TI HK Services Limited

Anti-Money Laundering and Counter-Terrorism Policy
March 2021

Contents

1. Preamble

a) Background

Ti HK Services Limited is a limited company duly incorporated on 29 June 2020 pursuant to the laws of Hong Kong, under registration number 2955324 and having its registered address at Unit 1904-5, Trade Center 135 Bonham Strand, Sheung Wan, Hong Kong (the "**Company**").

The Company is a treasury services company, providing treasury consulting, collection and payment services to Titan FX Limited, a company duly incorporated on 18 May 2017 pursuant to the laws of Vanuatu, under registration number 40313 and having its registered address at Govant Building, 1276 Kumul Highway, Port Vila, Vanuatu (the "**Customer**").

The Company still established comprehensive anti-money laundering ("**AML**") and counter terrorist financing ("**CTF**") procedures for the compliance of the "The Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Chapter 615" ("**AMLO**") and all applicable laws and regulatory requirements that are relevant to AML or CTF.

These procedures and relevant documents are used to avoid any person/entity from making use of the Company's money services as channels to commit money laundering, terrorist financing or any criminal activities. These procedures and relevant documents are also designed to help the staff understanding respective responsibilities under applicable AML and CFT regulatory requirements, and implementing our Company's AML and CFT systems during their normal course of employment.

b) What is money laundering and terrorism financing?

Money Laundering ("ML")
Under the AMLO, money laundering is defined as means, transactions with the aim to conceal or change the identity of criminal proceeds, so that the money, after such processing, will appear to have originated from a legitimate source.
Criminal proceeds often come in the form of cash which is a common medium of exchange in the world of drug trafficking and organized crime. The AML procedures provide the three common stages in money laundering:

1. **Placement** - the physical disposal of cash proceeds derived from illegal activities;
2. **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and
3. **Integration** - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

The Company could be used by criminals to convert money from one currency to another and/or transfer money from one country to another, to make it more difficult for investigators to trace.

Terrorist Financing ("TF")
Under the AMLO, terrorism financing is defined as:

a. the provision or collection, by any means, directly or indirectly, of any property

i. with the intention that the property be used; or
ii. knowing that the property will be used, in whole or in part, to commit one or more terrorist acts; or

b. the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or
c. the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

Terrorist financing generally includes the carrying out of any transaction that involve funds owned by terrorists, or funds that have been or are intended to be, used to facilitate the commission of terrorist acts. Terrorist financing focuses on the directing of funds, whether legitimate or not, to terrorists.

As money may be sent overseas by using the services of the Company, we should be able to identify and report transactions with terrorist suspects.

c) Scope

The purpose of the procedures is to prevent the Company from being engaged in terrorism financing and money laundering. Therefore, AML and CTF measures include:

1. Appointment of a compliance officer and money-maundering reporting officer;
2. CDD procedure;
3. Ongoing Monitoring;
4. Suspicious transaction reports;
5. Record-keeping;
6. Staff training and screening.

The procedures are applicable to the Company and it is the sole responsibility of the Company to ensure that the Customer also adheres to these procedures.

The management shall review the existing procedures on an annual basis in order to address any potential AML or CTF risk, and to take a proactive approach to mitigate the identified ML or TF risk. Senior management will ensure the existing operation process allows staff to escalate potential or identified ML/TF issues on a timely basis.

The management will assign the compliance officer or engage an external professional firm to conduct a regular review of AML/CFT systems on an annual basis.

The management will perform periodic ML/TF risk assessments every two years (or when trigger events occur) to understand how and to what extent the Company is vulnerable to ML/TF risk. The risk assessment must be capable of identifying the various risk factors exposed to our Company. The management, compliance officer and their delegates will determine risk control measures in response to each identified risk factor subject to our Company's ML/TF risk appetite.

2. Appointment of a compliance officer and money-laundering reporting officer

a) Compliance officer ("**CO**")

The director of the Company is appointed as CO.

