

Clover Leaf B.V. Anti-Money Laundering (AML)

Policy (Version 1.4)

EFFECTIVE: MAY 16, 2025

TABLE OF CONTENTS

	Page
I. Policy Statement	1
II. Purpose.....	2
III. Audience	3
IV. Definitions.....	4
V. Policy Implementation	4
II. Information Sharing.....	15
III. Program Administration.....	15
IV. Employee Training and Reporting Guide	16
V. Ownership	18
VI. Governance & Oversight	18
VII. Compliance and Consequences of Non-Compliance.....	19
VIII. Related Documents / Resources.....	20
IX. Questions / Contact Information.....	20

Key Information

Policy Owner	Frank Nonnenmacher
Approving Official(s)	Bryan Weisgal; HBM Group
Responsible Office	Legal and Compliance Department
Effective Date	June 1, 2025
Next Review Date	December 1, 2025

Version History

Version	Date	Description Changes	Revised By	Classification
1.1	3/15/2024	Initial Draft	Frank Nonnenmacher	Internal, Confidential
1.2	5/29/2024	Draft for Launch of MyPrize.com	Frank Nonnenmacher	Live in Beta
1.3	8/1/2024	Revised August 1, 2024 for clean-up and to reflect updated additional controls	Frank Nonnenmacher	Update
1.4	6/1/2025	Annual revision and submission to CGA Portal	Frank Nonnenmacher	Update & Submission to Portal

I. Policy Statement

Clover Leaf B.V.. and its affiliates and subsidiaries (also collectively known as “**MyPrize**” or the “**Company**”) has established, documented and maintains an Anti-Money Laundering (“**AML**”) Program to prohibit and actively prevent money laundering and any activity that facilitates money laundering, the funding of terrorism, or criminal activities by complying with all applicable requirements under the Sanction National Ordinance and the Kingdom Sanction Act and supporting regulations, including without limitation the National Ordinance on Identification (NOIS and National Ordinance on Reporting Unusual Transactions (collectively, known and referred to as the “Regulations”).

To remain within compliance of the Regulations, MyPrize follows the guidance of the leading AML guidance and enforcement programs throughout the world, most notably the U.S. Bank Secrecy Act, which imposes a duty on financial institutions to identify and report potential money laundering activity, terrorist financing, illegal activities, and certain other unusual transactions conducted by or through the business, and also to make and retain certain records regarding customers, transactions and accounts.

Over time, a number of additional statutes and regulations have been enacted across regulatory frameworks that expand and strengthen the scope of enforcement powers with regard to the Regulations. Together, these statutes and regulations place a number of responsibilities on financial institutions, such as: (i) identifying their customers and evaluating the risks of performing transactions for them; (ii) monitoring for unusual or unexpected activity investigation such activity, and alerting the authorities to such activity when appropriate; and (iii) screening transaction participants against various sanctions lists maintained by enforcement agencies.

The Company is committed to implementing and upholding an AML program influenced by the CGA’s guidance and the BSA’s prescribed pillars in order to mitigate AML risks. Under a risk-based BSA/AML program, there are five (5) minimum requirements referred to as “pillars”:

- Pillar 1: A senior compliance officer (or Chief Compliance Officer or BSA Officer) (“**AML Compliance Person**”) having sufficient knowledge, authority, and resources to oversee the company’s AML program.
- Pillar 2: A risk-based written compliance program consisting of policies, procedures, and internal controls that is reasonably designed to prevent the business from being used to facilitate money laundering and other criminal activity and to ensure compliance with applicable reporting requirements.
- Pillar 3: An AML training program for employees that includes both training for new personal and annual training for all employees;
- Pillar 4: A periodic independent review of the company’s performance in carrying out its AML compliance obligations.
- Pillar 5: Customer due diligence, including customer identification and verification, beneficial ownership identification and verification, and understanding the purpose and nature of customer relationships to develop a customer risk profile.

The company has designed its AML policies and programs (collectively, the “**Program**”) based on the Company’s risks, in order to provide the framework for effective compliance with BSA/CGA guidance and also broader Regulations, and to communicate the Company’s clear commitment to creating a strong compliance culture for the Company’s staff. The Program is established in order to promote the Company’s compliance with applicable laws and regulations, to identify and prevent money-laundering, and to facilitate the reporting of unusual activity and to otherwise support the Company’s compliance with any applicable reporting responsibilities.

