

POLICY OF THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

BITTECH B.V.

Confirmed

By the BITTECH B.V.

Management board member



Theodoros Michailidis

on

October 28, 2024

Table of Contents

Policy statement	- 3 -
Terms and definitions.....	- 4 -
Customer Due Diligence	- 6 -
Ongoing customer due diligence	- 7 -
Higher risk customer	- 7 -
Politically exposed persons	- 7 -
Enhanced due diligence	- 8 -
Simplified due diligence	- 8 -
Monitoring	- 9 -
Transactions under increased monitoring	- 9 -
Transactions record keeping	- 11 -

Reporting of unusual transactions	- 12 -
Suspicious transactions indicators	- 12 -
Reporting form.....	- 14 -
Staff training	- 15 -
High risk and prohibited jurisdictions	- 16 -
Sanctions compliance	- 16 -
Risk assessment	- 17 -
Anti-bribery and corruption policy	- 20 -

Policy statement

Bittech B.V. (hereinafter- the “Company”) is a Company established and authorised under the laws of Curaçao and operates its regulated activities in terms of license No.: 970, providing online gaming services.

This policy was generally based on and is in compliance with Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) issued by the Gaming Control Board of Curacao, that are based on National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92), and the National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99), the Sanctions National Ordinance, Curaçao Minimum Internal Control Standards, Curaçao Criminal Code, National Ordinance on the Obligation to report Cross-border Money Transportation, FATF recommendations and FATF Guidance on the Risk-Based Approach for Companys.

The aim of this policy is to prevent possible misuse of the services provided by the Company for the money laundering or terrorist financing purposes as well as to implement the money laundering prevention and counter terrorist financing measures established by the law. The following policy and procedures on the prevention of money laundering and terrorist financing is established and must be followed by the managers and employees of the Company.

With this statement, the board members of Bittech B.V. confirm that the Company commits to combat the abuse of its facilities, products and services for the purpose of money laundering and terrorist financing. The policy applies to all directors, officers, employees.

The Company intends to comply with current anti-money laundering and terrorist financing legislation as well as provisions and guidelines, in particular the laws and guidelines regarding customer due diligence and the reporting of unusual transactions, i.e. the NOIS and the NORUT.

The Company will ensure that its business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. To comply with the above-mentioned legislation, the Company agrees to organise staff training in order to be sure that

all employees are aware of all the potential risks that can arise due to non compliance with the AML/CFT policy and the consequences will follow.

The AML/CFT policy should be revised by the Compliance officer of the Company on a yearly basis and approved by the board member.

Terms and definitions

In this policy the following definitions are used:

- 1) “Compliance Officer” means an employee of the Company who is appointed by the managing director of the Company as the officer responsible for the AML/CFT questions in the Company.
- 2) “Customer” means a person that uses the services provided by the Company.
- 3) “Employee” means any natural person who is employed by the Company on the basis of employment agreement or other agreement.
- 4) “EU Sanctions” means economic or financial sanctions or trade embargoes imposed, administered or enforced from time to time by the European Union.
- 5) “FATF” or “Financial Action Task Force” means an independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;
- 6) “FATF Recommendations” means a framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;
- 7) “Facilitation payments” also called “facilitating”, “speed” or “grease” payments, these are small unofficial payments made to secure or expedite the performance of a routine or necessary action to which the payer of the facilitation payment has legal or other entitlement.
- 8) “FIU” or “The Financial Intelligence Unit” means the Reporting Center of Curaçao; since the latest changes to the AML/TF laws, this is the official name of the FIU (in Dutch: Financiële Inlichtingen Eenheid). FIU Curaçao falls directly under the Minister of Finance. The Head of FIU Curaçao is the administrator of its transactions database.
- 9) “GCB” or “Gaming Control Board” means a foundation, incorporated on April 19, 1999, with the specific purpose of becoming the regulator for the entire gaming industry operating in and from Curaçao.
- 10) “Money laundering” or “ML” means the process by which criminals attempt to conceal the illegal origin of the proceeds of their criminal activity (drugdealing, weapons dealing, human trafficking, kidnapping, etc.) allowing them to maintain control over the proceeds and ultimately, providing a legitimate cover for their sources of income. In the Criminal Code of Curaçao, the penalization of the three types of money laundering (habitual money laundering, intentional money laundering and money laundering by default) is regulated.

