Esports Club Limited (corp.)
Reg. № 2760999 Unit 1503 15F № 69 JERVOIS STREET SHEUNG WAN HONG KONG
support@skinshunter.com

www.skinshunter.com

Anti-Money Laundering (AML) and Client Due Diligence (CDD) Program: Compliance and Supervisory Procedures

~~Last Updated 25/02/2019~~

This AML and CDD Program is designed to establish and Anti-Money Laundering Program and Procedures of Customer Due Diligence (CDD) for the users of our site as required by applicable law and regulations in our residence country, EU and worldwide.

Our AML and CDD Program are risk-based. That means that the program's AML policies, CDD procedures and internal controls are designed to address the risk of money laundering specific to our site. We must identify that risk by looking at the type of customers we serve, where customers are located, and the types of services we offer.

1. AML Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the applicable legislation worldwide and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment- related fraudulent activity.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

We have designated director as our Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for our AML program. He has a working knowledge of the applicable rules and its implementing regulations and is qualified by experience, knowledge and training.

The duties of the AML Compliance Person will include monitoring our compliance with AML obligations, overseeing communication and training for employees, and filing necessary reports if applicable. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that necessary reports are filed with the authorized authority when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce our AML program.

If necessary, we will provide authorized body with contact information for the AML Compliance Person and will promptly notify them of any change in this information.

3. Customer Identification Program and CDD Procedures

We will collect the following minimum information from the users who logged into site
1 full name
2 date and place of birth
3 residential address

If the user holds a valid account in any bank or other financial institution and the validity (operability) of such an account is confirmed by the bank or other financial institution which is subject to AML rules and complies with it, we are entitled by the law to rely upon their CIP or KYC procedures and shall not made any additional CIP or KYC procedures.

We do not open or maintain customer accounts within the meaning of applicable laws, in that we do not establish formal relationships with “customers” for the purpose of effecting transactions in cash or any other financial instruments. If in the future we elect to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions, we will first establish, document and ensure the implementation of appropriate CIP procedures.

Bank confirmed CDD procedure

The user willing to register in our system (on our Site) and open a SKINSHUNTER account should provide us with minimum information as described below.

Upon registration and when the user wishes to made his\her first payment transaction the payment institution we are working with shall initiate due check which shall consist of a short (according to bank\financial institution rules) blocking of a minimum sum (about EUR 1.00) from the bank account\credit card the user wishes to use with respect to a transaction related to his

use of his SKINSHUNTER account. Upon successful check the bank\payment system shall confirm to us the identity of the client.

a. Required Customer Information

Prior to opening an account, we will collect the following information for all accounts, if applicable, for any person that is opening a new SH account and whose name is on the SH account:

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential address (for an individual)

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. We will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means and non-documentary means. We will use documents to verify customer identity when appropriate documents are available.

In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Checking references with other financial institutions (see Bank Confirmed CDD procedure applied for users having valid bank or credit card)

We will use non-documentary methods of verification when:

(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;

(2) the firm is unfamiliar with the documents the customer presents for identification verification;

(3) the customer and firm do not have face-to-face contact; and

(4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before the account is opened.

If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a necessary report in accordance with applicable laws and regulations.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified..

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to file a report in accordance with applicable laws and regulations.

e. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers: the notice shall be published on our Site in the following form:

Important Information About Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

g. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements.

4. Customer Due Diligence Rule

As a rule, we do not open or maintain accounts for legal entity customers. If in the future we elect to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures.

a. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, using the customer risk profile if we create one as a baseline against which customer activity is assessed for suspicious transaction reporting. By suspicious transactions we also mean fraud, and inconvenient or intentionally high selling price abuse.

5. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions

a. Due Diligence for Correspondent Accounts of Foreign Financial Institutions

We will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions.

6. Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

We do not open or maintain private banking accounts.

7. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business.

The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a necessary report is filed.

A. Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business.
- Customer with no discernable reason for using the firm's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

B. Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify the AML Compliance Person. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.

8. AML Recordkeeping

a. Responsibility for Required AML Records and Report Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that reports are filed as required.

b. Reports Maintenance and Confidentiality

We will hold Reports and any supporting documentation confidential. We will not inform anyone outside of appropriate law enforcement or regulatory agency about a reports. We will segregate AML and CDD reports filings and copies of supporting documentation from other firm books and records to avoid disclosing.

We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a report according to the applicable law.

9. Program to Independently Test AML Program

a. Staffing

The testing of our AML program will be performed at least *every two calendar years* by personnel of our firm, none of whom are the AML Compliance Person nor do they perform the AML functions being tested nor do they report to any such persons. Their qualifications include a working knowledge of applicable requirements. To ensure that they remain independent, we will separate their functions from other AML activities. Independent testing will be performed more frequently if circumstances warrant.

b. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

10. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person. We will also review the AML performance of supervisors, as part of their annual performance review.

11. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to *the president/chairman of the board*. Such reports will be confidential, and the employee will suffer no retaliation for making them.

12. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below.

Signed: PAVEL YUROVITSKIY
Title: DIRECTOR
Date: 25/02/2019