The Program is designed to address any risks and regulations related to all of the Company’s payment, withdrawal, purchase, and redemption transactions, whether such transactions are made in fiat currency, crypto currency, or any other items of value, the Company engages 3rd party contractors and trains its personnel, including its employees to track and ensure that no employees, users or other stakeholders are engaging in money laundering or other financial crimes.

II. Purpose

It is the policy of the Company to comply with all applicable laws and regulations concerning money laundering and the financing of terrorism, whether in fiat or crypto currency, and to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities, and were unable to be prevented, to report such activity to the relevant authorities in accordance with the Company’s legal obligations. The Company also implements the proper procedures and controls to ensure the compliance with these requirements. The Company’s policies and internal controls are designed to ensure compliance with relevant regulations regarding AML, including the BSA and CGA and its implementing regulations, and will be reviewed and updated on the periodic basis to account for changes in regulations and changes in the company’s business model. The Program is designed based on the Company’s risk profile. The Program is intended to address these risks and to communicate the Company’s clean commitment to creating a strong compliance culture to the Company’s staff.

Specifically, the Program and its implementing procedures are designed to:

- i. Outline applicable regulations and key provisions;
- ii. Outline the potential risks and consequences of non-compliance;
- iii. Outline the Company’s AML and Sanctions internal controls;
- iv. Ensure the Company documents efforts to meet its legal and regulatory obligations;
- v. Ensure compliance training is provided to all staff members, as appropriate;
- vi. Ensure periodic compliance quality assurance and independent testing and review; and
- vii. Ensure regular reporting to Executive Management, the Company’s Directors, and the Company’s AML and Sanctions officers and reporting protocols.

This Policy is designed to ensure full compliance with the following laws and regulations and any further acts issued in pursuance thereof:

- The National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (NOIS) (N.G. 2017 no. 92);
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- 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);
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99);
- Regulatory requirements of the Financial Intelligence Unit (FIU) Curaçao;
- Sanction National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction;
- International standards issued by the Financial Action Task Force (FATF).
- Curacao Gaming Control Board's Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, January 2025

III. Audience

This Program applies to all activities, services, products, and Employees of the Company, including the Company's officers, directors, full-time Employees, part-time Employees, temporary Employees, or contractors employed by the Company or affiliates of the Company, as well as the Company's third-party service providers as relevant. Such individuals will be provided with regular training to ensure awareness of this policy and their obligations under it, at least on an annual basis or more frequently as required. All employees are also expected to familiarize themselves with the third-party vendors engaged by the Company to assist in AML activities related to fiat currency and crypto currency. The Company processes transactions in crypto currency, and intends to process transactions via credit card and other forms of fiat currency; to these endeavors, the Policy and Program is intended to address the scope and breadth of all such transactions and ensure that the Company does not engage, foster, aid, or otherwise encounter any forms of illicit money laundering or terrorism financing.

IV. Definitions

A. **Money Laundering** can be defined as engaging in acts designed to obfuscate the true origins of criminally derived proceeds in order for the proceeds to appear to have originated by legitimate means, or for the assets themselves to appear legitimate. Money laundering may occur every time a transaction happens or when any relationship is established that involves any type of property that has been obtained through crime. Money laundering is understood to occur in three stages. First, criminally derived proceeds enter the financial system in the “placement” stage, during which funds are deposited into bank (or other types of) accounts by checks, money orders, or cash. Second, in the “layering” stage, the funds are transferred to other accounts at the same or other (financial) institutions to further distance the funds from their criminal origin. Lastly, in the “integration” stage, the funds are used for legitimate or illegitimate purposes, such as to purchase legitimate assets, fund legitimate businesses, or to fund other criminal activities. These three stages do not always reflect reality, as not all crime generates cash and therefore any form of property can take part in money laundering. Generally, any contribution to this process, by dealing in some way with assets that are known or suspected to come from crime, is a money laundering offense. Therefore, each of the above stages would be considered money laundering on its own.

B. **Terrorist Financing** may involve obfuscating the origin of criminal proceeds, however, it may also consist of concealing the intended use of funds, which could be for criminal purposes. In other words, terrorist financing may involve originally legitimate funds that are planned to be for criminal purposes. The legitimate source of funds may be from any source, including charitable donations, foreign government sponsors, businesses, and personal employment. Essentially, terrorist financing involves raising, holding, or moving funds – lawfully or criminally obtained – for terrorist purposes. It is important to note that terrorist attacks are not necessarily costly, and thus transactions associated with terrorist financing may be in small amounts and not particularly complex. Lastly, the actual methods used by those laundering funds and those conducting terrorist financing may be similar.

