Charltons - Hong Kong Law Newsletter - 02 May 2012

[online version](http://www.charltonslaw.com/new-anti-money-laundering-and-counter-terrorist-financing-requirements-for-sfc-licensed-corporations/)

# New Anti-Money Laundering And Counter-Terrorist Financing Requirements For SFC Licensed Corporations Effective 1 April 2012

## Introduction

New statutory customer due diligence (**CDD**) and record-keeping obligations for financial institutions were implemented by the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615) (the **AMLO**) which came into effect on 1 April 2012. The AMLO was enacted to better align Hong Kong’s anti-money laundering (**AML**) and counter-terrorist financing (**CTF**) regimes for financial institutions with international standards as recommended by the Financial Action Task Force (**FATF**). The AMLO provides a uniform set of requirements for financial institutions (**FI**s) in the banking, securities, insurance and remittance and money changing sectors.

## The AMLO

The key features of the AMLO include the following:

1. It gives supervisory and enforcement powers to four regulatory authorities (**RA**s), the Securities and Futures Commission (**SFC**), the Hong Kong Monetary Authority (**HKMA**), the Insurance Authority (**IA**) and the Customs and Excise Department (**CED**).
2. It codifies into statutory obligations the CDD and record-keeping obligations of FIs which are set out in Schedule 2 to the AMLO (**Schedule 2**). These obligations largely reflect those previously provided for in administrative guidelines issued by the SFC, the HKMA and IA, respectively.
3. It provides for supervisory and criminal sanctions for non-compliance with the statutory requirements. Supervisory sanctions can include orders for remedial actions, public reprimands and fines. Criminal liability will be incurred if an FI contravenes certain specified statutory obligations (the **Specified Provisions** as set out in section 5(11) AMLO) knowingly or with an intent to defraud. Persons concerned in the management of an FI and employees of an FI may be criminally liable if they knowingly or with an intent to defraud cause or permit the FI to contravene a Specified Provision.
4. It puts in place a licensing regime and anti-money laundering framework for remittance agents and money changers.

## Guidelines On Compliance

The four RAs published the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (the **AML/CTF Guideline**) in January 2012 to provide generic guidance on compliance with the Schedule 2 obligations that is applicable to all FIs.

Each of the four RAs has a slightly modified version of the AML/CTF Guideline that provides guidance specific to their respective sectors (presented in italics) in addition to the generic guidance applicable to all sectors. The SFC has published an additional guideline, the Prevention of Money Laundering and Terrorist Financing Guideline for Associated Entities (the **AE Guideline**) to provide guidance for associated entities (**AE**s), as defined in the Securities and Futures Ordinance (**SFO**). The AML/CTF Guideline applies to licensed corporations (**LC**s) but not to AEs, who are not required to comply with the AMLO. The AML/CTF Guideline and the AE Guideline replace the previous Prevention on Money Laundering and Terrorist Financing Guidance Note (the **AMLGN**). The AML/CTF Guideline and the AE Guideline took effect on 1 April 2012 to coincide with the AMLO coming into force.

This note contains a summary of some of the key issues arising from the AML/CTF Guideline and the AE Guideline.

The AML/CTF Guideline can be found on the website of the Hong Kong Government Logistics Department at the following locations:

[SFC version](http://www.gld.gov.hk/egazette/pdf/20121604/egn20121604410.pdf)

[HKMA version](http://www.gld.gov.hk/egazette/pdf/20121604/egn20121604408-1.pdf)

[IA version](http://www.gld.gov.hk/egazette/pdf/20121604/egn20121604409.pdf)

[CED version](http://www.gld.gov.hk/egazette/pdf/20121604/egn20121604409.pdf)

## Outline Of The AML/CTF Guideline

In summary, the AML/CTF Guideline covers the following principal areas:

* AML/CTF systems and business conducted outside Hong Kong
* Risk-based approach
* Customer due diligence
* On-going monitoring
* Financial sanctions and terrorist financing
* Suspicious transaction reports
* Record keeping
* Staff training
* Wire transfers

## AML/CTF Systems (Chapter 2)

The AMLO requires FIs to take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of money laundering (**ML**) and terrorist financing (**TF**) and to prevent a contravention of any CDD or record-keeping requirement of Parts 2 and 3 of Schedule 2 to the AMLO (section 23 AMLO).

