

**ANTI-MONEY LAUNDERING AND
KNOW YOUR CUSTOMER POLICY
OF
SPARK STREAM LTD.**

CONTENT

1. Introduction	3
2. Money Laundering	3
3. The Money Laundering Reporting Officer (MLRO)	4
4. Risk Based Approach	4
5. Money Laundering Offences	5
6. Reporting of Suspensions	8
7. Employee Awareness and Training	10
8. Record Keeping and Monitoring	10
9. The MLRO's Annual Report	11

1. Introduction

Spark Stream Ltd is a limited liability company, registered under the laws of Belize with registration number 000044910, having its registered address at Sea Urchin Street, San Pedro, Ambergris Caye, Belize (the "Company"). The Company is operating the website bet55.net. The Company is licensed in the State of Anjouan under the Computer Gaming Licensing Act 007 of 2005.

This Anti-Money Laundering and Know Your Customer (AML/KYC) Policy outlines the standards and procedures established to verify the identity of clients, prevent fraud, and ensure compliance with applicable anti-money laundering (AML) and counter-terrorist financing (CTF) regulations. The purpose of this policy is to protect the organization, its customers, and the financial system from misuse by ensuring that all customers are properly identified and their activities are appropriately monitored.

Money laundering is the common term for the process by which a person seeks to conceal the proceeds of crime by exchanging criminal property for so-called clean money. Activities associated with money laundering include:

- acquiring, using or possessing criminal property;
- handling the proceeds of crimes such as theft, fraud and tax evasion;
- being knowingly involved in any way with criminal or terrorist property;
- Investing the proceeds of crimes in other financial products or through the acquisition of property or assets;
- transferring criminal property; and financing of terrorist activities

For the purposes of this Manual, the term money laundering will mean money laundering and terrorist financing.

The proceeds of crime or "criminal property" means any property which constitutes or comes to represent a person's benefit from criminal conduct. Criminal property (which also includes "terrorist property") can take any form: e.g. money, securities, tangible and intangible property and money, whether or not it is "clean" money, which is used to fund terrorism.

2. Money Laundering

Businesses which are seen as likely targets for money launderers wishing to use them as a means to channel the proceeds of crime include: solicitors; accountants; authorized Companies; money services businesses; high value dealers; and trust or company service providers.

There are number of "obligations placed on these businesses, such as:

- a. the identification of customers;
- b. the appointment of a nominated individual to be responsible for reporting suspicious persons and transactions;
- c. the implementation of systems and procedures to combat the use of their services by money launderers;
- d. ensuring that employees are aware of their obligations under the legislation.

3. The Money Laundering Reporting Officer (MLRO)

The MLRO has overall responsibility within the Company's businesses for the establishment and maintenance of effective anti-money laundering systems and controls. This will include providing sufficient information to the Board to enable them to review the effectiveness of these systems and controls and ensure that they remain effective in reducing the risk that the Company is used for money laundering.

The MLRO's responsibilities are:

- a. receiving internal reports from Employees concerning suspicions of money laundering;
- b. taking reasonable steps to access any relevant Information held by the Company including any information held in relation to:
 - i. the financial circumstances of the Client or any person on whose behalf the Client is acting; and
 - ii. the features (type, frequency, volume) of the Transactions which the Company has entered into with or for the Client.
- c. obtaining and using national and international findings on countries and jurisdictions found to be materially deficient in their anti-money laundering procedures and ensuring the Company's compliance with national and international sanctions
- d. taking reasonable steps to establish and maintain adequate arrangements for awareness and training {whether by himself or someone else}; and
- e. making annual reports to the Company's Board of Directors.

The MLRO has full access to all existing client information held by the Company. All Employees must comply with any request by the MLRO to review such information and any other information that the MLRO may ask to see.

4. Risk Based Approach

The Company has adopted a risk-based approach to assessing the most cost effective and proportionate way to manage and mitigate the money laundering risks to the Company.

The application of the Risk Based Approach stipulates that subject persons may determine the extent of the application of Customer Due Diligence requirements on a risk—sensitive basis, depending on the type of customer, business relationship, product or transaction.

The possibility to apply different measures on the basis of the particular ML/ FT risks is a novel concept within the ambit of AML/ CFT. The principle behind this is that resources should be directed proportionately in accordance with the extent of the ML/FT risks posed, so that the business, products and customers posing the highest risks receive the highest attention.

