



Next To You B.V.

AML & CFT Policy

This document sets out the Company's strategy to combat money laundering, prevent terrorist financing, and keep crime out of gambling.

Version history

Document revision history

Document Name	AML & CFT Policy		
Maintainer:	Fergus Mac Conmara - AML Officer	Approver:	Elena Karaïskou - Head of Legal and Compliance
Status:	Approved	Version:	2.3
		Changes:	Update of list of restricted countries /Update of policy to meet new requirements set out in the Curaçao GCB AML Regulations
		Date:	25/10/2024

Table of contents

1. Introduction.....	4
2. Key Concepts.....	4
3. Applicability and Regulatory framework.....	5
4. AML/CFT Business Risk Assessment.....	6
4.1. Geographical risks.....	7
4.2. Customer risks.....	7
4.3. Transactional Risks.....	8
4.4. Product Risks.....	8
4.5. Operational risks.....	8
4.6. Intermediaries' risks.....	9
5. Customer Acceptance Policy.....	9
5.1. Customer Due Diligence (CDD).....	10
5.2. Acceptable documents.....	11
5.3. Enhanced Due Diligence (EDD).....	12
5.4. Ongoing Monitoring.....	13
6. Governance.....	14
6.1. Management and “the tone from the top”	14
6.2. Training.....	14
6.3. Employee screening.....	14
6.4. Independent Audit Function.....	15
7. Reporting of Suspicious Activity.....	15
7.1. Obligations of the Employee.....	16
7.2. Obligations of the CO.....	16
7.3. Tipping off.....	17
7.4. Failure to disclose.....	17
8. Record Keeping.....	17
9. Anti-Bribery, Anti-Corruption and Whistleblowing.....	18
10. Policy / procedure review.....	18
Appendices A,B and C.....	20

1. Introduction

Next To You B.V. hereafter (NTY B.V.) is committed to the industry goal of keeping crime, and the proceeds of crime out of gambling. Maintaining a safe environment for our customers and our staff is a core pillar of the business.

This document sets out the strategy of NTY B.V. (the “Company” or “NTY B.V.”) to comply with applicable anti-money laundering and counter-terrorism financing (“AML/CFT”) regulations, requirements, and best practices, specifically applicable to the jurisdictions the company operates within, and in line with the company's risk appetite and the risk assessment of the business.

The AML/CFT policy, in conjunction with the AML/CFT Business Risk Assessment (“BRA”), is intended to support the company in its risk assessments and continuous monitoring for potential money laundering (“ML”) and terrorism financing (“TF”).

Specifically, the policy helps the company to:

- Carry out risk assessments and identify areas where there may be a heightened vulnerability to ML/TF;
- Prepare, maintain, and approve written policies, procedures, and controls detailing how the Company manages the risk of ML/TF;
- Review and update the policies, procedures, and controls to reflect changes to the risk landscape and the continuously evolving internal approach to AML
- Provide training and guidance to all employees on how to effectively implement the policies and controls outlined within, and how to monitor the risks and outcomes;
- Ensure that adequate resources, funds, and systems are in place to support the controls needed to identify, assess, and manage AML risks; and
- Monitor the effectiveness and adequacy of the Company's policies and controls, and make improvements where required.

The Policy is in place to ensure a company culture of clear intent, realistic evaluation, and actionable processes, in order to carry out the Company's goals of combating ML/TF.

2. Key Concepts

Money laundering is the process whereby a criminal / or criminal organisation seeks to conceal the true origin of funds or proceeds of crime in order to create the impression that these funds have a legitimate and lawful source.

Money laundering is usually conducted in three stages; (1) placement; where the criminal attempts to insert the proceeds of crime into the financial system, and (2) layering; where the criminal attempts to separate the proceeds of crime from the source and true ownership by a sequence of transactions in order to distort the audit trail and obstruct investigative efforts, followed by (3) integration; the final step where the criminal will introduce the funds with an appearance of being legitimate into the economy, for example; by purchasing real estate, or luxury assets.

Criminal activity can include any kind of conduct that would be a criminal offence in Curaçao or any other country in which NTY B.V. operates, including but not limited to terrorism, drug trafficking, activities of criminal organisations, corruption, fraud theft, and tax evasion or other tax-related offences.

Terrorist financing is where the main focus for concealment is the final destination of the funds, but often also the source in order to dissociate the benefactor of the terrorist organisation, and therefore it may also pass through a process of placement and layering.

Financing of Proliferation of weapons is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

3. Applicability and Regulatory framework

Incorporated and having its statutory seat in Curaçao, the Company is bound by the Curaçao legislation with regard to Anti-Money Laundering and Countering Financing of Terrorism. The local authorities in charge of the supervision of AML- CFT matters for the gaming sector are the Curaçao Gaming Control Board (GCB) (<https://www.gamingcontrolCuraçao.org>) and the local Financial Intelligence Unit 'FIU'.