The AML/CTF Guideline acknowledges that no system of policies, procedures and controls will prevent all money-laundering or terrorist-financing activities, but recommends that firms should implement adequate and appropriate AML and CTF systems taking into consideration:

* products or services that are vulnerable to money-laundering or terrorist-financing abuse;
* risks involving delivery and distribution channels, such as the use of intermediaries;
* situations where the customer can divest ownership of property while still controlling it;
* business or industrial sectors vulnerable to corruption and to which a customer is connected;
* transactions that may themselves be of a criminal nature; and
* countries or locations of operation to which customers or intermediaries are connected and are subject to increased risk of organised crime or corruption.

FIs are required to have effective controls covering oversight from senior management, the appointment of a compliance officer and money-laundering reporting officer, a compliance and audit function and staff screening and training. The compliance officer is the person within the FI responsible for oversight of activities relating to the prevention and detection of money laundering and terrorist financing. The money-laundering reporting officer is required to play an active role in the identification and reporting of suspicious transactions.

## Business Conducted Outside Hong Kong

The AMLO requires a Hong Kong-incorporated FI with overseas branches or subsidiary undertakings to put in place a group AML/CTF policy to ensure that branches and subsidiary undertakings that carry on the same business as the FI outside Hong Kong have in place procedures to comply with CDD and record- keeping requirements similar to those imposed by Parts 2 and 3 of Schedule 2 (section 22 of Schedule 2). If a branch or subsidiary undertaking is prevented by local laws from complying with Parts 2 and 3 of Schedule 2, the AMLO requires the FI to inform the RA and to take to additional measures to effectively mitigate the risks of money-laundering and terrorist-financing faced by the branch or subsidiary undertaking concerned. These obligations are replicated in the AML/CTF Guideline.

If there is property suspected to be the proceeds of money-laundering or terrorist-financing activities, the authorities in the relevant jurisdiction should normally be informed. If the property belongs to an account domiciled in Hong Kong, and if the suspected activity would be a criminal offence in Hong Kong, the Joint Financial Intelligence Unit (JFIU) in Hong Kong should be informed as well.

## Risk Based Approach (Chapter 3)

The AML/CTF Guideline recommends a risk-based approach to CDD and on-going monitoring as an effective way to combat ML and TF. According to this approach, FIs should take enhanced measures to manage and mitigate risks in the case of customers assessed to present higher risks of money laundering or terrorist financing. Conversely, simplified measures may be adopted for customers assessed to present lower risks. The AML/CTF Guideline suggests identifying and categorizing the money-laundering and terrorist financing risks at the customer level and establishing reasonable measures based on the risks identified.

The risk factors the AML/CTF Guideline suggests FIs take into account are:

1. Country risk – i.e. customers resident in or connected with high-risk jurisdictions such as:
	* Those identified by the FATF as having strategic AML/CTF deficiencies;
	* Countries subject to sanctions or embargos;
	* Countries that are vulnerable to corruption; and
	* Countries believed to have strong links to terrorist activities;
2. Customer risk – i.e. customers presenting a higher risk due to their nature or behaviour. Relevant factors might include:
	* The complexity of the relationship, including the use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial reason;
	* Where the origin of wealth (for high risk customers and politically exposed persons (**PEP**s)) or ownership cannot be easily verified; and
	* A request to use numbered accounts or undue levels of secrecy.
3. Product/service risk – factors indicating a higher risk might include:
	* Services that inherently provide greater anonymity; and
	* The ability to pool underlying customers or funds.
4. Delivery/distribution channel risk - examples include:
	* Sales through online, postal or telephone channels where a non-face-to-face account opening procedure is used; and
	* Business sold through intermediaries.

FIs are required to review regularly their risk assessment policies and procedures. They must also keep records and relevant documents of risk assessments conducted.

## Customer Due Diligence (Chapter 4)

The AMLO (section 2 of Schedule 2) and the AML/CTF Guideline (paragraph 4.1.3) set out what CDD measures are and the circumstances in which FIs must conduct CDD. The AML/CTF Guideline provides detailed guidance on the following:

1. The identification and verification of the customer, a beneficial owner and a person purporting to act on behalf of the customer;
2. Understanding the purpose and nature of the business relationship;
3. The timing of identification and verification of identity;
4. Keeping customer information up-to-date;
5. The CDD measures that are appropriate for different types of customers including natural persons, corporations, partnerships, unincorporated bodies and trusts;
6. The types of customers to whom simplified due diligence may be applied;
7. The situations in which additional measures to mitigate the risk of ML/TF or enhanced due diligence should be taken and particular obligations in relation to customers who are not physically present for identification purposes and politically exposed persons;
8. Jurisdictions that do not or insufficiently apply the FATF recommendations or otherwise pose higher risk;
9. Reliance on CDD performed by intermediaries; and
10. The situations in which FIs must perform the CDD measures set out in Schedule 2 and the AML/CTF Guideline to customers with whom the business relationship was established before 1 April 2012.