V. Policy Implementation

The Company will follow applicable directives issued in conjunction with the necessary regulatory bodies to prevent money laundering, terrorist financing, sanction violations, and other criminal activity. The Company will not engage in activities related to money laundering, terrorist financing, or involving any person or business who is under US, UN, or EU sanctions or a partner’s prohibited countries or watchlists or involving any country or region subject to comprehensive US sanctions. The Company has a four-stage risk-based approach to combatting money laundering, terrorist financing, sanctions violations, and other criminal activity:

A. **Identification:** Identifying the Company’s products and services could be used for money laundering and/or terrorist financing;

B. **Documentation:** Ensuring that the Company has clear and well documented policies and procedures in place for employees to understand the risks, to know what to look for, and to know how to report any unusual activity;

C. **Mitigation:** Implementing strong measures and defense mechanisms to prevent money laundering, terrorist financing, and other criminal activity from occurring in the first place or enabling the Company to detect and report such occurrences if they do happen; and

D. **Monitoring:** Closely monitoring identified risks and mitigating them by using the established measures on an ongoing basis and, where necessary, adjusting to any changes.

VI. Business Risk Assessment

The Company conducts a comprehensive Business Risk Assessment (BRA) to identify and evaluate its exposure to money laundering (ML), terrorism financing (TF), and sanctions risks. The assessment ensures that AML/CFT controls are commensurate with the risks associated with the Company's operations, products, services, customer base, and geographical footprint.

The BRA is reviewed annually and upon any material change to business operations or regulatory obligations. The BRA includes the following key areas:

Product and Service Risk: Evaluation of the ML/TF risks inherent in the Company's gaming offerings (e.g., online poker, sports betting, and virtual currency). Particular focus is placed on features allowing for rapid fund movement or cashout without proportional gameplay.

Customer Risk: Classification of customers by risk levels based on geographic origin, payment behavior, funding methods, and whether they are high-net-worth individuals, Politically Exposed Persons (PEPs), or associated with high-risk industries.

Geographic Risk: Analysis of exposure to countries listed by FATF, OFAC, or other relevant authorities as non-cooperative or high-risk, as well as jurisdictions with weak AML/CFT systems or under international sanctions.

Transactional Behavior Risk: Detection of patterns such as minimal gaming activity before large withdrawals, unusual use of bonuses, or frequent account top-ups followed by inactivity.

Findings from the BRA are documented and used to inform risk-based procedures and customer due diligence protocols. The effectiveness of controls derived from this assessment is validated through internal audits, transaction monitoring results, and independent testing.

VII. Customer Risk Assessment

The Customer Risk Assessment (CRA) is an essential element of the Company's risk-based approach, aimed at evaluating the ML/TF risk posed by individual customers. It informs the level of due diligence, ongoing monitoring, and other controls applied to each customer.

Each customer is assigned a risk rating (Low, Medium, High, or Very High) based on a set of risk indicators:

Identification and Verification Data: Including full name, address, date of birth, and documentary or non-documentary verification.

Behavioral Factors: Transaction volumes, frequency of deposits and withdrawals, and patterns of gameplay versus monetary activity.

Geographic Indicators: Whether the customer is based in or connected to high-risk or sanctioned jurisdictions.

Payment and Funding Sources: Use of crypto-assets, pre-paid cards, or anonymous funding methods increase risk; documented employment income or regulated bank transfers lower risk.

Third-party Data: Alerts or insights from vendors such as Sardine A.I. (sanctions and PEP screening) and Chainalysis (blockchain transaction tracing).

CRA is initiated at account creation and continuously updated based on the customer's activity and external inputs. Triggers for re-evaluation include:

- Cumulative deposits exceeding defined thresholds (e.g., \$2,000 or Cg.4,000, whichever is less).
- Document KYC Verification.
- Attempted withdrawals or redemptions.
- Alerts from internal or third-party systems.

High-risk customers undergo Enhanced Due Diligence (EDD), including documentation on source of wealth and intended usage of the platform. The CRA informs decisions on whether to escalate accounts, impose restrictions, or file unusual transactions to the FIU.