The Curaçao online gaming industry is licensed and regulated under the National Ordinance on Offshore Games of Hazard (Landsverordening Buitengaatsse Hazardspelen Curaçao), PB 1993, no. 63) and the FIU Curaçao which is the authority supervising adequate reporting of unusual transactions (<http://www.mot.cw/>).

The following ordinances and guidelines are applicable to the Company for the reporting of unusual transactions in Curaçao:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organisations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
- Kingdom Sanction Act (N.G. 2016, no. 54);

- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curaçao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update May 2024.

NTY B.V. checks for amendments to all Decrees and Regulations on a regular basis and updates the policies and procedures accordingly to meet any such changes. Besides these regulatory authorities, the Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ('FATF'), the Caribbean Financial Action Taskforce (CFATF) and the Guidelines and instructions of the European Commission as well as the 6th Directives of the European Union on AML and CFT.

The AML/CFT Policy applies to NTY B.V. and will be communicated to all employees of the licensed entity, NTY B.V., as well as the subsidiaries and sister companies within the group to which NTY B.V. outsources some of its operations, to ensure they are aware of their responsibilities under AML/TF regulation and the policies set out by the company. For each version update, the Policy will be communicated to staff anew. The policy will also be shared with any third party entering into a contract with the Company who has any access to transactional customer data or information which might otherwise present an ML/TF risk.

4. AML/CFT Business Risk Assessment

NTY B.V. ensures an AML/CFT business risk assessment ("BRA") of the business is carried out, assessing the inherent risks in the business, in order to implement and maintain proportionate policies and procedures.

The BRA covers:

- **Geographical Risks:** the characteristics of the country of residence and other geographical risks;
- **Customer Risks:** the general characteristics of the customer;
- **Product risks:** the characteristics of the products and services provided by the company;
- **Transactional risks:** risks connected to specific transactional behaviour;
- **Delivery channels:** the characteristics of intermediaries and interface risks;
- **Operational risks:** including risks connected to staff and the practical implementation of AML/CFT processes.

These risks have been analysed for potential threats to the business from ML/TF and the processing of proceeds of crime from perceived vulnerabilities in the business and the likelihood that they can be exploited for criminal intent. Following this, the likelihood of such risks arising will be analysed, and the impact this will have on the business should this risk factor materialise. Based on this information, the inherent risk can be measured, and proportional controls implemented in order to mitigate these risks.

The BRA is a living document; maintained and updated on a regular basis depending on changes in the business, changes in regulation or new risks identified in ongoing daily tasks and reviews - or as identified by

any supranational, national or sector specific risk assessments issued by regulatory authorities. The BRA, as well as the AML/CFT Policy, will be reviewed and approved by the board on an annual basis, at minimum. The BRA will also be sent for review, should new risks arise with a risk classification that warrants board awareness.

4.1. Geographical risks

Prospecting customers from countries that pose high ML/TF risks which lie outside of the business risk appetite will be blocked from registration and login. The Compliance department reviews the list of accepted countries on a regular basis, in line with certified and credible sources of information regarding the level of ML/TF risks, corruption, political unrest, and countries subject to sanctions (see **Appendix A** for the compiled list of banned countries), embargos or similar measures, countries with no/little AML (FAFT) or providing funding or support for terrorism.

When applying simplified measures for customer knowledge and requesting identity documentation in order to verify the customer, we may also request the nationality and country of birth of the individual in order to support the customer risk assessment. Should the customer appear to be from or linked to a potentially high-risk country (see **Appendix B**), additional verification checks will be carried out by the AML department before allowing the customer to deposit.

4.2. Customer risks

NTY B.V. recognized that risks related to the customer are the highest where it is possible to gamble anonymously, and the company does not allow for this. The remote setup of a gambling operation also carries risk due to the lack of physical meetings with the customer.

Every player is required to register and identify themselves with NTY B.V.. Further details of the KYC process are set out in section 5. A registered account is only allowed to be operated by the registered individual, and we do not allow for third-party use of an account. A customer is only allowed to hold one account with each brand, and an email can only be used once to register. The system is regularly scanned for links between accounts in the registered details.

Screening for Politically Exposed Persons ("PEPs") and Sanctioned Individuals is conducted at intervals using reputable 3rd party software and if a match or potential match should be found the account is placed under full review to also include open source media checks. Depending on the results the account can be immediately frozen (i.e. if found to be a definite sanctioned individual) or escalated to senior management for a decision on whether to continue the business relationship, request EDD or close the account. The Company will not rely solely on open-source information and will make regular contact directly with any customer identified as potentially risky to verify the customer information provided and obtain further documentation where required. Following the initial screening each customer is continuously monitored for any changes to their PEP/Sanctions' status and in instances where a change does occur, the above process is followed.

