REV. 2016-04

C 7 Traders AML & CTF Internal Procedures

The scope of engagement of C 7 Traders is restricted to providing an online platform to facilitate its account holders and customers to engage in trading in margined financial instruments as principal. For the avoidance of doubt, C 7 Traders does not enter into trades in margined financial instruments for and/or on behalf of any of its account holders or customers.

TABLE OF CONTENTS

Contents

1. SUMMARY

C 7 TRADERS VANUATU LIMITED (the Company) is an entity that is in the business of providing dealers in securities activities.

As such, we are considered as a "reporting entity" and we have to implement a compliance regime intended to ensure compliance with our reporting, record keeping and client identification requirements.

As a consequence, we have implemented a compliance regime for the following activities conducted on behalf of any of our clients:

- Forex Broker

The implementation of a compliance regime is a legislative requirement and a good business practice for anyone subject to the Anti-Money Laundering and Counter-Terrorism Financing Act No 13 of 2014 as amended by the Anti-Money Laundering and Counter-Terrorism Financing (Amendment) Act No. 2 of 2015 (the Act) and its regulations.

Article 33 of the Act provides that the AML and CTF Procedure Manual must contain internal policies, processes and procedures:

a. to implement the reporting requirements under Part 6 of the Act; and

b. to implement the customer due diligence requirements under Part 4 of the Act; and

c. to implement the record keeping requirements under Part 5 of the Act; and

d. to inform the entity's officers and employees of the laws of Vanuatu about money laundering and financing of terrorism, of the policies, processes and procedures and systems adopted by the entity to deal with money laundering and financing of terrorism; and

e. to train the entity's officers and employees to recognise and deal with money laundering and terrorism financing; and

f. on the role and responsibility of the AML and CTF Compliance officer; and

g. on the establishment of an independent audit function which is able to test its AML and CTF processes, procedures and systems; and

h. on the adoption of systems by the entity to deal with money laundering and terrorism financing; and

i. on the staff screening, recruitment and retention program.

A well-designed applied and monitored regime will provide a solid foundation for compliance with the legislation.

Company's compliance regime includes the following:

- Appointment of a compliance officer and his/her responsibilities;
- Customer Due Diligence (Identification and Verification);
- On-Going Customer Due Diligence and Transaction Monitoring;
- Reporting of financial and suspicious transactions to the FIU;
- Record Keeping (Customer and Transaction);
- Staff Training/Awareness;
- AML/CFT Audit Function; and
- AML/CFT Risk Management System.

2. APPOINTMENT OF A COMPLIANCE OFFICER AND HIS/HER RESPONSIBILITIES

The Company's appointed compliance officer is CHAN YUEN ANN

The Company's appointed alternate compliance officer is YANG SHIHAO

The compliance officer is in charge of ensuring the Company's compliance with the requirements of the Act and the regulations.

3. CUSTOMER DUE DILIGENCE REQUIREMENTS

A. Customer Due Diligence (Identification and Verification)

Effective "customer due diligence" (CDD) measures are an essential part of any system designed to prevent money laundering.

A customer will be one of the following:

a. An individual.
b. The trustee of an express trust or other similar legal arrangements where they are acting on behalf of these entities.
c. A legal person – bodies corporate, foundations, anstalts, partnerships, associations, or any similar bodies that can establish a permanent customer relationship with the Company or otherwise own property.

CDD measures need to be carried out:

- when establishing a business relationship,
- when carrying out an occasional transaction,
- where there is a suspicion of money laundering or terrorist financing; and
- where there are doubts concerning the veracity of previous identification information.

CDD procedures have to be applied to new clients.

Before entering a business relationship, the Company :

- Identifies a customer and verifies a customer's identity using reliable, independent source documents, data or information;
- Identifies the beneficial ownership and control of the customer and takes reasonable measures to verify the identity of the beneficial owners and controllers such that a financial service business is satisfied that it knows who the beneficial owners and controllers are;
- Obtains information on the nature of the customer's business and the customer's economic circumstances;
- Obtains information on the purpose and intended nature of the business relationship;
- Obtains information on the type, volume and value of the activity that can be expected within the relationship;
- Obtains information on the source of funds and, subject to the risk assessment, obtains information on the source of wealth;
- Monitors activity and transactions undertaken within the relationship to ensure that the activity or transaction being conducted is consistent with the Company's knowledge of the customer; and
- Keeps the information relevant and up to date.