VIII. Customer Acceptance Policy

The Customer Acceptance Policy (CAP) sets forth the onboarding requirements and thresholds for escalating due diligence procedures based on CRA outcomes. The Company uses a three-tiered Customer Identification and Verification system:

Level 1: Account Creation

Required: Email address.

Purpose: Establish account credentials and provide CIP notification.

Limitations: No monetary transactions permitted.

Level 2: Customer Due Diligence (CDD)

Triggered by: First attempted deposit or wager.

Required Information:

- First and Last Name
- Phone Number
- Full Residential Address (no P.O. Boxes; APO/FPO acceptable)

- Date of Birth
- Government-issued ID Verification (subject to specific policies and management's discretion);

The user-provided information must be verifiable by third-party vendors (including Sardine A.I. and Chainalysis) prior to transacting above the prescribed limits and can be provided in two ways: either as photos of government issues, unexpired IDs/selfie uploads (documentary), or as text inputs (non-documentary) when made available.

Level 3: Enhanced Due Diligence (EDD)

Triggered by:

- Withdrawal attempts or redemptions
- Cumulative deposits exceeding \$2,000 or (Cg. 4,000, whichever is less)
- Behavioral red flags or vendor alerts

Additional Requirements:

- Documentary proof of address (e.g., utility bill or bank statement)
- Source of wealth/income documentation for high-risk accounts, if applicable
- Explanation of transactional behavior or relationships, if applicable

All KYC information must be verifiable via approved third-party providers (e.g., Sardine) before the customer is allowed to transact beyond set limits.

Restricted Jurisdictions

The Company prohibits customers from countries under comprehensive sanctions and on the FATF's High-Risk Jurisdictions subject to a Call for Action list (e.g., Iran, North Korea, Syria, Myanmar) and maintains:

- A Non-Supported Countries List
- A Prohibited Jurisdictions List for monitoring and reference

Account Escalation and Review

High-risk accounts are subject to Compliance approval. PEPs are subject to management approval.

Customers failing to meet verification requirements may be suspended or permanently restricted from transacting.

All customer information and due diligence records are maintained for at least seven years from the date of collection or account closure, whichever is later.

IX. Customer Due Diligence

- i. Customer Due Diligence / Enhanced Due Diligence Implementation – Set forth in this subsection are the levels of information that the Company is required to provide:

- a. Level 1 (Sign Up) ☐ E-Mail
- b. Level 2 (Customer Due Diligence) ☐ First and Last Name, Phone Number, Full Address, Date of Birth, and ID Verification (subject to specific policies and management's discretion);
- c. Level 3 (Enhanced Due Diligence) ☐ Non-Documentary or Documentary Know Your Customer Verification; including:
 - (1) Documentation Supporting the User's Residential Address (NOTE: A Post Office Box shall not be accepted, however an Army Post Office or Fleet Post Office Box Number and/or description of the User's physical location is acceptable); and
 - (2) User's tax information (if applicable) (NOTE: the Company reserves the right to request tax information subject to the advice of the Company's advisors and representatives. From time to time, the Company may request Tax Identification Cards, Passport Numbers, Countries of Issuance, or additional documents of similar like and purpose).

ii. Notification – An important part of the CIP process is notifying the customer of the CIP requirements. It is the policy of the Company to communicate the CIP requirements prior to a submission of personal identifying information for validation.

iii. Balance Limits – Certain KYC information is required when a customer account reaches certain monetary transaction or balance limits and/or conducts certain actions. Additional limits or triggers for customer information verification may be required at the procedural level below these thresholds pursuant to a risk-based approach by the Compliance team. MyPrize utilizes the following conditions to determine when the customer needs to provide additional KYC information to advance to the next account level.

e.g. #1: Triggers that prompt Level 2 Verification include: (x) anytime the Company attempts to deposit funds on MyPrize.com; (y) anytime a User attempts to place a wager on MyPrize.com.

e.g. #2: Triggers that prompt Level 3 Verification include: (x) the Customer attempts to withdraw their balance on MyPrize.com; (y) The Customer's lifetime deposit history on MyPrize.com exceeds \$2,000 (or Cg. 4,000, whichever is less) in volume; or (z) a User's transaction or behavioral history is flagged by one of the Company's Vendors or the Company's internal controls.