Additionally, sanctions screening shall be performed on customers at the moment they request to withdraw funds from their accounts and in instances whereby the legislative framework governing sanctions applicable to Curaçao is subject to amendments or expansions. As a company complying with Curaçao legislation, NTY B.V. shall immediately and without prior notice freeze the funds or assets of designated sanctioned persons and entities in accordance with United Nations Security Council resolutions and the European Union's Common Foreign and Security Policy. In such cases, a report shall be filed with the FIU and NTY B.V. shall immediately proceed to freezing the resources of the customer concerned. When and if a match is confirmed by the supervisory organisation, NTY B.V. shall terminate the provision of services to the customer and shall inform the supervisory organisation on the type and amount of the frozen resources and on the actions that are being undertaken to implement the sanctions order or sanction decree on the basis of which the resources have been frozen.

4.3. Transactional Risks

NTY B.V. does not allow for cash payments and does not provide credit to our customers. NTY B.V. does not allow for P2P transfers between accounts.

Based on known indicators of potential ML, NTY B.V. has various tools in place to detect activity that corresponds to potentially suspicious behaviour and analyse the accounts and the transactions therein.

Some of the greatest ML/TF risks are connected to the deposits made into and going from the customer account. The Company therefore employs a closed loop policy, where a payment can only be made to the same method used to deposit. Where a payment method does not allow for a closed loop, we may allow for a withdrawal to another method provided the scenario poses a low risk, where we have sufficiently verified both the customer and the ownership of the payment methods used.

An attempt to withdraw the same amount, which was deposited, can be a sign of layering. We enforce the minimum wagering of x1 of the deposit before any withdrawal is paid out.

NTY B.V. accepts the following payment methods, subject to the usual transactional monitoring applicable to all payment methods:

- All Card types
- Bank Transfers
- E-wallets
- Vouchers

NTY B.V. will not accept the following payment methods:

- Cash
- Cheques
- RDC payments

4.4. Product Risks

The main game offering is RTP-based automated online slot machines ("slots"). NTY B.V. contracts with reputable, licensed, or certified game providers, to ensure the correctness of the game mechanics. All transactions are monitored to detect players that exhibit patterns that differ from the norm.

In the case of tournaments or points-based competitions over one or several RTP-based games, the winner/s are closely monitored by the Fraud team to detect any signs of collusion.

4.5. Operational risks

NTY B.V. employs a combination of automated solutions, and operational procedures in order to create a robust safety net to mitigate the risks connected to ML/TF. The implementation of certain processes and procedures in place to combat ML/TF and keep crime out of the business, relies on human effort, and the knowledge and assertiveness of our staff.

All operational staff are trained in AML/CFT, and the internal procedures put in place to identify, prevent, and mitigate ML/TF risks in the business, taking into consideration the latest approaches adopted in terms of pre-paid cards by using KYC and Source of Funds measures. Within operations, we have implemented a model consisting of "three lines defence", where each function is specialised in an area of customer knowledge measures, with a clear escalation line to CO.

4.6. Intermediaries' risks

NTY B.V. sets out to only contract with credible business partners and employs a risk-based approach in order to evaluate the risk each new business relationship may carry. When onboarding a new client, a risk assessment will be conducted to measure the risk in the relationship and an appropriate level of due diligence will then be carried out based on this risk assessment.

NTY B.V. also gives due consideration to the money laundering risks posed by business-to-business relationships. The assessment of these risks is based, among other things, on the risks posed to NTY B.V. by the jurisdictional location of the third-party, taking into consideration whether the company is based in a country flagged as risky by the UN, the FATF, OFAC or any of the countries NTY B.V. operates in.

Third-party suppliers are required to go through NTY B.V.'s third party due diligence procedure, where NTY B.V. will obtain information including but not limited to;

- Company details
- Licence information and copies of licences
- Directors and legal representatives
- Corporate shareholders
- UBOs
- CCO (when applicable)
- Certification of Incorporation
- Company Memorandum and Articles of Association
- Company AML policy
- Details of any work with high-risk jurisdictions or individuals considered high risk by FIUs or that hold FATF, UN, EU or OFAC sanctions.

For a full list of the third-party due diligence details recorded, please refer to the NTY B.V. Third Party Due Diligence form. This form is reviewed on an annual basis by the CO, and amendments are made where deemed necessary.

5. Customer Acceptance Policy

NTY B.V. customer acceptance policy is based on what is required under law and in line with the Company's risk appetite and the risk assessment of the business. Certain types of individuals will not be accepted as customers, by either being prevented from registering or blocked from using our site, such as:

- Under 18s;
- PEPs. Politically Exposed Persons may be subject to pressure and vulnerable to corruption. It is at the sole discretion of the Management to accept or deny PEPs as customers. The decisions are taken on a case-by-case basis depending on factors such as i) PEP class level. ii) value of transactions history. iii) deposit limits imposed on the account. iv) adverse media checks results and other mitigating factors resulting from full review of the account and available information on the individuals on FATF, UN, EU or OFAC sanctions lists.
- Residents, in countries deemed to be high risk, to measure AML/CFT risk;
- Individuals where we have reason to suspect involvement in ML/TF or other types of criminal activity;
- Self-excluded customers, excluded from our site or any national self-exclusion register available within the licence conditions;

- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent;

Other types of individuals will be investigated before a decision is made whether to block them from using our site, such as :

- Persons who repeatedly attempt to fund their gambling with deposits from business accounts;
- Customers identified as having abnormal amounts of multiple income sources, irregular income streams, high value depositors and disproportionate spenders.
- Customers where an increased risk level in the customer profile for any reason warranted us taking action or terminating the customer relationship.

