



AML/CTF Requirements for TCSPs

Ms. Christy YIU

Senior Solicitor

Companies Registry

20 December 2019

What are CDD Measures?

CDD measures prescribed in Schedule 2 to the AMLO:

- 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 authority [s.2(1)(d), Sch. 2]

When to Carry Out CDD?

CDD measures must be carried out: [s.3, Sch. 2]

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

If CDD 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]

Ongoing Monitoring Requirement

Continuously monitor 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



Enhanced Due Diligence (“EDD”) (1)

High-risk situations for which EDD measures apply include:

- the customer is not physically present for identification purposes
- the customer or the beneficial owner of the customer is a politically exposed person
- any situation specified by the Registrar 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

EDD (2)

Customer not physically present for identification purposes

[s. 9, Sch. 2]

- Further verifying the customer's identity on the basis of documents, data or information not previously used for the purposes of verification of the customer's identity
- Taking supplementary measures to verify information relating to the customer obtained by the licensee; or
- Ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorized institution, or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those in Schedule 2 and is supervised for compliance by a banking regulator in that jurisdiction

EDD (3)

Politically Exposed Persons (“PEPs”) [s. 10, Sch. 2]

- When TCSP licensees know that a customer or its beneficial owner is a PEP, they should, before establishing a business relationship or continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, carry out the following EDD measures:
 - obtain approval from its senior management; and
 - take reasonable measures to establish the customer’s or the beneficial owner’s source of wealth and the source of the funds

EDD (4)

Other high risk situations [s. 15, Sch. 2]

- As set out in the Guideline on Compliance of Money-Laundering and Counter-Terrorist Financing Requirements for Trust or Company Service Providers (“AML/CTF Guideline”):
 - corporate customer having issued bearer shares
 - customer from or transaction connected with higher-risk jurisdictions
 - situation specified by the Registrar of Companies
- Obtain approval from its senior management to establish or continue the business relationship; and
- Either take reasonable measures to establish the customer’s or beneficial owner’s source of wealth and the source of the funds; or take additional measures to mitigate the risk of money laundering or terrorist financing involved

Record-Keeping Requirements (1)

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, obtained in connection with the transaction
- In relation to a **customer**
 - 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; and
 - 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

Record-Keeping Requirements (2)

Duty to keep records [s. 20, Sch. 2]

- In relation to a **transaction**
 - records should be kept **for at least 5 years after the completion of the transaction**
- In relation to a **customer**
 - records 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**

Financial Sanction

The United Nations Sanctions Ordinance, Cap. 537 (“UNSO”)

- The Chief Executive may specify persons or entities designated by the Security Council of the United Nations or its Sanctions Committees for the purpose of financial sanctions, as “relevant persons” or “relevant entities”
- It is an offence for any person to make available any funds or other financial assets or economic resources to or for the benefit of relevant persons or relevant entities; or to deal with any funds, other financial assets or economic resources belonging to, owned or controlled by, such persons or entities

Counter-Terrorist Financing

- Terrorist financing (“TF”) is the financing of terrorist acts, and of terrorists and terrorist organizations
- **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
- Chapter 8 of the AML/CTF Guideline

Persons and Entities subject to Sanctions and Terrorists or Terrorist Associates

- TCSP licensees are reminded not to have any business relationship with any relevant person or relevant entity, as defined under the UNSO or any of its subsidiary legislation, which is subject to financial sanctions, or any terrorist or terrorist associate as defined under the UNATMO
- Lists of persons and entities subject to financial sanctions under the UNSO and list of names of persons designated as terrorists or terrorist associates specified under the UNATMO are available at the website of the CR's Trust and Company Service Providers Licensing Regime (www.tcsp.cr.gov.hk)

Counter-Financing of Proliferation of Weapons of Mass Destruction (“PF”)

- **The United Nations Sanctions (Democratic People’s Republic of Korea) Regulation, Cap. 537AE**
- **The United Nations Sanctions (Joint Comprehensive Plan of Action—Iran) Regulation, Cap. 537BV**
- 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

Reporting Suspicious Transactions

- Offences under:
 - **The Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405**
 - **The Organized and Serious Crimes Ordinance, Cap. 455**
 - **The 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**
- Chapter 7 of the AML/CTF Guideline



The End

