Anti-Money Laundering Awareness Training

Insurance Industry
Hong Kong
Anti-Money Laundering Awareness Training Overview

This program is intended to give individuals working in the Hong Kong Insurance Industry a basic knowledge of money laundering and terrorism financing, how these threats impact society and the financial system, and the anti-money laundering measures that have been implemented in Hong Kong to control them.

The training is presented in four sections or knowledge blocks, followed by an assessment. Each knowledge block should take about ten minutes to complete and the total course should be completed in 50 minutes. The knowledge blocks are:

- Introduction to Money Laundering – Basic Concepts
- Anti-Money Laundering Law and Regulation in Hong Kong
- Customer Due Diligence/Know Your Customer
- Reporting Suspicious Transactions
Anti-Money Laundering Awareness Training Overview - Navigation

- To advance to the next screen, click on the **next/forward** button.
- To return to the previous screen, click on the **back** button.
- To return to the beginning of the knowledge block, click on the **return** button.
- To turn off the sound for the presentation, click on the **speaker** button.
- For help with definitions or terminology, click on the **help** button.
- Clicking on these icons will produce a pop-up screen with additional information.
Money laundering has been called the “Crime of the 21st Century,” and it is an essential part of all trans-national and organized criminal activity. Those criminals who want to keep the proceeds of their illegal activities must try to conceal or disguise the source, ownership, or control of those proceeds. They must launder their money.

Many money laundering schemes involve the conversion of cash into other assets – bank deposits, financial instruments, property such as cars or jewelry, or real property. This process of conversion and the concealment of the true ownership or control of the asset may require multiple financial transactions and the use of banks, businesses, and associates to complete.
Introduction to Money Laundering – Basic Concepts

Because criminals must use financial institutions, including providers of insurance products as part of money laundering schemes, governments around the world have attacked the problem of money laundering and terrorism financing by regulating industries that are vulnerable to exploitation by money launderers.

These regulatory controls include requiring financial institutions to conduct due diligence in their relationship with their customers or clients – to Know Your Customer – and to be able to identify signs of money laundering or terrorism financing within the account.
Basic Concepts – The Money Laundering Process

The process of money laundering is sometimes referred to as a cycle consisting of three stages, placement, layering, and integration. Remember that while this process frequently involves large amounts of currency, it applies to non-cash laundering schemes as well.
Basic Concepts - Placement

Placement is the initial stage of the money laundering cycle and it could also be considered a conversion phase, as the purpose is to change the form of the illicit funds or to move them away from the criminal activity.

Many money laundering schemes involve the placement of large amounts of cash, and the conversion of this cash into some other form. This may include bank deposits, the purchase of financial instruments, or the use of wire transfers.

In the insurance industry, cash may be used to pay and settle premiums and may be an indicator of money laundering activity.
Basic Concepts - Layering

**Layering** is the second stage of the cycle, and is designed to distance the funds or assets from the criminal activity. Layering schemes use nominees to hold assets in names other than the criminal’s, businesses or legal persons to hold property or conduct transactions. Bank accounts are used to conduct multiple transactions that conceal the source or origin of funds. Criminals may also move funds offshore, where laws protect records from disclosure.

Insurance products can be used as layers when the customer/policyholder involves third parties, ceding rights to a claim or requesting payment to a person not naturally associated with a claim.
Basic Concepts – Integration

In the Integration stage, the criminal finally has full use of the illegal proceeds, which appear to come from a legitimate or legal source. The purpose of the Integration stage is to provide that explanation. Some integration schemes are designed to show that the money was the proceeds of a loan or the sale of property. Others show that the money is the revenue from a legitimate business.

Insurance products can be used in this stage by launderers who are attempting to show that the funds are from a legitimate insurance claim or a payment from an investment-type insurance product.
Basic Concepts – Regulatory Control

The government of Hong Kong has joined other nations, the United Nations, and international bodies in passing uniform legislation and implementing other regulatory measures to control money laundering and terrorism financing.

Hong Kong is a member of international bodies such as the Financial Action Task Force (FATF) and the Asia/Pacific Group on Money Laundering (APG) that create recommendations for legislation and other preventive measures to combat money laundering. These recommendations form the basis for Guidance from the Office of the Commissioner of Insurance and the Joint Financial Intelligence Unit.
Knowledge Block 1 - Introduction to Money Laundering – Basic Concepts is Complete

You have completed the first knowledge block and can continue to the next section by pressing the Next button.

If you would like to go back and review the content in this knowledge block, press the return button.
Anti-Money Laundering Law and Regulation in Hong Kong

Hong Kong has several laws which address money laundering and which can be applied to cases of money laundering or terrorism financing. In addition to the statutes, there are regulations covering the individual industries that are considered “financial institutions” and are at risk for exploitation by money launderers.