The risk level will be decided by a combination of automated monitoring matrices and manual account reviews. NTY B.V. utilises its internal country risk assessment to determine the risk level of each country, and from which countries it will and will not accept customers. For full details, please refer to the NTY B.V. Country Risk Assessment.

Active customers are monitored, in terms of behaviours and transactions, and should the risk level in the account increase we may apply enhanced measures for due diligence or terminate the customer relationship. The expected nature of the customer relationship is that of entertainment. Based on this expectation information is collected, and the profile of a player is assessed, in order to identify deviations from the expected customer profile.

For full details of the NTY B.V. AML risk scoring measures, please refer to the NTY B.V. Risk Scoring document.

5.1. Customer Due Diligence (CDD)

At Onboarding stage, the registration process requires the customer to accept the T&Cs expressly prohibiting our services to minors, declare first and last name, date of birth, contact details, home address, country (place of birth and nationality are collected at a later stage for non-low risk customers). The requests for CDD which follow throughout the business relationship are checked against the data provided by the customer to ensure that the identified person is the same as the one who registered.

Customer due diligence is carried out as required by our regulatory obligations in order to sufficiently verify our customers, to be satisfied that the customers are who they say they are; to determine whether customers are acting on behalf of others; and in order to guard the Company against being used for fraud, money laundering or other criminal activity.

NTY B.V. has an obligation to identify the customer when establishing a business relationship and to verify the provided details. As a remote casino operator, we must also apply customer due diligence measures in relation to any transaction whether the transaction is executed in a single operation or in several operations which appear to be linked. The CDD measures to be taken are as follows:

- Identifying the player and verifying that customer's identity using reliable, independent source documents, data or information;
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being

conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

CDD measures are undertaken at intervals; or when the casino has doubts about the veracity or adequacy of previously obtained customer identification data. If the CDD has not been completed, the customer will be blocked from depositing funds into the account or withdrawing funds from the account. If the customer fails to provide the requested documentation at a stage where this is required, the account will be closed after a lapse of 30 days and a subjective unusual activity report will be filed if the risk in the customer relationship calls for this; if there is reasonable ground to suspect ML/TF activity.

CDD measures are also undertaken at any point, regardless of transaction values, when there is suspicion of money laundering or terrorist financing or there is doubt about the veracity or adequacy of previously obtained customer identification data or there is an increase in the customer AML risk score deeming it necessary.

Continuous monitoring is in place to track customer behaviour and where transactions are deemed to be unusual, further investigations are undertaken by the Compliance team. These investigations will include, but not be limited to, the following:

- Inactivity period followed by intense activity
- Game type behaviour and amounts played
- Withdrawals amount against Deposits amounts
- Transactional behaviour
- Payment method used

NTY B.V. may request Source of Funds or Source of Wealth from the customer for AML or social responsibility reasons should the customer exhibit any of the above unusual behavioural patterns, if the employee has concerns or is suspicious about the customer, or for any other AML or social responsibility-based reason.

Source of Funds check: NTY B.V. interprets Source of Funds (SoF) as the origin of the money used to fund the customer's transactions with NTY B.V. NTY B.V. shall establish the bank account or payment method from which the funds were deposited, and the activity involved in generating said funds, such as personal savings, inheritances, and gambling winnings. Where Source of Funds is requested, the employee should verify the documents and should they have any concerns over the source of the funds or the customer's affordability, they will escalate to the CO for further assessment.

Source of Wealth check: NTY B.V. interprets Source of Wealth (SoW) as the total volume of a customer's accumulated wealth, which may include income from employment, business interests, and investments. As with SoF checks, the employee will escalate to the CO should they have any concerns.

5.2. Acceptable documents

The following methods / documents are accepted as a means of verification of identity as long as the document contains photographic evidence of the player, is valid, and not expired:

- Passport
- Driving licence
- National Identification card (photographic)
- Residents Permit

The following methods/documents are accepted as a means of verification of residential address as long as the document contains the current residential address of the player and is no older than three months:

- Recent Utility bill (gas, electricity, water, satellite TV, landline phone bill)

- Government letter
- Local authority council tax bill

NTY B.V. reviews existing records and regularly refreshes the documentation obtained for the purpose of applying CDD measures. Valid Proofs of identity are asked for from the players one month before the expiration of the documentation held by NTY B.V.. Proofs of address are updated on a regular basis notwithstanding the implementation of EDD measures. Jurisdiction specifics are further detailed in appendices, and the CDD measures are further described in the CDD processes and procedures.