- 11) “NOIS” or “National Ordinance on Identification when rendering Services” (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92 as mentioned on page 3.
- 12) “NORUT” or “National Ordinance on the Reporting of Unusual Transactions” (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99 as mentioned on page 3.
- 13) “Office of Foreign Assets Control” or “OFAC” means a department of the U.S. Treasury that is charged with enforcing economic and trade sanctions imposed by the U.S. against countries and groups of individuals.
- 14) “OFAC Sanctions” means economic or financial sanctions or trade embargoes imposed or enforced from time to time by the U.S. government and administered by OFAC.
- 15) “Reporting code” means a unique code, assigned by the FIU to each reporting entity/Company, for the purpose of reporting unusual transactions;
- 16) “Politically exposed person” or “PEP” means an individual who is or has been entrusted with promoting public functions, including head of state or government, senior politician, senior government, judicial or military official, senior executive of publicly owned corporation, and important political party official.
- 17) “Reporting Form” means the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction;
- 18) “Sanctions National Ordinance” means the National Ordinance also known as the “Sanctielandsverordening”, published under N.G. 2014. No. 55 as last amended.
- 19) „Services“ means online gaming services provided by the Company.
- 20) “Terrorist financing” or “TF” means a behaviour as referred to in the International Treaty of New York with regard to combating terrorism financing, signed on December 9th, 1999 (Tractatenblad 2000, no. 12; Tractatenblad 2002, no. 110.
- 21) “Transaction” means an action or combination of actions by or on behalf of the client as referred to in art. 1, par. 1, sub o, of the NOIS or art. 1, par. 1, sub c, of the NORUT.
- 22) “United Nations” or “UN” means an international nonprofit organization formed in 1945 to increase political and economic cooperation among its member countries.
- 23) “UN Sanctions List” means an UN-issued list of countries and individuals that face economic, trading, or diplomatic limitations due to their criminal or peace-violating activity.

Customer Due Diligence

Before starting business relations with the customer, the Company must identify the customer and verify that customer’s identity using reliable, independent source documents, data or information.

The Company performs customer due diligence (CDD) process when:

1. establishes business relations (during onboarding);
2. carries out occasional transaction above the applicable designated threshold of 4000 Cg. (a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of 4000 Cg.)
3. there is a suspicion of money laundering or terrorist financing; or
4. the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Clients' identification and verification

Pursuant to article 3 of the NOIS, the identity of resident and nonresident personal customers shall be established through one of the following valid documents:

- a driver's license;
- an identity card;
- a travel-document or passport; or
- other document designated by the Minister of Finance (The Minister of Finance hasn't designated any other document yet.)

The Company checks the document, its validity terms, signs of a fake documentation, and make sure with all available sources that the person is a real holder of the document. In addition, an AML analyst checks whether the potential customer is not included in the blacklists, Sanctions lists (OFAC, UN, EU), adverse media, as to whether the person is not a PEP.

The information about the customer's place of residence is also collected and recorded in the files. In line with the requirement to verify all customer information, including addresses, we will also ensure compliance with the CGA regulations, which explicitly require verification of customer addresses.

However, the Company can check the IP address of the client and compare it with the client's profile and stated place of residence.

If doubts arise relating to the identity of the client after the Company has accepted the customer and customer accounts have been opened, the relationship with the customer must be re-examined to determine whether it should be terminated and whether the incident must be reported to the FIU in accordance with art. 2d of the NOIS.

The Company will not open or maintain an anonymous account or an account in a fictitious name.

Ongoing customer due diligence

a. The Company performs ongoing due diligence on the business relationship and checks transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, their risk profile, including where necessary the source of funds¹.

b. The Company ensures that documents, data, and information collected through the CDD measures are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers. For all clients repeated CDD is performed once the threshold is exceeded, and on a yearly basis for the low-risk customer group and quarterly basis for the high-risk customer group.

Higher risk customer

The Company should develop risk profiles to determine the customer categories which expose the Company to higher risk².

According to the Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) issued by GCB, the high-risk customers include:

- customers from countries identified as not having adequate AML/CFT systems;
- customers from countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- customers from countries identified as having significant levels of corruption or other criminal activity;
- customers from countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country;
- politically exposed persons, their families and their associates.
- For such high-risk categories, the Company applies **Enhanced Due Diligence (EDD)** measures to ensure stronger monitoring, verification, and mitigation of potential risks.

Politically exposed persons

During onboarding, in addition to applying normal customer due diligence measures, the Company must identify whether the customer is politically exposed person or no.