The laws that apply to authorized insurers, reinsurers, appointed insurance agents, and insurance brokers are:

- Section 7 of the Anti-Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance, Cap. 615 (the AMLO)
- Section 4A of the Insurance Companies Ordinance, Cap. 41 (the ICO)
- Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP)
- Organized and Serious Crimes Ordinance (OSCO)
- United Nations (Anti-Terrorism Measures) Ordinance (UNATMO)
The Insurance Authority of Hong Kong and the Joint Financial Intelligence Unit provide guidance to authorized insurers, reinsurers, appointed insurance agents, and insurance brokers that are expected to understand and comply with the provisions of the applicable Anti-Money Laundering laws. These are:

- Section 7 of the Anti-Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance, Cap. 615 (the AMLO)
- Section 4A of the Insurance Companies Ordinance, Cap. 41 (the ICO)
The AMLO imposes Customer Due Diligence and record-keeping requirements on insurance companies and other financial institutions, and gives the Insurance Authority the power to regulate the insurance industry in Hong Kong with respect to AML policies. Criminal violations of the AMLO carry penalties of 2 to 7 years in prison and fines of up to $1 million. Penalties against the insurance company can include fines of up to $10 million or 3 times the amount of profit gained or costs avoided, whichever is greater.
Anti-Money Laundering Law and Regulation in Hong Kong - DTROP

The Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP) does not specifically apply to insurance companies, but does provide for investigation of assets related to drug trafficking. This includes the freezing of assets on arrest and the confiscation of assets upon conviction, which may include insurance products acquired as part of a criminal scheme.
The Organized and Serious Crimes Ordinance (OSCO) also does not specifically relate to insurance companies but does give the police and customs authorities power to investigate organized crime and Triad activity which may seek to use insurance companies or insurance products as vehicles for money laundering.

The OSCO creates an offence of money laundering in relation to indictable organized crime charge. Courts can confiscate the proceeds of organized and serious crime and issue restraint orders against property of persons charged with organized crime offences. This could include insurance products.
The United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) is directed at preventing the financing of terrorism and implements the special recommendations of the Financial Action Task Force. UNATMO permits terrorist property to be frozen and subsequently forfeited, and criminal violations carry a penalty of 14 years in prison and a fine.
The additional provisions against “tipping off” or notifying an individual of a disclosure (filing of an STR), and failing to disclose knowledge that assets or property are the proceeds of crime, both carry 3-year prison terms. Regulatory measures, such as requiring Customer Due Diligence, monitoring, and the reporting of suspicious transactions, add to the effectiveness of the AML program.

This block has explained what Hong Kong’s anti-money laundering laws and regulations are. The next block will describe what the laws and rules require, and how a “financial institution” such as an insurance provider can be in compliance with these measures.
Knowledge Block 2 - Anti-Money Laundering Law and Regulation in Hong Kong is Complete

You have completed the second knowledge block and can continue to the next section by pressing the Next button.

If you would like to go back and review the content in this knowledge block, press the return button.
The first requirement for financial institutions in Hong Kong is that they conduct Customer Due Diligence (CDD), which includes ongoing monitoring, follows a Risk Based Approach (RBA). This generally means that when customers are assessed to be at higher risk for money laundering or terrorist financing, the insurance company will be required to undertake Enhanced Due Diligence (EDD) measures to mitigate that risk.

Where the risk is assessed to be lower, the company may take simplified measures. The purpose of CDD is not to prevent the company from doing business with the customer, but to effectively manage the money laundering risk.
In order to understand the customer’s risk, the financial institution must not only fully identify the customer at the time an account is opened, it must also understand the nature of the customer’s business and be able to identify suspicious or illegal transactions. This is also described as **Know Your Customer**.

The CDD/KYC measures must be ongoing and provide a financial profile of the customer’s account to understand the origin of funds and to recognize transactions that are not normal for the individual or business, inconsistent with legitimate business activity or make no financial or economic sense.

**Documents and records must be kept for a minimum of six years following the transaction or closing of an account.**
Identification Requirements – Hong Kong Residents

- Full name, date of birth, nationality, identity document
- Hong Kong Identity Card number
- Insurer should retain a copy of the Identity Card
- Non-permanent residents should provide travel documents (passport), copy retained by insurer
Identification Requirements – Foreign Persons

- Government issued identification documents that are the equivalent of those issued in Hong Kong.
- Documents provided by a regulatory authority in the foreign country or in Hong Kong.
Address Verification

- Insurer should verify residential and permanent address by use of a **utility bill** (3 months)
- Government correspondence within the past 3 months
- Statement issued by an authorized **financial institution** within the past three months
- Record of a visit or acknowledgement of a receipt signed by the customer in response to a letter sent by the
- **Mobile phone** or pay TV bill issued within the past 3 months
- **Letter from employer** confirming employment contract or residence
- **Lawyer’s confirmation** of property purchase or ownership
- In the case of a non-resident in Hong Kong, a government issued identity card showing correct residential address or bank statements showing residence.
Customer Due Diligence/Know Your Customer