X. Ongoing Monitoring

- The Company will conduct ongoing monitoring to identify concerning transactions and, on a risk basis, maintain and update customer information, including information regarding

the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for concerning transaction reporting. The Company will utilize a combination of automated and manual monitoring methods applying internal tools, the vendor reports, and referrals from Partners (card networks, financial institutions, etc.). By monitoring transactional activity through the combined use of technology and manual analysis. The objectives of an effective transaction monitoring process include:

- A. A risk-based monitoring methodology;
- B. A proficient review process;
- C. A competent escalation process; and
- D. The prompt reporting of unusual activity.

The Compliance department will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, and will document when and how this monitoring is carried out. Such reviews will be conducted at the direction of and under the supervision of the AML Compliance Person or his or her designee.

- **Fraud Prevention** – The Company maintains a fraud-prevention program to establish integrity and security for the MyPrize platform. The Company shall collect applicable customer data and utilize a combination of automated and manual monitoring methods, applying internal tools, alerts generated from third-party vendors, and referrals from Partners (card networks, financial institutions, etc). The objectives of an effective fraud prevention process include:

- E. A multi-level approach to preventing illicit activity from the MyPrize platform;
- F. a proficient review process to halt illicit purchases;
- G. an efficient analysis process to identify and flag potential fraud trends; and
- H. identifying any red flags that consist of documents/identification that has been altered or forged to circumvent MyPrize's controls.

The Compliance department will be responsible for the monitoring of the program, any updates to the controls, additional testing for accuracy, and will document when and the development of the program. These duties include to thoroughly investigate and work on related cases within a reasonable timeframe with a supporting analysis and documentation maintained to support the outcome of any review.

XI. Reliance on Third Parties to Perform Customer Due Diligence

The company uses third-party providers to analyze, review and verify customer-provided datapoints. Alerts or insights originate from vendors such as Sardine A.I. (sanctions and PEP

screening) and Chainalysis (blockchain transaction tracing). Additional information is found below:

i. Sardine A.I. – As a supplement to the Company’s own internal policies and reviews, the Company has engaged Sardine A.I. to: (a) conduct Sanctions Checks and “PEP” checks whereby Sardine compares information provided by MyPrize users against comprehensive watchlists and databases that aggregate PEPs, persons with global sanctions, and persons that may be on crime and terror watchlists; (b) Sardine A.I. is also engaged to provide KYC verification; (c) Sardine A.I. is engaged to analyze customer behaviors and transaction information for transaction monitoring and behavior analytics; and (d) Sardine A.I. is engaged for case management purposes.

ii. Chainalysis – The Company also engages Chainalysis, a Company dedicated to tracing blockchain transactions by providing compliance and investigation software that allows MyPrize to track any crypto or virtual currency transactions and ensure that also such crypto transactions are compliant with applicable laws, and the Company’s AML Policies and Programs.

XII. Reporting of Unusual Transaction

MyPrize will report any unusual transactions to the Curacao FIU if they’re believed to be involved in potential money laundering. To protect the Compliance department, the AML Compliance Person ensures MyPrize personnel can report violations of the Program anonymously. Employees engaging with customers or accessing customer information will receive anti-money laundering (AML) training to recognize unusual or potentially suspicious behaviors. If employees suspect involvement with proceeds of crime, they must submit an Internal Unusual Activity Report (IUAR) to the AML Compliance Person within 24 hours. The AML Compliance Person will investigate and determine if a report to the Financial Intelligence Unit (FIU) of Curaçao is warranted within 48 hours.

MyPrize staff will be trained to identify unusual transactions based on customer profiles and specific indicators. All unusual transactions must be reported to the CO in an approved format, accompanied by supporting documentation.

Unusual transactions include:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 (equivalent USD 2,700) or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:

1. A cashless transaction in the amount of Cg. 5,000.00 (equivalent USD 2,700) or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 (equivalent USD 2,700) or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 (equivalent USD 2,700) or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000.00 (equivalent USD 2,700) or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 (equivalent USD2,700) resets per game day of the user.

The AML Compliance Person further ensures that this mechanism is well publicized to all personnel and will take necessary steps to ensure reports of potential violations remain anonymous and confidential. Regardless of whether a report is made anonymously, MyPrize has zero tolerance for retaliation against an employee for reporting a potential violation up to and including termination. All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

Further, the Company will retain copies of all actions, decisions, and processes outlined in this document for a minimum of seven years. The records will be electronically stored, to be printed as a hard copy when necessary. The records will also be organized in a manner that facilitates easy retrieval to enable reporting to the Curacao FIU without undue delay.