For identification the Company uses available open sources and databases, such as <https://www.cia.gov/the-world-factbook/>, google, etc.

When the customer is identified as a PEP, AML analyst must:

¹ FATF recommendation 10 d

² Art. 2, par. 4, of the NOIS

- Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- Take reasonable measures to establish the source of wealth and source of funds; and ☐ Conduct enhanced ongoing monitoring of the business relationship.

It is also important to determine whether a customer is a domestic PEP or has been entrusted with a prominent function by an international organization.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Enhanced due diligence

The Company shall conduct enhanced due diligence (EDD) for high-risk customers, consistent with the risks identified.

Examples of enhanced CDD measures include³:

- Obtaining additional information on the customer (e.g., occupation, volume and assets, information available through public databases, internet etc.) and updating more regularly the identification data of customer, at least once per 3 months;
- Obtaining information on the source of funds or source of wealth of the customer;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Simplified due diligence

The Company is allowed to conduct simplified due diligence (SDD) measures, if the risks of money laundering or terrorist financing are lower. The simplified measures should be commensurate with the lower risk factors (e.g., the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring)

If the client does not fall into any of the high-risk categories listed above and no negative information is found in open-source media, **simplified due diligence** may be performed, which means:

- Reduced frequency updates of customer identification, no more than once per year.
- Reduced degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

³ Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) issued by GCB

Simplified CDD measures shall not be applied whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, including high turnovers.

Monitoring

Once the proper due diligence procedure is undertaken and based on the results of the latter the customer is accepted, the further monitoring of the customer, transactions and behaviors are applied. Ongoing monitoring is carried out to ensure that customers meet the requirements stipulated in this policy and our services are not used for any ML/TF purposes as well as to enable us to establish the possible ML/TF actions and undertake the respective preventative measures.

To monitor all the transactions undertaken by the customer and be able to assess their consistency with the risk profile of the customer, during this procedure it must be assessed whether the risk profile or financial position of the customer changed. Records should be amended to reflect these changes. Previous records should still be kept in file.

The Client Due Diligence measures should be also taken every time where the following circumstances reveal:

1. when there are doubts about the veracity or adequacy of previously obtained identification data of the customer;
2. in any other case when there are suspicions that the act of ML or TF is, was or will be performed.

Since the Company provides its services electronically, it also must be sure that the person who acts from the customer's name is a genuine customer, and that the personal details and documents belongs to him, and were not stolen and fraudulently used by the scammer. That is why the Company performs on the location of the computer used when customers' accounts are opened, or during gambling, including IP checks. IP addresses provide information about the country where the computer being used is located.

Company's security service is responsible for checking IP addresses and comparing them with the data provided by the customer.⁴

⁴ <https://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Company's.pdf>

Transactions under increased monitoring

The Company pays particular attention to:

Accounts

- Dormant accounts, accounts without any activity;

Deposits followed by daily cash withdrawals that continue until the transferred sum has been removed. The Company freezes such transactions.

- When opening an account, the customer refuses to provide information required by the financial institution, attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

- The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.

Funding and withdrawals

Customers are allowed to top up their accounts and withdraw the funds using various methods, such as (bank cards, wire transfers, e-wallets, pre-paid cards, cryptocurrency exchanges, and other). All available methods are listed on the Company's webpage.

The Company strictly monitors all the top-ups and withdrawals, and decline the transaction in the following cases:

- If the account is used not with the aim to make bets;
- If the customer tries to top-up the account and then to withdraw funds without making a bet;
- If the customer tries to transfer funds between the payment systems;
- If the customer tries to top-up the account or withdraw the funds using the wallet that belongs to other person

As also the Company keeps under increased monitoring the following situations:

- The deposit or withdrawal of funds in amounts which fall consistently just below identification or reporting thresholds.
- The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.
- The deposit or withdrawal of multiple monetary instruments (FIAT, crypto funds) at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.
- If the customer suddenly begun to deposit/to withdraw large amounts, that are not within his profile or not corresponds to his occupation.

Withdrawal is possible only to the account from which the betting account was replenished.

□

Any transfers between users' accounts are not possible.

Customers characteristics and behaviors analysis

- The name of the customer was already used for the registration of another account, using the same or slightly different spelling.
- Shared address for individuals, when different customers state the same residency address.
- Stated occupation of the customer is not commensurate with the level or type of activity (for example, a student or an unemployed individual who replenishes the account with large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transactions linked to locations of concern

- Replenishing the account or withdrawing the funds from and/or to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).
- The opening of account from locations of specific concern.⁵

Transactions record keeping

The Company maintains records, containing the information and documentation necessary to decide whether the objective of the CDD measures was met, and to establish the background and purpose of transactions, for at least five years after the business relationship is ended, or after the date of the occasional transaction⁶.