5.3. Enhanced Due Diligence (EDD)

Measures of enhanced customer due diligence go beyond that of the CDD. Enhanced measures are warranted especially in cases identified as high risk and should be consistent with the risks identified:

- When a customer or potential customer is a PEP, or a family member or known close associate of a PEP;
- Where the customer is a citizen of a high-risk country;
- Where a transaction is complex and unusually large, or there is an unusual pattern of transactions;
- When the customer makes use of products or performs transactions that may favour anonymity;
- When new products and business practices are introduced, including new delivery mechanisms and the use of new technologies for both new and existing products.
- When the risk profile of the customer is high, and any other case which, by its nature; can present a higher risk of money laundering or terrorist financing;

The EDD measures that NTY B.V. applies in case there is a higher risk of money laundering or terrorist financing include but are not limited to:

- Obtaining information on the reasons for intended or performed transactions;
- Conducting enhanced monitoring of the business relationship, in which the transaction is made, to determine whether that transaction or that relationship appear to be suspicious;
- Obtaining additional information on the intended nature of the business relationship;
- Applying transactional restrictions on an account to ensure the payment methods being used carry less risk
- Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the customer relationship, including greater scrutiny of transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Seeking additional independent, reliable sources to verify information provided by the customer;
- Taking additional measures to better understand the background, ownership and financial situation of the customer, and other parties to the transaction, i.e.: payslips, savings, inheritance, bank statements, etc.

Enhanced measures may range from utilising information available in open sources to obtaining documentation from the customer to establish and verify Source of Wealth (SOW) / Source of Funds (SOF).

The Company will however not rely solely on open-source information and will make regular contact directly with any customer identified as potentially risky in order to verify the customer information provided and obtain further documentation where required. Verbal assurances from the customer should not be considered conclusive; evidence should be requested where applicable. Suspicious activity will be investigated and reported to the relevant FIU, and a decision reviewed and made by the responsible person in regard to terminating the customer relationship.

5.4. Ongoing Monitoring

NTY B.V. conducts ongoing monitoring of the business relationship, including:

- scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the knowledge of the customer and the customer's risk profile;
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying customer due diligence measures up to date.

Customer due diligence measures must also be adopted at other appropriate times to existing customers on a risk-based approach when becoming aware that the circumstances of an existing customer relevant to the risk profile for that customer have changed, such as:

- a change of identity of the customer;
- transactions which are not reasonably consistent with NTY B.V. knowledge of the customer.

Risk assessments of all customers are carried out on an ongoing basis, where the level of customer due diligence will vary depending on the risk profile of the customer.

At NTY B.V. we utilise both automated data reporting and manual reviews to carry out risk assessments of all customers on a risk-based approach. We have implemented an automated risk scoring solution, which evaluates all player activity based on multiple risk flags which could indicate ML/TF activity and assigns a risk score to the customer account where customers with a higher score are subject to manual AML reviews. In addition to this, we also have specific alerts to flag activity that warrants an AML review.

When NTY B.V. conducts ongoing transaction monitoring and notices that a customer's transactions deviate from expected patterns, it shall investigate this unusual activity and, if necessary, determine the source of the funds used. The extent of ongoing monitoring will depend on the customer's risk profile.

a. Risk scoring and alerts

The NTY B.V. AML risk score is based on known indicators of potential ML, enabling the identification and scrutiny of unusual patterns of transactions. The automated score is regularly reviewed and improved to enhance accuracy. In addition to the score, alerts are in place to highlight activity that warrants increased scrutiny.

b. Manual Reviews

Our customer-facing staff, and staff that reviews customer accounts and activity in their daily tasks, are trained to recognise activity that should warrant further investigation and will in these cases submit an internal unusual activity report to the CO for further review.

NTY B.V. implements manual controls further detailed in the AML Review procedures based on the risk level in the account where dedicated staff will review the account and activity therein to evaluate if there is reasonable ground for suspicion or if the activity can be explained with further investigation and measures.

Higher risk customers will also be added to a monitoring list, where dedicated staff will regularly follow up on such customers. If the risk profile of a customer increases beyond the company's risk appetite, and suspicious activity is detected, a report to the FIU will be made and the customer relationship terminated.

NTY B.V. utilises an internal customer risk scoring chart to determine the risk level of its players, prioritising AML reviews on customers scoring 'High'.

6. Governance

In order for ML/TF risk to be properly targeted, it is important to nurture a culture of compliance and make sure the right knowledge and support are consistently present throughout the business.

6.1. Management and “the tone from the top”

Management and the board commit themselves to ensure that a positive cultural attitude toward AML/CFT prevails in the organisation. This will be driven by the encouragement of various initiatives, including setting the tone from the top, by supporting and enabling the continuous operational efforts to combat ML/TF, including sufficient resourcing and appropriate training. This includes not only hiring staff but hiring the most appropriate staff. The business is required to notify the CO of any product changes which may affect the AML policies, such as

changes to deposit limits, registration forms, or any area which may otherwise affect the customer data collected or deposits, withdrawals, and transactional activity.