XIII. Anti-Money Laundering Compliance Program

When an employee of the Company detects a red flag, or other activity that may be concerning, he or she will notify Compliance (if the activity was not detected by Compliance). Under the direction of the AML Compliance Person, the Company will determine how to further investigate the matter which may include gathering additional information internally or from third-party service providers, contacting the government, and suspending or closing the account.

A. **Internal Controls** – The Company has implemented the following internal controls to mitigate risks targeted by the Program, each as described below: (i) KYC Program; (ii) Transaction Monitoring; (iii) Sanctions and Prohibited Jurisdictions; and (iv) Fraud Prevention.

B. **Know Your Customer Program** – The Company has established, documented, and maintains a KYC Program. The Company will: (1) collect certain identification information

from each customer; (2) utilize risk-based measures to verify the identity of each customer; (3) record customer identification information and the verification methods and results; and (4) provide the required CIP notice to customers for which the Company seeks identification information to verify their identities. Each customer of MyPrize will be initially screened at onboarding and periodically thereafter for as long as they remain a customer.

C. Customer Identification Program (the “CIP”)

i. **CIP Account Creation** – In order to open up a MyPrize account, a customer must provide their email for a level 1 account. As the account reaches specific milestones, the account will reach new levels and will provide additional information, all of which will be confirmed either through the Company’s due diligence processes or through the use of a third-party vendor.

ii. **CIP Customer Due Diligence** – Customer Due Diligence (“CDD”) refers to the process the Company will use to collect and evaluate relevant information about its customers throughout the entire relationship to determine the risk the customers pose for financial crimes. The Company uses the following third-party tools and services to perform CDD.

iii. **Enhanced Due Diligence** – In certain circumstances, the Company may identify a customer who requires additional information before the customer will be allowed to engage in transactions through a customer account. For these customers, Enhanced Due Diligence (“EDD”) may be conducted by collecting and evaluating the information listed below in addition to the information listed above that is collected from every customer.

For customers that are identified as “high risk”, the Company may collect information:

- a. concerning their source of wealth and/or income (i.e., bank statement, pay stubs, investment account statement, tax returns);
- b. concerning the usage of services and expected activity;
- c. regarding the relationship between the source or destination of funds and/or purpose of the transaction and/or the relationship between the high-risk customer and other MyPrize customers; and/or
- d. any other pertinent information to ensure a reasonable belief that the customer’s identity has been properly ascertained and that the customer is not involved in any illicit activity.

iv. **Recordkeeping** – The Company shall retain User information for a period beginning upon the User signing up on MyPrize.com until seven (7) years following the date the account is closed; such information shall include:

- a. All CDD / EDD or any other identifying information received by the Company;
- b. Descriptions of any steps taken by members of Compliance to identify such customers; and
- c. Any additional due diligence information collected by the Company.

Additionally, the Company will retain copies of all ID documentation obtained from the customer for a minimum of seven years following the date of verification is performed or the account is closed, whichever is most recent. If customers request that their data be erased, MyPrize's response to such request will be in accordance with the Company's Privacy Policy.

Further, the Company will retain copies of all actions, decisions, and processes outlined in this document for a minimum of seven years. The records will be electronically stored, to be printed as a hard copy when necessary. The records will also be organized in a manner that facilitates easy retrieval to enable reporting to FinCEN within 30 days of a request.

v. **Sanctions, Prohibited Jurisdictions & Politically Exposed Persons** – The Company is committed to complying with all applicable sanctions, including U.S. UN, and EU sanctions, by taking the following measures:

- a. prohibition of individuals or entities listed on applicable assets freeze lists, such as the US list of specially designated nationals and block persons, the EU consolidated list of financial sanctions targets, or any list maintained by any relevant authority;
- b. prohibition of entities owned or controlled by entities on the lists referred above;
- c. we prohibit and restrict Users in certain countries or territories. For example, US Persons are generally prohibited from dealing with Cuba, Iran, Syria, North Korea, and Crimea ("**Restricted Territories**"); and
- d. the Company routinely monitors customers against the following Sanctions lists:
 - OFAC SDN list
 - OFAC non-SDN lists
 - EU Sanctions list
 - United Nations Sanctions list
 - UK His Majesty Treasury (HMT) list.

