes of steps taken, as well as the rationale of any decision made after taking these steps in writing and make them available to the Registrar, other competent authorities and auditors *[para. 5.14]*

RECORD-KEEPING *[CHAPTER 8 OF THE AML GUIDELINE]*

	Each Customer	Each transaction
For how long should records 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. For occasional transaction involving an amount ≥ HK$120,000, **at least 5 years** beginning on the date on which the occasional transaction is completed. *[para. 8.4]*	**At least 5 years** after the completion of a transaction regardless of whether the business relationship ends during the period. *[para. 8.6]*
What records should be kept?	(i) The original or a copy of documents and a record of the data and information obtained: • in the course of **identifying and verifying** the identity of the customer/ beneficial owner of the customer / beneficiary / persons who purport to act for the customer / other connected parties; • throughout the CDD and **ongoing monitoring process**; and • on the **purpose and intended nature** of the business relationship (ii) The original or a copy of records and documents- relating to the customer's **account and business correspondence** with the customer and any beneficial owner of the customer (iii) The results of any analysis undertaken *[para. 8.3]*	The original or a copy of the documents, and a record of the data and information obtained in connection with each transaction the licensee carries out, both domestic and international, which should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity *[para. 8.5]*

COUNTER-FINANCING OF TERRORISM

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** *[para. 6.5 of the AML Guideline]*.

(a) section 6 empowers the Secretary for Security to freeze suspected terrorist property
(b) section 7 prohibits the provision or collection of property for use to commit terrorist acts
(c) section 8 prohibits any person from making available or collecting or soliciting property or financial (or related) services for terrorists and terrorist associates
(d) section 8A prohibits any person from dealing with any property knowing that, or being reckless as to whether, the property is specified terrorist property or property of a specified terrorist or terrorist associate
(e) section 11L prohibits any person from providing or collecting any property, with the intention or knowing that the property will be used, to finance the travel of a person between states for a specified purpose (i.e. the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs); or the provision or receiving of training that is in connection with the perpetration, planning or preparation of, or participation in, one or more terrorist acts (even if no terrorist act actually occurs as a result of the training))

FINANCIAL SANCTIONS

It is an offence under the relevant Regulations of the **United Nations Sanctions Ordinance (Cap. 537)** for any person

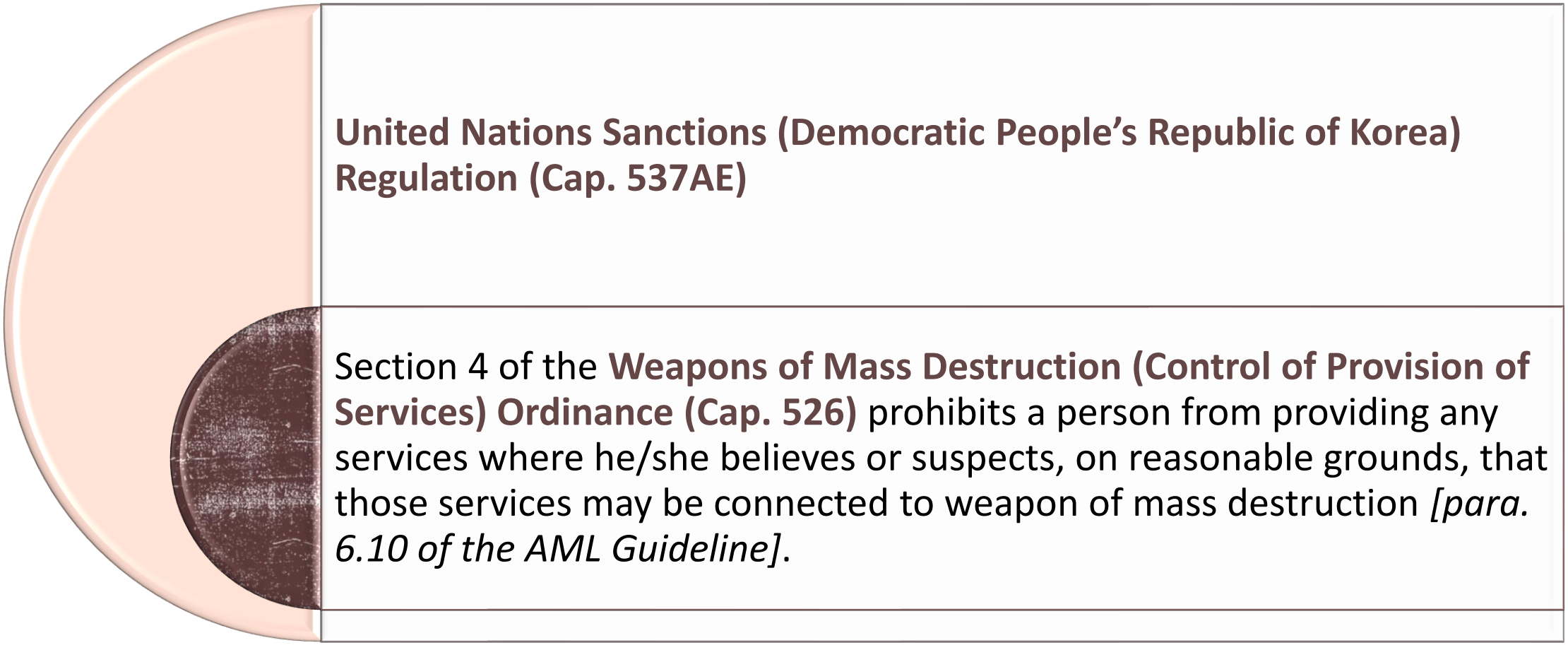
(a) to make available, directly or indirectly, any funds or other financial assets or economic resources to, or for the benefit of,