B. On-Going Customer Due Diligence and Transaction Monitoring

CDD must also be applied to existing clients at appropriate times on a risk-sensitive basis.

The risk assessment for existing business relationships must include a review of the information and documentation held in respect of those customers. Such a review will highlight those relationships where there is doubt about the veracity or adequacy of the information and documentation held.

An appropriate time to conduct CDD procedures on existing relationships will therefore be at any time when we become aware that any of the circumstances listed below apply either as a result of the risk assessment or otherwise:

a. A transaction that is suspected may be related to money laundering or terrorist financing.

b. A pattern of behavior that causes us to know or suspect that the behavior is or may be related to money laundering or terrorist financing.

c. Transactions or patterns of transactions that are complex or unusually large and which have no apparent economic or visible lawful purpose.

d. We become aware of anything which causes it to doubt the identity of the person who, in relation to the formation of the business relationship, was the applicant for business.

e. We become aware of anything which causes it to doubt the veracity or adequacy of CDD information and documentation already produced.

f. A suspicion of money laundering or terrorist financing in respect of a person for whom identification evidence is not already held.

g. A change in identification information of a customer.

h. A change in underlying principals or third parties on whose behalf a customer acts.

i. A change in the beneficial ownership and / or control of a customer.

j. An absence of meaningful originator information on wire transfers.

k. In respect of wire transfers, where a one-off payment in excess of VT 1,000,000 is to be made.

4. REPORTING OF FINANCIAL AND SUSPICIOUS TRANSACTIONS TO THE FIU

Suspicious Transactions and Suspicious Activity

Suspicious transactions are financial transactions that we have reasonable grounds to suspect are related to the commission of a money laundering offence. This includes transactions that we have reasonable grounds to suspect are related to the attempted commission of a money laundering offence.

Suspicious transactions also include financial transactions that we have reasonable grounds to suspect are related to the commission of a terrorist activity financing offence. This includes transactions that we have reasonable grounds to suspect are related to the attempted commission of a terrorist activity financing offence.

This applies not only when the financial transaction has been completed, but also when it has been attempted.

As a general guide, we consider that a transaction may be connected to money laundering or terrorist activity financing when we think that it raises questions or gives rise to discomfort, apprehension or mistrust.

The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business and from one client to another. We valuate transactions in terms of what seems appropriate and is within normal practices in our particular line of business, and based on our knowledge of our client. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist activity financing.

Money Laundering Offence

Under Vanuatu law, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (such as money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means most serious offences under the Penal Code or any other Vanuatu Act. It includes, but is not limited to those relating to illegal drug trafficking, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation, tax evasion and copyright infringement.

A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Vanuatu.

Terrorist Activity Financing Offence

Under Vanuatu law, terrorist activity financing offences make it a crime to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorist crimes.

This includes inviting someone else to provide property for this purpose. It also includes the use or possession of property to facilitate or carry out terrorist activities.

Making an STR

Once we have detected a fact that amounts to reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering offence or a terrorist activity financing offence, a suspicious transaction report must be sent to FIU within 2 days.

Confidentiality

We are not allowed to inform anyone, including the client, about the contents of a suspicious transaction report or even that we have made such a report. This applies whether or not an investigation has begun. Because it is important not to tip our client off that we are making a suspicious transaction report, we will not be requesting information from the individual conducting or attempting the transaction that we would not normally request during a transaction.

5. RECORD KEEPING (CUSTOMER & TRANSACTION)

Record keeping is an essential component of the audit trail procedures to ensure that tracing and confiscation of criminal and terrorist funds can be made.

The records that we prepare and maintain are such that :

a. supervisors, auditors and law enforcement agencies will be able to assess the effectiveness of the AML/CFT policies and procedures that are maintained by us;

b. any transactions or instructions effected via the Company on behalf of any individual customer can be reconstructed;

c. any customer can be properly identified and located;

d. a CDD profile can be established for all customers for whom there is a business relationship;

e. all suspicions received internally, and STRs made externally, can be identified;

f. the rationale for not passing on any internal suspicions to the FIU can be understood; and

g. we can satisfy, within a reasonable time frame, any enquiries or court orders from the appropriate authorities as to disclosure of information.