The records must allow to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as provide, if necessary, evidence for prosecution of criminal activity.

The records that are obtained through e.g., CDD measures:

- copy of identification documents;
- name;
- address and place of residence of the client;

⁵ <https://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf>

⁶ Implementation of art. 7, paragraphs 1 and 3, of the NOIS and FATF Recommendation 11

- the nature, number and date and place of issue of the identification document;
the nature of the service;
- the nature, origin, destination, the size and other unique features of the values involved;
- individual transactions;
- member account files; and
- business correspondence, including the results of any analysis undertaken.

The Company is required to maintain numbered accounts in such a way that full compliance can be achieved with the FATF Recommendations.

Transactions thresholds

The designated threshold for transactions is USD 3,000. Transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

The threshold was set based on FATF Recommendation 22 and Regulations for AntiMoney Laundering and Combating the Financing of Terrorism (AML/CFT) issued by GCB. [Reporting of unusual transactions](#)

The Curaçao AML/CTF-legislation defines the circumstances that indicate whether a transaction must be deemed unusual. These circumstances are referred to as "indicators". Unusual transactions must be reported to the Curaçao Financial Intelligence Unit (FIU Curaçao). This applies to executed transactions as well as proposed transactions. FIU Curaçao determines if the reported transaction should also be categorized as a suspicious transaction.⁷

[Suspicious transactions indicators](#)

A transaction is deemed unusual if one or more indicators apply. Indicators can be objective or subjective.

Subjective indicators are dependent on the opinion of the service provider. If he believes that the circumstances surrounding the transaction coincide with those described in the indicator, the transaction is unusual and reporting is mandatory.

Objective indicators are not open to interpretation and rely on hard facts, for instance whether the lower limit for the transaction amount is exceeded, if a client's name appears on certain lists, or whether the transaction has been reported to the police in connection with money laundering. When an objective indicator applies, the transaction must be deemed unusual and reported to the FIU.

For the Company sector, the lottery sector and providers of internet gambling, Curaçao

⁷ <https://www.gamingcontrolcuracao.org/regulatory-scope>

□

AML-regulation, The Decree Indicators Unusual Transactions [“Regeling Indicatoren Ongebruikelijke Transacties” (PB 2015, no. 73), Annex F] has set three (3) objective indicators and one (1) subjective indicator. In addition to these indicators, the GCB can issue guidelines, indicating red flag-situations pertinent to the gaming business.

For the Company sector, the lottery sector and providers of internet gambling, the following indicators apply at the transactional level:

Objective indicators	Subjective indicators
A transaction that is reported to the police or the judicial authorities in connection with money laundering or the financing of terrorism.	Transactions that give reason to assume they could be related to money laundering or to the financing of terrorism.
A proposed transaction by or for the benefit of a natural person, legal person, group or entity, whose name appears on a list that has been drawn up pursuant to the Sanctions National Ordinance.	
A transaction of the value of NAf 5,000 or more (or its equivalent in foreign currency), regardless of the method of payment, be it cash, by check or other form of payment, or electronically or by another non-physical way. This includes amongst others: 1. a transfer from the bank account of the service provider to a local or international bank account at the request of the client; 2. taking funds in deposit or releasing funds held in deposit at the request of a client; 3. Selling tokens (which includes chips and credits) to a client; and 4. Pay-out of prize money. In the event multiple Company patrons appear to be acting in unison, the amounts of their individual transactions shall be added together to evaluate whether the transactions need to be reported according to the NORUT.	

Source: www.gamingcontrolcuracao.org

By virtue of art. 11, third paragraph, of the NORUT, the Company shall examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose, in order to decide whether or not to report the transactions as unusual transaction to the FIU.⁸

The Company shall maintain records, containing the information and documentation necessary to decide whether or not to report the transaction or pattern of transactions to the FIU, for at least five years after the business relationship is ended, or after the date of the occasional transaction or transaction pattern). Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity. Such records shall be made readily available at the request of the Gaming Control Board.

Reporting form

The Company shall record each unusual transaction individually on a Reporting Form. Individual Reporting Forms are numbered sequentially. Any Reporting Form that is voided shall be retained by the Company.