### Identity of Directors

For corporate customers, FIs are required to identify and record the names of each of its directors and verify the identity of those directors on a risk-based approach.

### Company Registry Search

The CDD requirements for a corporate customer include: (i) confirming that the company is registered and has not been dissolved, wound up, suspended or struck off; (ii) independently identifying and verifying the names of the directors and shareholders recorded in the company registry in the place of its incorporation; and (iii) verifying the address of its registered office in its place of incorporation (paragraph 4.9.10 AML/CTF Guideline).

FIs are required to verify the above information by performing a search at the Hong Kong Company Registry and obtaining a full company search report in respect of all non-listed Hong Kong incorporated companies. Alternatively, the FI may obtain a certified true copy of a company search report certified by the Company Registry or a professional third party. The company search report must have been issued within the previous six months.

For companies incorporated in other jurisdictions that maintain public company registries, the relevant information should be verified by a similar company search enquiry of the relevant registry and a company search report should be obtained. The FI may, as in the case of a Hong Kong incorporated company, obtain a copy of a company search report issued within the previous six months which is certified by a company registry or professional third party. A certificate of incumbency (or equivalent) can be obtained instead if there is no public company registry in the jurisdiction of the company’s incorporation or a certified true copy of a certificate of incumbency issued within the previous six months which is certified by a professional third party. As a third option, a document comparable to a company search report or certificate of incumbency certified by a professional third party in the relevant jurisdiction and verifying that the required information is correct and accurate may be accepted by an FI.

The company search requirement does not apply to any customer eligible for simplified due diligence under section 4(3) of Schedule 2 to the AMLO.

The company search requirement is one of the principal differences between the AML/CTF Guideline and the AMLGN which it replaces. Under the AMLGN, a company search was required only for higher risk categories of customers or where there was doubt as to the identity of a corporate customer’s beneficial owners, shareholders, directors etc.

### Persons Purporting to Act on Behalf of a Customer

Section 2(1)(d) of Schedule 2 to the AMLO requires FIs to identify all persons purporting to act on behalf of customers, take reasonable steps to verify their identities and verify their authority to act on behalf of customers. The AML/CTF Guideline provides that as a general rule, FIs should identify and verify the identity of persons who are authorised to give instructions for moving a customer’s funds or assets. Appendix A to the AML/CTF Guideline sets out further methods that would be considered reasonable for verifying the identity of a person purporting to act on behalf of a customer (paragraph 4.4.2 AML/CTF Guideline).

The AML/CTF Guideline allows FIs to adopt a streamlined approach in verifying the identities of account signatories based on its risk assessment of the customer. For example, in lower risk situations where the FI faces difficulties in verifying signatories of customers that have long lists of account signatories, the provision of a signatory list, recording the names of the account signatories whose identities and authorities to act have been confirmed by a department or person of the customer which is independent to the persons whose identities are being verified, may be sufficient to demonstrate compliance with the requirement to verify the identity of persons purporting to act on behalf of the customer. Non-exhaustive examples of customers for which the streamlined approach could be followed include financial institutions and listed companies.

As regards verification of a person’s authority to act, FIs are required to obtain written authority, which in the case of a corporate customer should be the board resolution or similar written authority.

### Nominee Companies

Section 4(3) of Schedule 2 to the AMLO allows the application of simplified due diligence for customers that are also FIs such that an FI is not required to identify and verify the beneficial owners of other FIs. In the fund distribution business, the fund distributor often opens an account with a fund house (another FI) in the name of a nominee company to hold fund units for customers of the fund distributor. This could potentially result in the nominee company (rather than the fund distributor) being regarded as the customer of the fund house. The nominee company, not being an FI, would not be eligible for the application of simplified due diligence.

Paragraph 4.10.6 therefore provides that, subject to certain safeguards, the fund distributor (and not the nominee company) will be recognised as the customer of the fund house in such cases. The safeguards that apply are that the fund distributor must: (i) be an FI as defined in the AMLO; (ii) have conducted CDD on the underlying customers of the fund; and (iii) be authorised to operate the account which is in the name of the nominee company pursuant to a contractual document or agreement.

### Investment Vehicles

Similarly, where an FI providing fund management or custodian services to an investment vehicle opens and operates an account in the name of the investment vehicle with another FI, the FI providing the services (and not the investment vehicle) will be regarded as the customer of the other FI. Accordingly, the FI may apply simplified due diligence procedures. This treatment is subject to requirements that: (i) the underlying investors must have no control over the management of the investment vehicle’s assets; (ii) the service provider must have conducted CDD on the investment vehicle pursuant to the AMLO; and (iii) the service provider must be authorised to operate the account which is in the name of the investment vehicle pursuant to a contractual document or agreement.