C 7 TRADERS
VANUATU LIMITED

6. STAFF INFORMATION ABOUT AML / CTF PROCEDURES AND STAFF TRAINING / AWARENESS

We establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new directors or partners and all new appropriate employees.

Therefore, we satisfy ourselves that the directors, partners and employees are fit and proper for the performance of their roles. When recruiting new employees, we check references, degrees and country of issuance, professional history. Due diligence applicable to new customers may also be done on new employees on a case by case basis.

Employees awareness raising and training cover :

a. The provisions of AML/CFT legislation and employees‘ personal obligations and liabilities under it particularly with respect to failure to make STRs;

b. Our policies and procedures to prevent money laundering and terrorist financing including:

- CDD requirements and the need to know the customer‘s true identity and enough about the type of business activity expected in relation to the customer or client entity at outset (and on an ongoing basis) so that unusual and suspicious activity can be identified in the future; and
- Record keeping procedures;

c. Our internal reporting procedures;

d. New developments, including information on current techniques, methods and trends in money laundering and terrorist financing.

7. AML / CTF AUDIT FUNCTION

An AML audit serves as an integral part of our business by helping to protect us from being an unintentional conduit for money laundering and fraud.

The audit is a systematic check of our AML/CFT risk assessment and our AML/CFT program by a suitably qualified person (the auditor). The end result is a written report on whether we meet the minimum requirements for our AML/CFT risk assessment and our AML/CFT program;

The AML/CFT program is adequate and effective throughout a specified period; and any changes are required.

Audits of the Risk Assessment are limited to assessing whether this document complies with all of the obligations in the Financial Transaction Reporting Act.

Audit of the Program includes whether it complies with all of the obligations in the Act; whether the policies, procedures and controls are based on the AML/CFT risk assessment; whether the policies, procedures and controls are adequate; and whether the policies, procedures and controls have operated effectively throughout the period.

8. AML / CTF RISK MANAGEMENT SYSTEM

Determing the Risk

We undertake an assessment to estimate how vulnerable we are to money laundering and terrorist financing. In doing so we consider the extent of our exposure to risk by reference to the nature, scale and complexity of our activities, our customers, products and services and the manner in which we provide these products and services to our customers, and the reliance which is placed on any third parties for elements of the CDD collected. These risks are properly addressed by policies, procedures and controls.

We record and document our risk assessment. The assessment is undertaken as soon as reasonably practicable after the relevant person commences business and regularly revisit and update to keep it up to date.

The following list of considerations is to help undertaking this risk assessment.

a. Actively involving all members of senior management in determining the risks posed by money laundering and terrorist financing within those areas for which they have responsibility.

b. Considering organizational factors that may increase exposure to the risk of money laundering and terrorist financing e.g. business volumes and outsourcing aspects of regulated activities or compliance functions.

c. Considering the nature, scale and complexity of our business, the diversity of the operations, the volume and size of our transactions, and the degree of risk associated with each area of the operation.

d. Considering who the customers are and what they do.

e. Considering whether any additional risks are posed by the jurisdictions with which the customers (including introducers) are connected. Factors such as high levels of organized crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect money laundering and the financing or terrorism will affect the risk.

f. Considering the characteristics of the products and services that we offer and assessing the associated vulnerabilities posed by each product or service.

g. Considering how we establish and deliver products and services to our customers. E.g. risks could be higher where relationships may be established remotely (non-face-to-face), or may be controlled remotely by the customer (straight through processing of transactions).

Organizational Risk

Organizational factors that may enhance the level of exposure to the risk of money laundering and terrorist financing include:

a. target market place;

b. monetary strategies;

c. business volumes;

d. geographical areas of business activity;

e. outsourcing aspects of regulated activity / compliance functions.