In order to comply with the economic and trade sanctions administered by OFAC and other government agencies, the Company will not do business with, or make funds directly or indirectly

available to, sanctioned individuals and entities. The Company will screen all customers against OFAC and other relevant sanctions lists at onboarding and on a periodic basis as needed, as well as when the issued lists are updated. The Company may utilize third-party vendors to conduct these checks.

The Company will have in place a process to freeze and block accounts of all customers that are a confirmed sanctions match, and will escalate those customers to business partners requiring such escalations within 24 hours.

The Company maintains a Non-supported Countries list which includes a list of countries that the Company does not do business with due to sanctions or other high risks. Additionally, the company maintains a “Sanctioned Jurisdictions List” which contains a list of countries that are not supported but are used as a reference for sanctions-based controls. The Company will keep these lists updated and seek to prevent customers who reside in those countries from utilizing the Company’s platform.

Any Company employee or third-party service provider who violates the rules or permits another to violate the rules in this policy may be subject to disciplinary action, including dismissal. There are potential personal and institutional consequences, including civil and/or criminal penalties for violating the below rules related to sanctions.

Company employees, contractors, or third-party providers who become aware of a potential sanctions violation should bring it up to the attention of Legal and Compliance. The full Sanctions Program can be found in the MyPrize Sanctions / OFAC Policy.

Further, in order to mitigate the risk from trading with customers who are Politically Exposed Persons (PEPs) or subject to Sanctions, the Company’s active customer base is screened using a third-party screening solution provided by Sardine. Sardine’s technology uses RDC (Regulatory DataCorp) for screening support. Customers are screened at the following intervals:

- i. First purchase or deposit, if applicable;
- ii. First redemption; and
- iii. Daily thereafter (for previously screened customers).

The comparison produces alerts for potential matches that are reviewed to be confirmed as true matches or dismissed as false positives by the Company’s AML analysts.

The term “Politically Exposed Persons” is broad and generally includes all persons who fulfill a prominent public function. This includes:

- i. Heads of State, Heads of Government, Ministers, Deputy and Assistant Ministers, and Parliamentary Secretaries;
- ii. Members of Parliament;
- iii. Members of the Courts of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- iv. Members of courts of auditors, Audit Committees or of the boards of central banks;
- v. Ambassadors, charge d’affaires and other high-ranking officers in the armed forces; and

- vi. Members of the administration, management or boards of State-owned corporations.

The term “immediate family members” of PEPs includes:

- i. The spouse, or any partner recognized by national law as equivalent to the spouse;
- ii. The children and their spouses or partners; and
- iii. The parents.

The following factors are considered by AML analysts when determining if an alert is a true match or a false positive in connection with an identified name:

- i. If only part of the name matches (e.g., only the last name matches but the first name does not), then it is not a valid match;
- ii. Check if the customer’s name matches all the former names and aliases in the sanctions hit list; and
- iii. If the names match, look for other information to determine if the hit is a true match (e.g., date of birth, address).

The AML Compliance Person determines whether to maintain or terminate the business relationship with a customer if adverse watch list matches are detected. This decision is based on the nature and severity of the negative information found. The account may be closed permanently or continued, depending on the AML Compliance Person’s judgment.

II. Information Sharing

MyPrize fully cooperates with federal government authorities, law enforcement authorities, and other financial institutions on AML investigations to the extent allowable under privacy and other laws. In particular, MyPrize supports any requests from government agencies, including subpoenas and National Security Letters.

The AML Compliance Person monitors the procedures in place to ensure MyPrize receives, documents, and responds to requests for information sharing, such as subpoenas and National Security Letters. The AML Compliance Person will ensure that these procedures include notification of the Compliance department to allow for the review of any relevant customer activity for AML risk.

My Prize prohibits personnel from disclosing information about its Program or activities, including any investigations related to any customers, without receiving written permission from the AML Compliance Person.

III. Program Administration

At least annually, the Compliance Officer will review the Program and related procedures. They will recommend appropriate changes for approval by the Board. The review includes

consideration of applicable law, feedback on the effectiveness of the Program, internal controls set forth in the Program, and any supervisory examination or audit input.

No part of the Program or its supporting procedures should be interpreted as contravening or superseding any other legal and regulatory requirements imposed upon the Company. Any conflict between the Program and the Company's other legal obligations must be submitted immediately to the AML Compliance Person for further evaluation who will, if necessary, consult with legal counsel.