Each report about an unusual transaction will include at least the following information:

- a. the identity of the client;
- b. nature and number of the identification document of the client;
- c. the nature, date, time and place of transaction;
- d. the amount, destination and origin of the funds, securities, precious metals, or other values involved in the transaction;
- e. the circumstances that identified the transaction as unusual.

In case of manual reporting to the FIU (I.e. reporting by non-electronic means), the following items must be added:

- a. Reporting code;
- b. Date and time of the report;
- c. Amount of the transaction, including the currency in which it is to be executed;
- d. In case of non-cash transactions, the bank(s) and account number(s) the client wishes to use in the transaction;
- e. Whether or not the Company executed the transaction;
- f. Any other relevant facts or circumstances pertaining to the client or the proposed transaction.

Then the Compliance Officer should sign the Reporting Form if it is submitted manually.

⁸ Implementation of art. 11, par. 3, of the NORUT

The Company will not conclude the unusual transaction if the information, necessary for the report, cannot be obtained or if the objective of the CDD measures⁹ was not met.

The Company should report to the FIU within 48 hours the details of the transaction as recorded on the Reporting Form. The Company can use an electronic system approved by the FIU for this purpose, or submit a paper copy of the Reporting Form. Submission of paper forms shall not be done by fax for the purpose of data security. In either case, the Company will retain a copy of the Reporting Form for its own records, which are available to GCB upon request.

Submission of Reporting Forms will be confirmed in a confirmation letter from the Company to the FIU, which references only the transaction numbers of the submitted Reporting Forms. The FIU shall confirm receipt of confirmation letters by means of a stamped, signed and dated return of the confirmation letter. This letter confirms receipt of the corresponding Reporting Forms and serves as indemnification in a civil or criminal procedure. The Company shall file such letter with the copy of the original Reporting Form.

The Unusual transactions report can be submitted through the FIU official webpage.

Main indicators and their definitions for UTR can be found at FIU [webpage](#).

Staff training

In order to comply with the regulation, as also to decrease the possibility of money laundering and terrorism financing through the Company's services, the Company initiates staff training. Staff must be trained in accordance with their role and level/nature of responsibilities. The staff that will need to be trained are

- accounting staff,
- finance department,
- fraud management department,
- information technology department,
- customer services staff, □ compliance staff.

Individuals who have responsibilities to monitor or approve transactions in connection with the gambling receive more comprehensive training.

During the training the Company introduces this policy principles to the employees.

There is a mandatory training for all the new employees. New staff is educated in the importance of KYC policies and the basic requirements at the Company. Training for the current staff supposed to be held no less than once per year or more often if necessary.

⁹ Art. 2, par. 2, of the NOIS and FATF Recommendation 10

Explicit responsibility is allocated within the organization for ensuring that the Company's policies and procedures are managed effectively and are in accordance with local supervisory practice.

The channels for reporting suspicious transactions are clearly specified and communicated to all personnel.

High risk and prohibited jurisdictions

The Company pays particular attention to clients and transactions performed by natural persons that reside in countries with strategic deficiencies in the fight against money laundering and terrorist financing¹⁰.

In order to decrease ML/TF risks the Company in addition evaluates each customer based on the geographical location and residency. As of the guide for high-risk jurisdictions, the Company uses FATF high risk and other monitored jurisdictions publications, as also EU highrisk third countries list.

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the "black list".¹¹

The Company does not provide any services to the FATF "black listed" countries, i.e.

- Democratic People's Republic of Korea (DPRK)
- Iran

The Company may provide its services to the countries that are under increased monitoring and are so called FATF "grey list" jurisdictions, if the service is allowed in the place of residence of the customer. However, the customers from the "grey list" territories are considered as highrisk customers and are reviewed based on EDD principles. The same applies for EU high-risk third countries (excl. DPRK and Iran).

Sanctions compliance

The Company is required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update its AML/CFT policy and procedures accordingly to reflect such

¹⁰ NOIS 5i

¹¹<https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2025.html?utm>

amendments. Such information contains lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in.¹²

The Company does not provide any services to the sanctioned entities or individuals. In order to comply, the Company is going to obtain the sanctions screening tool. Currently the Company uses open sanctions screening tools, that are available in the open sources, such as:

- [OFAC Sanctions list search](#);
- [UN Security Council Consolidated List Search](#);
- [EU Sanctions lists](#).

Risk assessment

According to FATF Recommendations, Designated nonfinancial businesses and professions (DNFBPs) are required to take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities.