6.2. Training

All staff, including management, are made aware of the company's obligations under anti-money laundering and counter terrorist financing regulations, and the risks the company faces in relation to this. Training is carried out and adapted to the role and the responsibility of the staff, and a log maintained of the training carried out. The CO has received specialised training fit for the role.

All staff, regardless of their role, are required to pass an initial AML/CFT training course which is reviewed on a bi-annual basis by the CO and amended where necessary to ensure adequacy and consistency with the NTY B.V. AML policy.

The Compliance team will notify the business of any changes to AML requirements, key rulings that may affect the business, and any other AML related information which may otherwise be of note to employees.

6.3. Employee screening

NTY B.V. will only contract with and hire individuals of good standing. When hiring new staff, NTY B.V. makes sure to collect an appropriate level of due diligence to verify the age and identity of a new employee and to allow for background checks. For key positions in the company, responsible for crucial areas within the business, more extensive measures for due diligence are carried out.

The following documentation will be collected from all employees;

- Copy of ID;
- Information on employment history and references;
- A police conduct report will also be collected to ensure new staff do not have a criminal record.

6.4. Independent Audit Function

NTY B.V. shall be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit shall be performed by sufficiently qualified persons and shall be independent, thus performed by people not involved with the organisation's AML compliance staff. The audit tests shall include at a minimum:

- An evaluation of the institution's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The testing scope and results shall be documented. Any deficiencies are to be reported to senior management and the designated officers, with a request for prompt corrective actions to be taken by a specified deadline. The audit will also consider whether senior management was responsive to earlier audit findings.

7. Reporting of Suspicious Activity

NTY B.V. will continuously monitor ongoing business relationships and examine individual transactions to detect activities or transactions that are suspicious or inconsistent with what is known about the customer. If any employee has any suspicions about the activity or transactions of any customer, they will report it immediately to the CO.

The CO will then assess the activity and determine whether an unusual Activity Report is required and if so, will immediately report it to the relevant Financial Intelligence Unit (FIU).

NTY B.V. utilises an Unusual Transactions Report template, according to the Curaçao Law and Regulations, to inform the relevant FIU of such activities or transactions with details including but not limited to; customer's information, IP address, account balance, dates and details of the suspicious activity, details of the investigation, payment methods used, card details, deposits and withdrawal and verification document details. For a comprehensive list of the details submitted as part of these reports, refer to the NTY B.V. Suspicious Transactions Report template (see Appendix C).

7.1. Obligations of the Employee

Employees of NTY B.V., following the given training, will report to the CO without delay any suspicions found during the functions inherent in their position within each operational department. As stated in the KYC Procedures, this is set up by NTY B.V. as the first line of defence (e.g.: manual AML Alerts raised by the operational team within NTY B.V., including but not limited to; customer refusal to provide proof of identity, sudden change of playing pattern, abnormal deposit pattern, frequent and not explained change of payment methods, stacking deposits without clear intention to play, forged documents provided by the customer, criminal mindset).

7.2. Obligations of the CO

The Nominated Officer shall consider any internal report (or any suspicion found in his reviews) and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a customer is engaged in money laundering or terrorist financing. If so, the Nominated Officer shall submit a report to the Financial Intelligence Unit (FIU). In any case, when a report is escalated, and submitted as subjective, NTY B.V. will aim at ending the business relationship with the concerned customer. Whenever reporting, NTY B.V. will therefore request defences (appropriate consents) from the FIU to close the player accounts and potentially proceed with withdrawals pending thereon. Without being granted an appropriate consent by the FIU, NTY B.V. will abstain from taking any action that could affect the following investigation.

The CO has responsibility for, among other things:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organise training sessions for the staff on various compliance-related issues;
- To analyse transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements;
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

Furthermore, the CO will appoint an AML Officer to support the implementation of the Policy and serve as a delegate in the event that the CO is absent.

7.3. Tipping off

Tipping off is a criminal offence. If, during the establishment or course of the customer relationship, or when conducting occasional transactions, any employee of NTY B.V. suspects that any transaction or behaviour is related to money laundering or terrorist financing, NTY B.V. prohibits disclosure of this information or of the fact that a report is being escalated to the FIU. A risk exists that customers could be unintentionally tipped off when the company is seeking to perform its obligations in these circumstances. The customer's awareness of a possible report or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation.

7.4. Failure to disclose

Failing to report knowledge, suspicion or when there are grounds to suspect money laundering to the CO as soon as reasonably practicable after the information came to your attention, is a criminal offence. Employees have an obligation to be vigilant and raise any such activity directly to the CO.

Through training and by fostering a culture of accountability in ongoing day to day tasks, employees are kept aware of their obligations to raise any suspicious activity to the CO directly. Employees who do not make an internal report to the CO when knowledge or reasonable suspicion exists, may face criminal sanctions which may include a prison term of up to five years.