  (i) designated persons or entities;
  (ii) persons or entities acting on behalf or at the direction of the designated persons or entities mentioned in (i); or
  (iii) entities owned or controlled by any persons or entities mentioned in (i) or (ii); or

(b) to deal with, directly or indirectly, any funds or other financial assets or economic resources belonging to, or owned or controlled by, such persons and entities falling within (a) above. *[para.6.7 of the AML Guideline*]

- 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.

COUNTER-FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION



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

Section 4 of the **Weapons of Mass Destruction (Control of Provision of Services) Ordinance (Cap. 526)** prohibits a person from providing any services where he/she believes or suspects, on reasonable grounds, that those services may be connected to weapon of mass destruction *[para. 6.10 of the AML Guideline]*.

DATABASE MAINTENANCE AND SCREENING (1)

Licensees should establish and maintain effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF *[para.6.12 of the AML Guideline]*.

Licensees should *[para. 6.13 of the AML Guideline]*:

- identify terrorist suspects and possible designated parties, and detect prohibited transactions
- maintain a database of names and particulars of terrorists and designated parties, which consolidates the various lists that have been made known to the licensee
- alternatively, subscribe to such a database maintained by a third party service provider and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database

DATABASE MAINTENANCE AND SCREENING (2)

Licensees should include in the database *[para. 6.15]*:

(i) the lists published in the Gazette or on the website of the Commerce and Economic Development Bureau; and

(ii) the lists that the Registrar draws to the attention of licensees from time to time

DATABASE MAINTENANCE AND SCREENING (3)

Licensees should implement an effective screening mechanism, which should include:

(a) screening its customers and any beneficial owners of the customers against current database at the establishment of the relationship; and
(b) screening its customers and any beneficial owners of the customers against all new and any updated designations to the database as soon as practicable

The screening requirements should extend to connected parties and persons purporting to act on behalf of a customer using a risk-based approach.

[paras. 6.16 and 6.17 of the AML Guideline]

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, terrorist financing, financing of proliferation of weapons of mass destruction or sanctions violations, a suspicious transaction report ("**STR**") should be made to the Joint Financial Intelligence Unit ("**JFIU**") (www.jfiu.gov.hk) *[Chapter 7 of the AML Guideline]*.

TIPPING OFF

It is an offence ("**tipping off**") to reveal to any person any information which might prejudice an investigation; if a customer is told that a report has been made, this would prejudice the investigation and an offence would be committed.

[para. 7.6 of the AML Guideline]

HOWEVER, making enquiries to customers, when conducted properly and in good faith, will not constitute tipping-off. If a licensee reasonably believes that performing the CDD process will tip off the customer, it may stop pursuing the process. The licensee should document the basis for its assessment and file a STR to the JFIU.

[para. 5.13 of the AML Guideline]

STAFF TRAINING

- Ongoing staff training is an important element of an effective system to prevent and detect ML/TF activities. *[para. 9.1 of the AML Guideline]*

Effective implementation of AML/CTF training

Scope and frequency of training should be tailored to the specific risks faced by the licensee and pitched according to the job functions, responsibilities and experience of the staff. *[para. 9.2]*

Licensees should implement a clear and well-articulated policy for ensuring that relevant staff receive adequate AML/CFT training. *[para. 9.3]*

Licensees are encouraged to consider using a mix of training techniques and tools in delivering training, depending on the available resources and learning needs of their staff. *[para. 9.6]*

Licensees should monitor the effectiveness of the training. *[para. 9.8]*

Licensees should maintain records of who have been trained, when the staff received the training and the type of the training provided for a minimum of **3 years**. *[para. 9.7]*

Thank you!

www.cr.gov.hk