### Detecting and Reporting Suspicious Activities

The AMLO requires FIs to continuously monitor their relationships with customers (section 5 of Schedule 2). This includes ensuring that customer information is up-to-date, monitoring the customer’s activities and transactions to see if they are consistent with the nature of its business, risk profile and source of funds and identifying large, complex or unusual transactions. The ability to detect and monitor suspicious activities is a part of the fitness and properness of the management of an FI.

When monitoring a transaction or a series of transactions, firms should take note of:

* the nature, type and amount involved;
* the destination and origin of the payment or receipt; and
* the customer’s normal activity or turnover.

When monitoring its relationships with customers, firms should take note of;

* new products or services the customer offers which may pose higher risk of money-laundering or terrorist-financing;
* new corporate or trust structures the customer creates; and
* changes in the customer’s stated business activity or increases in its turnover.

Significant changes in customer relationships warrant further customer due diligence to be performed.

### Risk-based Approach

In a risk-based approach, monitoring activities are proportional to the risk profile of a customer. For example, politically-exposed persons would have a higher risk profile. Firms should ensure that the procedures and management information systems are in place to provide its staff with timely information needed to perform further due diligence on high-risk customers.

FIs should take the following into account in their monitoring procedures:

* the size and complexity of the firm’s business;
* the risks of money-laundering and terrorist-financing activities involved in its business;
* the firm’s systems and controls;
* the monitoring procedures already in place; and
* the firm’s products and services.

When investigating large, complex or unusual customer transactions, firms should document any questions they ask the customer and the customer’s responses. Such questions do not constitute tipping off the customer that their activities are under investigation and therefore do not constitute a criminal offence. Nevertheless, firms should be careful not to tip off the customer in their questioning. Suspicious transactions should be reported to the JFIU.

## Suspicious Transaction Reports (Chapter 7)

Under Section 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance (CAP 405) and the Organized and Serious Crimes Ordinance (CAP 455), it is an offence to fail to disclose knowledge or suspicion that property represents proceeds of drug trafficking or an indictable offence. Under Section 12 of the United Nations (Anti-Terrorism Measures) Ordinance (CAP 575), it is an offence to fail to disclose knowledge or suspicion of terrorist property.

By reporting its knowledge or suspicion of property that may be involved in the above activities, firms can obtain a statutory defence against the abovementioned offences. These reports must be filed before the firm undertakes the reported transactions and any relevant transactions must be undertaken only with the consent of the JFIU. If the report is filed after the firm has undertaken the reported transactions, it must be filed on the firm’s own initiative as soon as reasonably possible. Reports should be filed in a standard form or through the use of the e-channel “STREAMS”. Firms should visit [the website of the JFIU](http://www.jfiu.gov.hk/en/) for details.

Firms should be aware that:

* it is an offence to tip off any person with any information that may jeopardise an investigation;
* informing a customer that a suspicious transaction report has been filed would constitute tipping off the customer, which is an offence;
* if there is suspicion of money-laundering or terrorist-financing activities, disclosure should be made as soon as reasonably practical even where no transaction has been conducted;
* internal controls must be in place to prevent directors, officers or employees from tipping off a customer that is the subject of a suspicious transaction report.

Employees should be given sufficient guidance to enable them to recognise possible money-laundering or terrorist-financing activities. An employee that has reported suspicion of any such activities using the procedures established by the firm for such disclosures has satisfied his statutory obligation fully.

### Internal Reporting

FIs should appoint a Money Laundering Reporting Officer (**MLRO**) to handle employee reports of suspicious transactions. The MLRO must consider all internal disclosures he receives in the light of full access to all relevant documentation and parties. This officer is also responsible for checking that the FI has policies and procedures in place to ensure compliance with the legal and regulatory requirements involved in reporting suspicious transactions. The AML/CTF Guideline states that the MLRO should also play an active role in identifying and reporting suspicious transactions, including the review of exception reports or large or irregular transaction reports in addition to ad hoc reports from staff members.

All staff should be made aware of the identity and role of the MLRO, the procedures involved in making an internal report and the need for such reports to reach that officer as soon as practicable. While staff are allowed to consult with supervisors or managers before submitting a report to the MLRO, internal reports must not be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/compliance function. The MLRO must acknowledge receipt of every report and remind the reporting employee of the obligation not to tip off the customer under suspicion. All reports to the MLRO and all reports to the JFIU must be recorded and documented.