- Must include copy of articles of incorporation and business registration
- Identifications of all officers and directors, and the ownership structure of the company
- Verify the business address and details of operation of the company.
- Insurer should look behind the customer to identify those who have ultimate control or beneficial ownership over the business or the customer’s assets.
- Review from time to time the status of the legal person or trust to determine whether the form has changed or been modified.
- Insurer should verify information with Internet websites and other sources.
Customer Due Diligence – Red Flags

- Customer provides false or fraudulent identification documents to open account
- Customer seeks or accepts very unfavorable contract/policy/terms
- Customer seeks a policy/transaction that has no business purpose or makes no economic sense
- Customer requests that details about the account opening or other transaction not be reported to the government (No STR filing)
- Customer seeks to corrupt or bribe a company employee regarding customer due diligence
- Customer uses corporate vehicles or structures whose only purpose is to avoid transparency.
Customer Due Diligence/Know Your Customer

- Funds are received from a country designated as a high risk for money laundering.
- Premium is paid from a foreign account in a different jurisdiction or domicile than the customer’s residence.
- Customer uses multiple sources of funds or types of instruments to settle a transaction.
- Customer overpays a premium and is unwilling to use the overpayment for next installment.
- Multiple payments for premiums from different accounts which do not exceed a reportable threshold (structuring).
- Money passes through a number of different persons or entities, preventing transparency and disguising the source of funds, (layering).
Customer Due Diligence – Red Flags

- Customer seeks an early termination or early surrender of investment type policies, especially with penalty or when this makes no economic sense
- Customer cancels policy and requests a refund to a third party
- Customer overpays a premium, and request payment of the excess to a third party in a foreign currency.
- Customer terminates the policy early and requests the refund cheque be issued to a third party
- Policyholder changes beneficiaries without the insurer’s knowledge or consent
- Customer makes large or simultaneous requests of advance redemption of policies, or uses them to obtain loans – especially accepting disadvantageous conditions.
Knowledge Block 3 - Customer Due Diligence/Know Your Customer is Complete

You have completed the third knowledge block and can continue to the next section by pressing the Next button.

If you would like to go back and review the content in this knowledge block, press the return button.
Reporting Suspicious Transactions

Suspicious transactions and suspected money laundering activity observed in the course of business must be reported by the insurer, but what exactly does this mean?

Under Section 25A of the DTROP and the OSCO, failure to disclose that a person “knows or suspects” that property represents the proceeds of drug trafficking or an indictable offense, is a crime, punishable by 3 months imprisonment and a $50,000 fine.

Such reports must be filed as soon as it is reasonable practical to do so.
Reporting Suspicious Transactions

Filing a Suspicious Transaction Report with the JFIU satisfies the legal obligation to disclose or report the suspicious activity.

If an insurance agent or broker reports a suspicion to the appropriate person designated by the employer, his or her legal obligation to disclose has been satisfied.
Reporting Suspicious Transactions

Knowledge and suspicion of money laundering must be reported. This includes:

• Actual knowledge
• Knowledge of circumstances that would indicate facts to a reasonable person
• Knowledge of circumstances that would cause a reasonable person to make additional inquiries.

In deciding whether to report a suspicious transaction, the key is to recognize the difference between “normal” or regular business activities conducted by the customer and those which are unusual or out of the ordinary. This comes back to knowing your customer and the Customer Due Diligence measures that began at the outset of the business relationship.
Examples of Suspicious Transactions/Activity

- Transactions or instructions that make no business sense or have no apparent economic purpose
- Transactions or instructions that are unnecessarily complex, are illogical, inconvenient, or insecure
- Transactions that are much larger, more frequent, or otherwise out of the normal pattern for the customer.
- Customer refuses to provide information in response to a CDD request
- Customer requests transfers to or from high-risk jurisdictions or to entities not connected with the business enterprise
- Unnecessary routing of funds through third-party accounts
Reporting Suspicious Transactions

- DTROP, OSCO, and UNATMO prohibit the insurer or its staff from disclosing that it has filed a Suspicious Transaction Report. This “tipping off” is a criminal offense.
- Suspicious Transaction Reports should be electronically filed via the STREAMS system at the JFIU, accessible at www.jfiu.police.gov.hk
- Urgent disclosures can be noted on the form.
REPORT MADE UNDER SECTION 25A OF THE
DRUG TRAFFICKING (RECOVERY OF PROCEEDS) ORDINANCE OR
ORGANIZED AND SERIOUS CRIMES ORDINANCE /
SECTION 12 OF THE UNITED NATIONS (ANTI-TERRORIST MEASURES) ORDINANCE
TO THE JOINT FINANCIAL INTELLIGENCE UNIT ("JFIU")

Date:
Ref. No.:

(A) SOURCE
Name of Institution:  
Tel. No.:
Reporting Officer:  
Fax No.:
Signature:  
Email:

(B) SUSPICION
Please provide details of transaction and property arousing suspicion and any other relevant information
relating to money laundering associated predicate offence(s) and/or terrorist financing. Please also
include any explanation given by the person(s) conducting the transaction and/or dealing with the property.
Particulars of account holder, person conducting the transaction and the transactions are to be given in the
following sections)
Knowledge Block 4 - Reporting Suspicious Transactions is Complete

You have completed the fourth knowledge block and can continue to the next section by pressing the Next button.