Taking into account the abovementioned recommendation as also Risk Based Approach Guidance for Companies¹³, the Company has developed its and described its risk assessment policy below.

First of all the risks were divided into main risk categories associated with the business activities of the Company.

Geographic risk

As was already stated in the previous section of this policy, some countries pose an inherently higher ML/TF risk than others. Customers that are associated with higher risk countries, as a result of their citizenship or country of residence, are evaluated based on enhanced due diligence principles. In addition, since the Company provides its services remotely, it ensures that IP locations of the customers are being checked.

Customer risk

Determining the potential money laundering or terrorist financing risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework.

Categories of customers whose activities may indicate a higher risk include: □

Customers that are PEPs;

¹² https://gamingcontrol.spin-cdn.com/media/Company/20191111_aml_cft_regulations_aug_2016.pdf

¹³ <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-tcpsps.html?utm>

- High spenders. Customers may become high spenders because of their cumulative spending over a period of time or casual customers who gamble a relatively large amount of money on a limited number of occasions, perhaps even during a single visit, could equally be considered as high spenders. In both cases, an additional EDD should be performed, and source of funds requested.
- Disproportionate spenders. When the threshold is exceeded, the Company performs repeated due diligence, where AML analyst evaluates information about the client and defines whether high value gambling is consistent with a Company's information about customer's known level or sources of assets (e.g., a customer's bank account) and/or income. If and when this information is obtained it may assist in assessing whether a customer's level of gambling is commensurate to her/his assets or level of legitimate income.
- Casual customers. Even regular customers may pose a risk, particularly if their spending pattern changes, e.g., it dramatically increases or their rated play does not fit their playing profile e.g., minimal play.

In order to decrease the customer risk, the Company developed the following risk mitigation rules:

- The Company provides its services only for the physical persons; thus, it decreases the risk of ML/TF using legal entities.
- The Company does not provide its services to Unknown customers.
- The Company does not open several accounts to the same customer.
- It is not possible to open an anonymous account without identification and verification.

Product Service and Transaction risk

The Company also considers operational aspects (i.e., products, services, games, and accounts/account activities) that can be used to facilitate money laundering and terrorist financing activities. The following potential transaction risks can occur:

- Proceeds of crime. However, when money is transferred to a Company, there is a risk that the funds may originate from illegal activities, such as check fraud, credit or debit card fraud, narcotics trafficking, or theft from an employer. In order to mitigate this risk, the Company pays greater attention to high and disproportionate spenders.
- Identity fraud. Details of financial institution accounts may be stolen and used on web sites. Stolen identities may also be successfully used to open financial institutions accounts, and such accounts may also be used on web sites. Internet Provider (IP)

Number checks are useful in preventing criminals from opening multiple Company accounts using stolen identities, using the same computer. Company will be aware of these risks because of the 'charge back' system.

- Pre-paid cards. The customer can use a cash in order to top-up a prepaid card. Company cannot make the same level of cross reference checks on some types of pre-paid cards as they are able to perform on financial institution accounts.
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. However, e-wallets which only accept money from financial institution accounts in the customer's name will not usually pose any greater or lesser money laundering risk than if funds are received directly from the financial institution. However, the Company is aware that when customers make payments into e-wallets from their financial institution accounts, the statements issued by their financial institutions may only record the payment to the e-wallet, not the transaction to the Company. This may be useful for dishonest customers who wish to disguise their gambling.

In order to decrease the transaction risk, the Company developed the following transaction risk mitigation rules:

- Customers are allowed to use their deposit accounts only for gambling purposes. The Company does not allow its customers to withdraw funds without gambling.
- It is not possible to perform inter- account transfers between customers.
- The Company accepts transfers from the licensed financial entities and does not allow topups/withdrawals to/from “black listed” and sanctioned entities and countries.
- The Company follows IP locations of the customers.

The Company adopts different strategies and approaches in the development of risk-based programs which are tailored to mitigate the money laundering and terrorism finance risks. The strategies to manage and mitigate money laundering and terrorist financing risks in a Company were designed to identify or prevent the activity from occurring through a combination of deterrence measures such as:

- Evaluation of customer and transaction risks.
- Management of customer accounts. Customer account's closure in case of misuse of an account.
- Appropriate CDD measures for customers.
- Record keeping to assist criminal investigations.
- Detection, e.g., monitoring for and reporting of suspicious activity.
- Staff training

All these measures were described in this policy above.