## Record-Keeping Requirements (Chapter 8)

The AMLO requires FIs to keep the following documents and records throughout the business relationship with the customer and for six years after the business relationship with the customer has ended:

* the original or a copy of the documents, and a record of the information, obtained in the course of identifying and verifying the identity of the customer, beneficial owner of the customer, beneficiary, person purporting to act on behalf of the customer and other parties connected to the customer;
* any additional information on the customer or its beneficial owner that may be obtained for the purposes of enhanced due diligence or ongoing monitoring;
* the original or a copy of the documents, and a record of the data and information, on the purpose and intended nature of the business relationship with the customer; and
* the original or a copy of the documents in relation to the customer’s account (such as their account opening form and risk assessment form) and any correspondence involving the customer or its beneficial owner (sections 20(1) and 23 of Schedule 2 to the AMLO).

FIs must also keep documents, and a record of information obtained, in connection with transactions carried out by a customer for six years after completion of the relevant transaction, regardless of whether the business relationship ends during that period (section 20 of Schedule 2 to the AMLO). These should include:

* the identity of the parties to the transaction;
* the nature and date of the transaction;
* the type and amount of currency involved in the transaction;
* the origin, destination and form (e.g. cash, cheques) of the funds involved;
* the form of instruction and authority; and
* the type and identification number of any account involved in the transaction.

In any event, FIs must ensure that the records retained are sufficient to permit reconstruction of individual transactions so as to provide evidence for prosecution of criminal activity, if necessary.

An RA may in certain circumstances require an FI to keep records relating to a specified transaction or customer for a period longer than six years by notice in writing.

Where an FI relies on an intermediary to carry out CDD measures, the FI remains responsible for compliance with the record-keeping requirements of the AMLO and the AML/CTF Guideline. FIs should ensure that the intermediary has systems in place to comply with those requirements. The FI must obtain immediately the information (but not the documents) obtained by the intermediary in carrying out a CDD measure. FIs must also ensure that the intermediary will, if requested by the FI, provide a copy of any document or record obtained as soon as reasonably practicable. If the intermediary’s services are terminated, it is required to pass to the FI all documents and records retained by it.

## Staff Training (Chapter 9)

Under Chapter 9 of the AML/CTF Guideline, FIs are required to put in place a clear policy for ensuring adequate training for their staff in the areas of anti-money laundering and counter-terrorist financing. The policy should be designed according to the individual needs of each FI, but should include training on statutory obligations (including those under the AMLO). Paragraph 9.9 of the AML/CTF Guideline requires staff training records to be maintained and kept for a minimum of three years, in line with the SFC’s Guidelines on Continuous Professional Training. FIs are also required to monitor the effectiveness of staff training.

## Wire Transfers (Chapter 10)

Section 12 of Schedule 2 to the AMLO sets out special requirements that are applicable to wire transfers, which are defined as “…transaction(s) carried out by an institution…on behalf of a person by electronic means with a view to making an amount of money available to that person or another person…at an institution…”.

Chapter 10 of the AML/CTF Guideline applies primarily to authorised institutions and money service operators. Other FIs are also required to comply with the requirements for wire transfers if they act as an ordering institution or beneficiary institution as defined in the AMLO. In most cases, the provisions of the AMLO and the AML/CTF in relation to special requirements for wire transfers are not applicable to corporations licensed by the SFC, as licensed corporations are usually the originators or recipients/beneficiaries in a wire transfer.

## AE Guidelines

Under the AE Guideline, AEs that are not authorised financial institutions are expected to follow the AML/CTF Guideline issued by the SFC as if they were licensed corporations. Those that are authorised financial institutions should follow the AML/CTF Guideline issued by the HKMA and also paragraphs 7.39 and 7.40 of the one issued by the SFC. These two paragraphs provide guidance to identifying suspicious transactions that involve businesses that deal in securities, futures and leveraged foreign exchange.

AEs that depart from the guidance of the AE Guideline must document their reasons for doing so. Departing from the AE Guideline may reflect upon the fitness and properness of the AE, but does not impose any legal liability of itself. However, such departure is admissible as evidence before any court in any proceedings under the SFO.

**This newsletter is for information purposes only.**

Its contents do not constitute legal advice and it should not be regarded as a substitute for detailed advice in individual cases.

Transmission of this information is not intended to create and receipt does not constitute a lawyer-client relationship between Charltons and the user or browser.

Charltons is not responsible for any third party content which can be accessed through the website.

If you do not wish to receive this newsletter please let us know by emailing us at unsubscribe@charltonslaw.com

**Charltons - Hong Kong Law Newsletter - Issue 153 - 02 May 2012**