The primary responsibilities of the CO include:

1. prevention and detection of ML and TF;
2. providing support and guidance to the management to ensure that ML and TF risks are adequately managed;
3. developing and/or continuously reviewing the Company's AML and CTF systems to ensure they remain up-to-date and meet current statutory and regulatory requirements;
4. overseeing all aspects of the Company's AML and CTF systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;
5. identifying and rectifying of deficiencies in the AML and CTF systems;
6. mitigating ML and CT risks arising from business relationships and transactions with persons from countries that do not or insufficiently apply the FATF Recommendations;
7. being the communication key on AML and CTF issues with the management, including, where appropriate, significant compliance deficiencies;
8. making changes in respect of new legislation, regulatory requirements or guidance; and
9. providing AMLC and CTF staff training.

b) Money-laundering reporting officer ("**MLRO**")

The MLRO is responsible for monitoring transactions and ensuring compliance with the procedures. The MLRO will also be responsible for reporting of suspicious transactions to the JFIU.

The MLRO shall have reasonable access to all the necessary information and documents, which would help him in the effective discharge of his responsibilities.

The responsibility of the MLRO may include:

1. reviewing all internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU;
2. maintaining all records related to such internal reviews;
3. providing guidance on how to avoid tipping off if any disclosure is made;
4. acting as the main point of contact with the JFIU and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.
5. putting in place necessary controls for detection of suspicious transactions;
6. receiving disclosures related to suspicious transactions from the staff or otherwise;
7. deciding whether a transaction should be reported to the appropriate authorities;
8. preparing annual review on the adequacy or otherwise of systems and procedures in place to prevent money laundering and submit it to the management.

After making appropriate investigations, the MLRO will consider, if appropriate, reporting the matter to the JFIU within reasonable time, if possible. Any suspicious transaction undertaken, should have prior approval of MLRO.

All records to the MLRO and the relevant authorities, shall be kept by the MLRO for a term of no less than 6 years after the matter has been closed.

MLRO shall act as the central contact point with the relevant authorities. Any failure to report suspicious matter by staff to the MLRO would render that member of staff to be subject to legal penalties and disciplinary action.

3. Corporate Customer due diligence ("CDD")

a) Requesting relevant document for the Customer's identity verification

The Company is acting as a treasury services company for the exclusive usage of the Customer. As a result, the Company cannot accept any other customer than the Customer. The CCD will focus solely on the Customer identification.

The Customer is required to disclose the following information:

(a) full name

(b) date of incorporation or registration

(c) place of incorporation or registration

(d) unique identification number (incorporation number or business registration number)

(e) name of directors, shareholders, beneficial owners and authorized representatives

(f) principal place of business (if different from the address of the registered office)

The Customer should also provide any of the following documents to allow us to verify the identify information given above:

(a) a copy of the certificate of incorporation and/or business registration

(b) a copy of the Customer's memorandum and articles of association which evidence the powers that regulate and bind the Customer

(c) a copy of the shareholders and redirectors registers

(d) a copy of the passports of each director, shareholder, beneficial owner and authorised representative

(e) a copy of the certificate of incumbency and certificate of good standing

(f) the details of the ownership and structure control of the Customer (an ownership chart)

(g) company search report issued within the last 6 months (if available)

(h) other relevant documents provided by a reliable and independent source (e.g., government body)

For documents in a foreign language, appropriate steps should be taken so that we are reasonably satisfied that the document provides evidence of the Customer's identity.

b) Requesting relevant document for associated persons

The due diligence procedures for the Customer involve identifying the Customer's connected parties, beneficial owners, directors and authorized persons/representatives ("**Associated Persons**") and verifying their identifiable information.

The Associated Persons are requested to disclose their full name, date of birth, nationality and unique identification numbers, and to provide the following identity documents for the purpose of verifying their identity:

Type of documents:

(a) Hong Kong permanent resident: Hong Kong Permanent Residential ID Card.
(b) Hong Kong non-permanent Resident: Hong Kong ID Card; Valid Travel Document; Government-issued document that certifies nationality (e.g., local identity card, driving licence).
(c) Foreigner: Valid Travel Document; or Government-issued document that certifies nationality (e.g., local identity card, driving licence).