Customer Risk

Clear customer acceptance policies and procedures are being developed. They have a system of risk grading which includes a description of the types of customer that are likely to pose a higher than average risk of money laundering and terrorist financing. The higher risk the customers, the more extensive the requirements.

Business Risk

We consider the extent to which we are exposed to money laundering and terrorist financing. In so doing, we take account of the primary objectives of money laundering. These include:

a. the intention and requirement to benefit and retain the proceeds of predicate crimes;

b. the need to disguise ownership of criminal property which could otherwise provide a link between the launderer and the predicate crime;

c. the desire to retain an element of control over the criminal property;

d. the need to disguise the origins of criminal property.

Organizational risk, customer risk and product/service risk, including the means by which those products and services are delivered are all taken into account.

Product / Service Risk

We consider the characteristics of the products and services that we offer and the extent to which we are vulnerable to money laundering and terrorist financing abuse. Particular risks are associated with the formation and management of companies and trusts. Generally, any form of legal entity or related service that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it is vulnerable. Examples include the following:

a. companies that can be incorporated without the identity of the ultimate underlying principals being disclosed;

b. certain forms of trusts or foundations including blind trusts, dummy settler trusts and settler directed trusts where knowledge of the identity of the true underlying principals or controllers cannot be guaranteed;

c. the provision of nominee shareholders;

d. companies issuing bearer shares;

e. correspondent banking relationships - a correspondent account can be used to transfer funds on behalf of unidentified third parties;

f. banking services for higher risk accounts or high-net worth individuals such as those offered by private banks;

g. wire transfers - speed and ease of transmission across jurisdictions;

h. any financial service or product that is capable of being provided on a non-face-to-face basis or controlled by a customer remotely.

The highest risk products or services are those with high values and volumes; those where unlimited third party funds can be freely received; or those where funds can regularly be paid to third parties without CDD on the third parties being obtained. For example, some of the highest risk products are those offering money transfer facilities through check books, wire transfers, deposits from third parties or other means. Corporate and personal current accounts and high value deposit / investment accounts naturally fall within this category.

Wealth management and private banking facilities can be particularly vulnerable. Some of the lowest risk products and services are those where funds can only be received from a named investor by way of payment from an account held in the investor‘s name. The funds can then only be redeemed to the same investor‘s account. Such products do not allow third party funding or payments and no opportunity is presented for the onward transmission of funds to third parties in the arrangement. Regulated open and closed-ended investment funds, some insurance products, retail credit business, some asset finance, and low value deposit/savings accounts generally fall within this category.

Notwithstanding the reduced risks of money laundering posed by such products and services, they provide criminals with an opportunity to convert property into a different form for the duration of the relationship and to conceal ownership of funds, particularly where they disguise their interest behind an entity that makes the investment on their behalf. Therefore no product or service is ever immune from the laundering process.

We also consider how we deliver products and services to our customers and the extent to which this might increase the risk. For example, risks are likely to be greater when relationships can be established remotely (non-face-to-face), or when they may be controlled remotely by the customer (straight through processing of transactions).

Activity Risk

We consider risks inherent in the nature of the activity of the account holder and the possibility that the transaction may itself be a criminal transaction. The arms trade and the financing of the arms trade is an example of an activity that poses multiple AML and other risks, for example:

a. Corruption risks arising from procurement contracts;

b. Politically Exposed Person (PEP) risks;

c. Terrorism and terrorist financing risks as shipments may be diverted.

In addition to the movement of weapons and the proceeds of corruption, international bodies have also drawn attention to the need for vigilance in identifying potential attempts by countries that are the subject of sanctions to raise funds for programs to develop nuclear and other weapons of mass destruction.

Contact Us

www.c7traders.com | Email: info@c7traders.com

C 7 Traders Vanuatu Limited
Govant Building, PO BOX 1276,
Port Vila, Vanuatu

T: +44 20 8144 8737
F: +44 20 3318 2803

C 7 Traders London Ltd.
27 Old Gloucester Street,
London,
WCIN, 3AX

T: +44 20 8144 8737
F: +44 20 3318 2803

Shanghai Branch
Nanjing XiLu, Jingan Qu,
Shanghai, China

T: +86 (013) 120801975
QQ: 3401966780
Wechat: C7traders