The Company has preferred this approach over a rules-based approach that may lead to a 'tick box' approach with the focus being placed on meeting regulatory needs rather than on effectively combating money laundering. The application of a risk-based approach ensures that measures to prevent or mitigate money laundering are commensurate with the risks identified and that resources are allocated in the most efficient ways.

The steps that the Company will take to achieve this are to:

identify the money laundering risks that are relevant to the Company; assess the risks presented by the Company's

- clients
- products
- delivery channels
- geographical areas of operation
- design and implement controls to manage and mitigate these assessed risks;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done and why.

This risk-based approach allows the senior management of the Company to apply its own approach to procedures, systems and controls, and arrangements that fit with the business of the Company and of its clients.

For identification purposes the levels of due diligence that will have to be undertaken will depend on the level of risk that Senior Management has assessed that the Company may be exposed to when dealing with or for a particular client.

From time to time the MLRO may require additional Information or actions be taken concerning clients or transactions that may not be set out in the published procedures, and Employees are expected to comply at all times with any such requirements.

5. Money Laundering Offences

The phrase "money laundering" covers all procedures aimed to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. This gives rise to three features common to persons engaged in criminal conduct, namely that they seek:

- to conceal the true ownership and origin of criminal proceeds;
- to maintain control over them; and
- to change their form.

Identification of Clients

A client is any person (including individuals, incorporated entities, partnerships, trusts etc.) to whom the Company provides, intends to provide, or has in the past provided a service in the course of carrying on its regulated business. A client for these purposes also includes a potential client.

Before acting for any client, the Company must carry out a process of Customer Due Diligence (CDD). CDD involves:

- a) identifying any client
- b) verifying the client's identity
- c) identifying the beneficial owner where relevant and verifying his or her identity
- d) obtaining information on the purpose and intended nature of the business relationship.

CDD must also be carried out whenever the Company suspects money laundering or has cause to be suspicious about or believes that any documents or other information that has been supplied is out of date or inaccurate. Any business relationship with a client will be subject to periodic review which may result in Employees being asked to conduct CDD or seek additional information from a client at any time.

The verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

Based on the instruments and services provided by the company, the assessed level of risk the Company may be exposed to increases at the time of a client withdrawal of funds. As all clients are screened prior to engagement through an electronic data identification verification that verifies that the client is not listed in a risk group (e.g. PEP's, Criminals and Terrorists), the risk for money laundering exists in the fund withdrawal process.

CDD: Individuals

In each case of a customer engagement, the Company must obtain the individual's:

- full name
- residential address
- date of birth

This Information must then be verified

Documents that could be used to meet this requirement are listed below:

Documents that identify the individual:

- Current signed passport
- Residence permit issued by Home Office on sight of own country passport
- Current photo card driving license
- Firearms certificate

Documents that verify the individual's address:

- signed record of home visit
- recent (within the last 6 months) utility bill that has been posted to the individual's home address
- local authority utility bill (valid for the current year)
- Bank, building society statement or passbook

The above lists are not exhaustive and where appropriate other forms of identification can be presented. Documents listed in the first column may also be used to verify the individual's address but the same document cannot be used to verify both the individual's identity and his or her address.

There are also a number of sources of electronic data that may be used but should not be relied upon as the sole means of identifying the individual.

If using electronic data as the sole means of verifying identity, then the source must be one that uses data from multiple sources collected over a period of time or incorporates checks that assess the strength of the information supplied such as one of the specialist agencies used by the Company for these purposes.

Failure to obtain CDD will cause the client account to be frozen and relationship termination process to be initiated.

Companies and other Incorporated entities

An incorporated entity is identified by:

- a. its registered number;
- b. its registered corporate name and any trading names used;
- c. its registered address and any separate principal trading addresses;

When identifying a corporate Employees should also obtain information about:

- I. its directors or partners (as appropriate);
- II. its owners and shareholders; and
- III. the nature of its business.

Documents suitable for verifying identity include the Certificate of Incorporation, Certificate of Registration, Memorandum and Articles of Association, Partnership Agreement, Shareholder Register, and the latest Report and Accounts. Employees should ask to see at least two of these documents

For each corporate Client, the Employee should obtain a list of all directors and shareholders, or partners. The identity of at least two executive directors or partners should be verified. At least one of these must be the person authorized by the client to instruct The Company. The identity of the major shareholders (anyone with an interest of 25% or more of the corporate) should also be obtained and verified.

Failure to obtain CDD will cause the client account to be frozen and relationship termination process to be initiated.