If you would like to go back and review the content in this knowledge block, press the return button.
Assessment

The three phases or stages of the money laundering cycle are:

- Placement, layering, and integration
- Active, passive, and corrupt
- Cash, check, and wire transfer
- Conversion, transactions, spending
Suspicious Transaction Reports are Submitted to the:

- Joint Financial Intelligence Unit
- Hong Kong Monetary Authority
- Hong Kong Commissioner of Insurance
- Bank of International Settlements
Assessment

Suspicious Transaction Reports must be submitted by the reporting Financial Institution (FI):

- As soon as it is reasonable to do so.
- By the end of the calendar year.
- Within 30 days.
- Within 24 hours.
Examples of identification acceptable for opening an account or establishing a relationship by a Hong Kong resident include:

- All of the above
- Hong Kong Identification card
- Hong Kong driver’s license
- Hong Kong passport
Documents and records relating to suspicious transactions or other account information must be retained for at least:

- Six years.
- One year
- Ten years
- Six months
Examples of identification acceptable for opening an account or other relationship by foreign persons include:

- Valid travel document (unexpired international passport)
- Correspondence with return address
- Employee identification card
- None of the above
Assessment

“Tipping off” the party that is the subject of a Suspicious Transaction Report:

- All of the above.
- Is an offence that can carry a three year penalty when intentional.
- Can be accidental and must be avoided when preparing the Suspicious Transaction Report.
- Is a risk that must be taken into account when performing Customer Due Diligence inquiries.
Money laundering often involves the conversion of large amounts of cash into some other form. The payment of a single-premium life insurance policy with a large sum of cash is an example of:

- Placement
- Layering
- Integration
- Structuring
In making premium payments, the policyholder uses funds that pass through a number of different persons or businesses, preventing transparency and disguising the source of the funds. This is an example of:

- Layering
- Placement
- Integration
- Fraud
Assessment

Examples of factors that increase risk and call for Enhanced Due Diligence include:

- All of the above.
- Customer/Policyholder is a Politically Exposed Person (PEP)
- Transactions involve third-parties in country at high-risk for narcotics trafficking
- The regulatory authority instructs that EDD measures be taken concerning the individual or business
Assessment Review

You scored: 10
Maximum Score: 10
Correct Answers: 10
Total Questions: 10
Accuracy: 100 %
Attempts: 1
Result: Passed, results reported to manager
Certificate and Management Notification

Print Certificate of Completion

Name on Certificate

Certificate and Management Notification

Section 6, Page 2 of 4
Glossary of Money Laundering Terms and Abbreviations

• **AMLO** – Anti-Money Laundering and Counter Terrorist Financing (Financial Institutions) Ordinance, Cap. 615
• **CDD** – Customer Due Diligence “Customer” = Policyholder
• **DTROP** – Drug Trafficking (Recovery of Proceeds) Act
• **EDD** – Enhanced Customer Due Diligence
• **ICO** - Insurance Companies Ordinance, Cap. 41
• **JFIU** – Joint Financial Intelligence Unit
• **MLRO** – Money Laundering Reporting Officer
• **OSCO** – Organized and Serious Crimes Ordinance
• **PEP** – Politically Exposed Person – Person entrusted with a prominent public function.
• **RBA** – Risk Based Approach
• **STR** – Suspicious Transaction Report
• **UNATMO** – United Nations (Anti-Terrorism Measures) Ordinance
Glossary of Money Laundering Terms and Abbreviations

- **Placement** – the initial stage of the money laundering cycle and it could also be considered a conversion phase, as the purpose is to change the form of the illicit funds or to move them away from the criminal activity.
- **Layering** – the second stage of the cycle, and is designed to distance the funds or assets from the criminal activity.
- **Integration** – the final stage of the money laundering process, in which the criminal obtains full use of funds that appear to come from a legal or legitimate source.
- **Structuring** – a laundering technique (placement) in which bulk cash is divided into smaller amounts to conduct transactions below legal reporting requirements.
- **Tipping off** – Making a disclosure to the subject of the report that a Suspicious Transaction Report has been filed. Intentional disclosures are criminal offenses.