The Associated Persons should also be requested to provide their residential address information.

The responsible staff should verify and record the Associated Persons' identity documents. For documents in foreign language, appropriate steps should be taken so that we are reasonably satisfied that the document provides evidence of the Associated Person's identity.

CDD against a Beneficial Owner

The AMLO defines the beneficial owner of a corporation as:

(a) an individual who:

i) owns or controls, directly or indirectly, including through a trust or bearer shareholding, more than 25% of the issued share capital of the corporation;

ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or

iii) exercises ultimate control over the management of the corporation; or

(b) if the corporation is acting on behalf of another person, means the other person.

c) Negative checking

All Associated Persons of the Customer must be screened.

If the checking that the Customer or its associated persons is confirmed to be a sanctioned party, a terrorist or located/domiciled in restricted jurisdictions, we should suspend the CDD process and prepare a suspicious transaction report ("**STR**").

A domestic or foreign politically exposed person ("**PEP**") is an individual who is or has been entrusted with a prominent public function in any government, including head of state, head of government, senior politician, judicial or military official and etc. Their spouse, partner, child or parent and close associate are also defined as PEPs.

An international organization PEP is an individual who is or has been entrusted with a prominent function by an international organization. Their spouse, partner, child or parent and close associate are also defined as international organization PEPs.

Our Company adopts a stringent approach to all kinds of PEPs. If the Customer or any of its Associated Persons is a PEP or becomes a PEP, we shall apply all the following enhanced due diligence measures:

1. obtaining approval from management

2. taking reasonable measures to establish the Customer's source of wealth and the source of the funds; and
3. applying enhanced monitoring to the Customer's transactions.

d) Handling the Customer incomplete CDD process

When we cannot verify the Customer identity because the Customer does not provide all relevant documents, we will do the following:

(a) suspend or terminate the business relationship with the Customer unless there is a reasonable explanation

(b) determine whether it is necessary to file a suspicious transaction report if deemed necessary

4. Ongoing monitoring

It is important for the Company to be able to correctly identify the Customer and its activities throughout the relationship. According to the AMLO, we are required to continuously monitor our business relationship with the Customer by:

1. reviewing from time to time documents, data and information relating to the Customer to ensure that they are up-to-date and relevant;
2. monitoring the activities of the Customer to ensure that they are consistent with the nature of business, the risk profile and source of funds. An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that Customer, or with the normal business activities for the type of product or service that is being delivered; and
3. identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF.

At the request of the CO, we shall monitor the following:

1. the nature and type of transactions (abnormal size or frequency);
2. the nature of a series of transactions (a number of cash deposits);
3. the amount of any transactions, paying particular attention to particularly substantial transactions;
4. the geographical origin/destination of payment or receipt; and
5. the Customer's normal activity or turnover.

5. Handling suspicious transactions

When conducting the Customer due diligence or transaction monitoring, if staff discover any suspicion which cannot be properly explained by the Customer or transactions that are relevant to restricted jurisdictions, the staff have to report the transaction to the JFIU.

All JFIU reports and relevant documents will be kept by the CO. The soft copies of the JFIU reports and relevant will be maintained in a computer folder or hard-disk, which can only be reviewed by the CO or staff designated by the CO.

The JFIU report must include details of the date of the disclosure, the person who made the disclosure, and information to allow the papers relevant to the disclosure to be located.

According to the AMLO, it is an offence to reveal to any person any information which might prejudice an investigation; if the Customer is told that a report has been made, this would prejudice the investigation and an offence would be committed. Any possible tipping off by staff would render that member of staff to be subject to legal penalties and internal disciplinary action.

All staff have the obligation to report a transaction if they know or doubt that the transaction may be related to ML/TF. Suspicion is subjective, staff are not necessary to know the nature of the underlying criminal activities. Where a transaction is inconsistent in amount, origin, destination, or type with the Customer's known, legitimate business or personal activities, the transaction should be considered as unusual and staff should be on alert.