Identification Records

All evidence establishing the identity of a client must be recorded or copied as appropriate and kept on the client electronic file together with details of all transactions undertaken with or for the client (this may be kept electronically but must be in a printable form). This information must be kept for a minimum period of 5 years.

6. Reporting of Suspicious

All client transactions will be subject to ongoing monitoring and review by the MLRO. Where the MLRO decides that a particular client or transaction should be subject to additional investigation, Employees are expected to comply with such investigation including any requests for additional information.

Any Employee who has any suspicion of money laundering by a person with whom the Company has any business dealings must immediately report the matter to the MLRO in writing

together with the full details. Having made such a report, the Employee concerned will have met his or her legal obligations under the Regulations. The MLRO will decide whether or not to report the matter to the authorities. The reporting of the suspicion of money laundering to the authorities is not a breach of duty or confidentiality to a client and provides important potential safeguards for the position of the company.

Any Employee who is discovered to have failed to report a transaction, which they knew to be suspicious or to have involved money laundering, will be subject to disciplinary action and potentially liable to prosecution unless the Employee has good reason for not reporting the transaction to the MLRO. Employees are therefore advised to report any suspicions, no matter how slight to the MLRO.

An Employee may first discuss their suspicions with their line manager who may then accept responsibility for making a report to the MLRO. Any line manager who is approached by an Employee to discuss a suspicious transaction or one known to involve money laundering must ensure that:

- a) the line manager himself or herself makes a report to the MLRO; or
- b) the Employee who made the approach makes a report to the MLRO; or
- c) the line manager records his or her reasons for not making a report to the MLRO.

Please note: any Employee who has discussed a suspicious transaction or one known to involve money laundering with a line manager may still make a report to the MLRO even if the line manager has undertaken not to do so.

The MLRO will consider any such report in the light of all of the relevant information for the purpose of determining whether or not the information or other matter in the report gives rise to knowledge or suspicion of money laundering.

Auditors and Employees are required to co-operate fully with the MLRO in discharging his duties.

The Company must ensure that all Employees who handle investment transactions of any kind (including back-office staff) are given training in recognition and handling of suspicious transactions and are aware of their individual responsibilities.

Suspicious transactions

Examples of transactions that may give rise to a suspicion of money laundering are set out below but will not necessarily by themselves give rise to sufficient suspicion to warrant a report being made:

- a) large or unusual settlements of deals in cash;

- b) buying and selling transactions with no discernible purpose or in unusual circumstances;
- c) instructions to credit sales proceeds to an account different from that of the original source account or to a third party;
- d) any transaction of a nature, size or frequency which appears unusual; and
- e) where the investor is Introduced by an overseas person and both are based in countries where drug production or drug trafficking may be prevalent.

Employees (including the MLRO) are not expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

7. Employee Awareness and Training

The Company will ensure that all Employees are given periodic training to ensure that each understands their obligations under the anti-money laundering procedures and the requirements for identification of clients. Employees should be aware that a failure in carrying out their responsibilities could result in criminal sanctions being imposed against them.

This training may be either internal or external and will cover:

- (a) the identity and responsibility of the MLRO;
- (b) the potential effect on the Company, its Employees personally and its clients of any breach of the law;
- (c) the money laundering risks that the Company faces;
- (d) the policies and procedures that have been put in place to reduce and manage the risks;
- (e) CDD and monitoring procedures;
- (f) how to recognize potential suspicious activity and the procedures for reporting to the MLRO
- (g) available industry guidance and sources of information.

8. Record Keeping and Monitoring

The MLRO will keep a detailed record of:

- (a) all steps taken to establish the identity of applicants for business or reasons as to why

steps have been taken in a particular case;

- (b) the full name, postal address and date of birth of each person with whom the Company does business;
- (c) the form and source of funds and/or securities used by the applicant for business;
- (d) the form and destination of funds paid or delivered to the applicant for business or another person on his behalf;
- (e) financial transactions carried out by the Company with or for each client or counterparty of the Company.

9. The MLRO's Annual Report

The MLRO will conduct an annual review of the Company's systems and procedures in relation to money laundering and will prepare a report to the Board on his or her findings. The report will include the following:

- (a) an assessment of the Company's compliance with its money laundering obligations and the effectiveness of the Company's systems and controls;
- (b) indicate how new information from the Government and other appropriate authorities in relation to money laundering has been used during the year;
- (c) gives the number of reports made by Employees to the MLRO

The Board will consider the report and take any necessary action to remedy deficiencies identified in the report.