8. Record Keeping

NTY B.V. shall maintain records for AML / CFT purposes, for a retention period of 5 years, including:

- copies of any documents and information obtained to satisfy the customer due diligence requirements, and enough supporting records in respect of each transaction which is subject to customer due diligence measures or ongoing monitoring to enable the transaction to be reconstructed.
- Internal and external reports on suspicious activity, including decisions and actions taken, or not taken, by the CO;
- Contact between the Nominated Officer and law enforcement or FIUs, including records connected to requests for a defence (appropriate consent);

Once the retention period has expired, any personal data shall be deleted unless NTY B.V. is required to retain records for a longer period of time for any reason, such as where legislation prescribes a longer retention period. Any laws or regulations on retention periods will supersede periods set out in the NTY B.V. policy.

9. Anti-Bribery, Anti-Corruption and Whistleblowing

NTY B.V. has a zero-tolerance policy on bribery and corruption. The company commits to safeguarding staff and the right to whistleblow. This is further detailed in the Anti-Bribery, Anti-Corruption and Whistleblowing Policy ("ABC Policy").

All employees are, on an annual basis, required to pass an Anti-Bribery, Anti-Corruption and Whistleblowing training course to ensure they are aware of the ABC policy and their obligations as employees. The training course is reviewed on a bi-annual basis by the CO to ensure adequacy and to make amendments where necessary.

10. Policy / procedure review

The departments responsible for designing, monitoring, and updating these internal controls are the CO and the Compliance Team.

The approver of The Policy is the Head of Compliance. In addition to this the Policy will be reviewed and approved by the board on an annual basis at minimum, or in case significant changes are done at a level which warrants a Board approval.

The company will perform an annual assessment on the risks inherent to the products when reviewing the policy. This assessment shall help to update the AML/CFT policy and the related procedures.

The CO and the Compliance Team will review the AML/CFT Policy on an annual basis at minimum, or whenever circumstances change to warrant a review and update of the document as set out by the following criteria:

- Annually, no later than 12 months from the date upon which the Policy was last reviewed;
- upon the discovery or recognition by an audit or risk assessment that the Policy requires amendment;
- upon the change of any relevant law or regulation which applies to the Policy;
- upon the finding by any regulator that an amendment to the Policy is required;
- upon the award of any new gambling licence in any new jurisdiction;
- upon the acceptance of customers from a jurisdiction / territory where the company did not previously accept customers;
- Upon acquiring a new product / vertical;
- Whenever significant changes occur in the business, that will have a direct or indirect impact on the area this document concerns.

Any amendment of the Policy shall, as soon as is reasonably practicable, be distributed or informed to all persons within the scope of the Policy for information of the amendment. Any change in Policy giving rise to a Procedure review shall be identified and such changes shall be implemented to the relevant Procedure. The Policy approver is responsible for making sure that the Policy is reviewed and updated on a regular basis.

NTY B.V. uses an adequately resourced internal audit department to monitor and evaluate the AML compliance program on an annual basis along with an accredited external auditor to perform an analysis of its internal AML procedures and their adherence to this policy as well as to the applicable regulations. The external audit should occur once every three years at minimum.

Signature :

DocuSigned by:

F14EF6F4354F4D8...

Name : Elena Karaiskou

Position : Compliance officer

Date : 10/28/2024

APPENDIX A

Below is the compiled list of countries/jurisdictions that present AML/CFT strategic deficiencies; however, it is not exhaustive and might also include other countries/jurisdictions that may be subject to restrictive measures (e.g., change in the FATF's Increased Monitoring / Call for Action Lists, and/or countries/jurisdictions with other AML / CFT shortcomings etc.). *Changes to Appendix A and B can be frequent and are not considered material changes and therefore do not require new document versions or additional sign-off.

- Bulgaria
- Burkina Faso
- Cameroon
- Croatia
- Democratic Republic of the Congo
- Haiti
- Kenya
- Mali
- Monaco
- Mozambique
- Namibia
- Nigeria
- Philippines
- Senegal
- South Africa
- South Sudan
- Syria
- Tanzania
- Venezuela
- Vietnam
- Yemen

- Iran (black-listed)
- North Korea - Democratic People's Republic of Korea (black-listed)
- Myanmar (black-listed)

APPENDIX B

Below is the compiled list of countries/jurisdictions that are subject to limitations of the applicability of NTY B.V.'s international licence; however, it is not exhaustive and might also include other countries/jurisdictions that fall under these market and/or licence applicability restrictions.