If the Customer has been reported to JFIU for a specific transaction, it will not be exempted for another report to JFIU if the Customer is related to another suspicious transaction.

MLRO or CO is the one to determine if he should make suspicious report to JFIU. A consent response from JFIU to a reported transaction should not be construed as "clean bill of health" for continued operation of the account or an indication that the account does not pose ML/TF risks. The responsible staff, CO and MLRO should take reasonable steps to control any ML/TF risk. If JFIU make injunction or restraint order against the Customer, the responsible staff should ensure that they can freeze the relevant property that is the subject of the order.

We are not obliged to continue business relationships with the Customer if such action would place us at risk. Management is suggested to indicate any intention to terminate a relationship in the initial disclosure to the JFIU, thereby allowing the JFIU to comment, at an early stage, on such a course of action.

6. Records keeping

The objective of record keeping is to ensure that we are able to provide the basic information about the Customer and to reconstruct the transactions undertaken at the request of the relevant authorities from time to time.

According to the AMLO, the Company is required to keep:

1. 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 and/or beneficial owner of the Customer and/or beneficiary and/or persons who purport to act on behalf of the Customer and/or other connected parties to the Customer;
2. any additional information in respect of a customer and/or beneficial owner of the Customer that may be obtained for the purposes of enhanced due diligence or ongoing monitoring;
3. the original or a copy of the documents, and a record of the data and information, on purpose and intended nature of the business relationship;
4. the original or a copy of the records and documents relating to the Customer's account and business correspondence with the Customer and any beneficial owner of the Customer (which at a minimum should include business correspondence material to CDD measures or significant changes to the operation of the account).

The Company should also be able to keep track of transactions. The records should include a track of the sums, frequencies, where funds are remitted to, currencies exchanged, and see if the trading

records are consistent with their descriptions at the time any transaction may possibly be considered suspicious.

In order to comply with the above requirements, all records of the Customer and transactions must be kept at the registered address of the Company and uploaded to the system at the end of each day

The Company will maintain the Customer/transaction records for 6 years after the end of the business relationship / the completion of the transaction.

The Company will provide the Customer and transaction information to the relevant authorities as and when demanded or under specific circumstances stated in the law.

All correspondence/reports, both internal or with the appropriate authority, in connection with suspicious transactions must be retained by the Company for a minimum period of 6 years after the relevant authority has closed the case.

7. New staff and staff training

All the managers and staff must be trained to be aware of the policies and procedures relating to the prevention of money laundering and the need to monitor all transactions to ensure that no suspicious activity is being undertaken.

Training on AML/CTF will be given to all staff and when there are any updates, the CO will update all staff on the changes and how to deal with these new updates.

During all training, the employees shall be told of their responsibility as per the law in force regarding obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering and terrorists financing activities.

In particular, the Company shall provide training to:

1. all new staff:
    i. an introduction to the background to money laundering and terrorist financing and the importance placed on money laundering and terrorist financing by the Company; and
    ii. the need for identifying and reporting of any suspicious transactions to the MLRO, and the offense of “tipping-off”;
2. members of staff who are dealing directly with the Customer:
    i. the importance of their role in the Company’s money laundering and terrorist financing strategy, as the first point of contact with potential money launderers;
    ii. The Company’s policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities;
    iii. training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required;
3. back-office staff:
    i. appropriate training on the Customer verification and relevant processing procedures; and
    ii. how to recognize unusual activities, including abnormal settlements, payments or delivery instructions;
4. managerial staff, including internal audit officers and COs:

i. higher-level training covering all aspects of the Company's AML/CFT regime; and
ii. specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the JFIU;

5. MLROs:
   i. specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and
   ii. training to keep abreast of AML/CFT requirements/developments generally.

All staff shall keep records of their own training records and make sure that all materials are maintained up to date and the CO may, from time to time, check how well they have maintained their records.

Any staff member failing or refusing to attend training will result in disciplinary action against them by the CO.

All training records shall be maintained for at least three years.

The Company's new joiners and existing employees are all subjected to appropriate screening in order to ensure high standards when hiring employees.