- Afghanistan
- American Samoa
- Aruba
- Austria
- Belize
- Belgium
- Bonaire
- Bosnia and Herzegovina
- Burma
- Burundi
- Central African Republic
- Curaçao
- Denmark
- Democratic Republic of the Congo
- Egypt
- Eritrea
- Estonia
- Germany
- Greece
- Greenland
- Guam
- Holy See (Vatican City)
- Italy
- Iraq
- ISIL and Al-Qaida
- Ivory Coast
- Lebanon
- Libya
- Lithuania
- Kuwait
- Malaysia
- Marshall Islands
- Maldives
- Netherlands
- Occupied Palestinian Territory
- Poland
- Puerto Rico
- Qatar
- Republic of Guinea
- Republic of Guinea-Bissau

- Russian Federation
- Saba
- Singapore
- Spain
- Somalia
- St. Eustatius
- St. Maarten
- Sudan
- Sweden
- Tunisia
- USA
- US Minor Outlying Islands
- US Virgin Islands
- Venezuela
- Zimbabwe

APPENDIX C

The below template consists of the NTY B.V.'s Internal Disclosure Form where employees are obliged to use and submit to the CO function at the mlro@tlf.com when they spot or suspect any suspicious activity and/or transactions.



Date:

Next To You B.V.

INTERNAL DISCLOSURE FORM

The following Suspicious Transaction Report is used to report any suspicious activity including suspicions of Money Laundering or Funding of Terrorism.

For internal use only | Property of Next To You B.V.

1
version

No reproduction / no distribution / no printed



Date:

Part 1: Registration Details

AccountID	
First Name	
Last Name	
Email address	
Email Address Verified [STRIKETHROUGH IF IRRELEVANT]	Yes / No
Residential Address	
Date of Birth	
Phone Number	
Phone Number Verified [STRIKETHROUGH IF IRRELEVANT]	Yes / No

Date / Time	
IP	
IP Location	
ISP	
User Agent	

For internal use only

Property of Next To You B.V.

2
version

No reproduction / no distribution / no printed



Date:

Closure Date [IF CLOSED]	
Closure Balance	

Part 2: Suspicious Activity Information

Date or Date range	
Type [STRIKETHROUGH IF IRRELEVANT]	- Money Laundering - Funding of Terrorism - Forged documentation - Bonus Abuse - Collusion / Irregular Gameplay — Credit or Debit Card Fraud
Details of the suspicious activity	
User acted alone or in a group [STRIKETHROUGH IF IRRELEVANT]	- Alone — In a group
Account IDs	



Date:

How did the investigation start? [STRIKETHROUGH IF IRRELEVANT]	- Internal Monitoring - Unusual transactions / gaming behaviour - Reported by the issuing bank - Reported by an E-wallet provider - Reported by the police/FIU/Competent Authorities - Reported by the licence issuer
3rd parties informed [STRIKETHROUGH IF IRRELEVANT]	- None - Issuing bank - E-wallet provider - Police/FIU/Competent Authorities - Licence Issuer

Part 3: Payment Details

Account Currency	
Payment Methods used to deposit [STRIKETHROUGH IF IRRELEVANT]	Debit Cards (VISA / Mastercard): - Emerchantpay - EMP Corp - Payabl - Paysend E-wallet providers: - Skrill - Neteller - MuchBetter - Ecopayz - EzeWallet Bank Transfers (Instant / online banking): - Interac - Volt

For internal use only

Property of Next To You B.V.

4

version

No reproduction / no distribution / no printed



Date:

	- iDebit - Instadebit
	Vouchers: - PaysafeCard - Cashlib - Neosurf - Flexepin
Payment Methods used to withdraw [STRIKETHROUGH IF IRRELEVANT]	Debit Cards (VISA / Mastercard): - Emerchantpay - EMP Corp - Payabl - Paysend
	E-wallet providers: - Skrill - Neteller - MuchBetter - Ecopayz - Ezeewallet
	Bank Transfers (Instant / online banking): - Interac - Volt - iDebit - Instadebit

Debit Card Details:	
Card Number	
Card Name	
Expiry Date	

5

For internal use only | Property of Next To You B.V.

version

No reproduction / no distribution / no printed



Date:

Issuing Bank	
Issuing Country	

E-Wallet Details:	
E-wallet Account Number	
E-wallet First Name	
E-wallet Last Name	
E-wallet email address	

Chargeback/RFI received	Yes / No
-------------------------	----------

Part 4: Deposits and Withdrawals Details

Total Deposits:	
Total withdrawals:	

Deposit Amount	Deposit Date / Time	Deposit IP	Deposit User Agent

For internal use only

Property of Next To You B.V.

6
version

No reproduction / no distribution / no printed



Date:

Withdrawal Amount	Withdrawal Date / Time	Withdrawal IP	Withdrawal User Agent

Part 5: Account Verification

Documents requested [SPECIFY REQUESTED DOCUMENTS]	
Documents received [SPECIFY RECEIVED DOCUMENTS]	

Social Network and Online Search	Yes / No
Links [INSERT LINKS SEARCHED]	

Customer communication	Yes / No
Relevant customer communication [INSERT CUSTOMER	

For internal use only

Property of Next To You B.V.

7
version

No reproduction / no distribution / no printed



Date:

COMMUNICATION]

Part 6: Gaming Activity

Games Played [STRIKETHROUGH IF IRRELEVANT]	- Slot Games - Live Table Games
Gameplay Review	

For internal use only

Property of Next To You B.V.

8
version

No reproduction / no distribution / no printed