IV. Employee Training and Reporting Guide

A. Training – MyPrize requires that all new employees subject to this policy, receive AML/OFAC training at least annually, New Employees are assigned to the training as a part of the onboarding process. Employees that are delinquent may be subject to disciplinary actions. Relevant employees include those responsible for the following:

- i. customer onboarding and due diligence (including high-risk customer monitoring;
- ii. monitoring customer transactions and electronic fund transfers;
- iii. addressing customer queries or concerns (customer service teams); and
- iv. technology functions related to AML activities.

B. **Job Specific Training** – All employees are provided with AML training tailored to their job level and are tasked with contributing to the prevention, detection, and reporting of money laundering, terrorist financing, and other criminal activity. The goals of the Company's training program are as follows:

- i. Ensure all Employees are familiar with relevant AML/OFAC requirements pertaining to their specific job functions and that they receive the most current information available.
- ii. Ensure all Employees are trained to identify risky activity and are able to manage and escalate such activity to appropriate personnel.
- iii. Ensure directors are knowledgeable regarding the Company's obligations and responsibilities under AML/OFAC regulations.
- iv. Inculcate an understanding of the significance of the Company's AML/OFAC efforts and help develop a strong culture of AML/OFAC compliance-related risks as they arise.
- v. Develop a cadre of staff and managers throughout the Company that are able to detect, escalate, and manage AML/OFAC compliance-related risks as they arise.

The AML Compliance Person is responsible for developing a risk-based training program and ensuring that staff members requiring advanced training due to their job description and/or responsibilities within the Company receive such training. My Prize will record and document its training procedures and materials.

C. **Reporting** – All individuals affiliated with the Company, including officers, directors, employees, and associated personnel, have a duty to aid the Company's endeavors to identify, prevent, and deter money laundering and other illicit activities aimed at financing terrorism or criminal operations via its services. If employees become aware of any behavior that may suggest money laundering or terrorist financing, they must promptly report it. Apart from the legal penalties mentioned above, the Company will hold its staff accountable for any failure to comply with the established guidelines.

i. *Employees Must:*

a. be on alert for unusual or potentially suspicious behavior in the course of their daily work;

b. report any suspicion promptly to avoid the offense of failure to report; and

c. keep the report and its content strictly confidential to avoid tipping off, particularly the individual who is being reported.

ii. Reports should be made via email to the AML Compliance Person. The report should be fact-based and free from speculation. Always keep the fact that you have reported and the content of your report strictly confidential.

iii. The Company values employee reports, which are crucial in its fight against money laundering, terrorist financing, and other criminal activity. Employees who fail to fulfill their AML/OFAC obligations may face criminal sanctions. Consequently, it is vital that employees promptly notify the AML Compliance Person whenever they encounter information that leads them to suspect a customer's involvement in criminal activity, an unusual or intricate transaction lacking an apparent economic rationale, or the submission of falsified documentation by a customer. Reports are to be made in writing in order to create an audit trail and a record of the appropriate actions being taken by the employee. All reports should be sent to the AML Compliance Person and should include at minimum:

a. Personal information collected during the CDD process, including full name, date of birth, permanent address, any documents provided and pertinent correspondence records;

b. Username(s);

c. Value of transactions (purchases, redemptions, balance, sufficient to reconstruct the transaction flow);

d. Reasons for reporting (as detailed as possible); and

e. Account status (active, suspended).

iv. **CONFIDENTIALITY / DUTY TO NOT DISCLOSE TO IMPACTED PERSONS** – employees must never inform the customer in question or third parties about their disclosure. The duty of confidentiality applies both to external reporting and any related information, including information received from FinCEN, the police, or any third party at a later date. The AML Compliance Person reviews all reports promptly, and each report receives an acknowledgement or, if necessary, a request for additional information. If an external disclosure is made, the identity of the employee who raised the suspicion is not revealed.

D. **Independent Testing** – My Prize will conduct independent testing on the Company's AML program on a periodic basis, and no less than twice annually. When conducted, the review will assess the implementation and effectiveness of the Company's AML/OFAC program and the adequacy of controls over any related risks. The Compliance Officer is responsible for updating the Company's risk assessment in regards to any issues raised during the independent testing and taking necessary corrective actions and remediate findings. Independent testing has not yet been conducted on the program but the decision to test will be determined at a later date.

E. **Outcomes and Conclusions** – The information gathered from these checks is analyzed by the AML Compliance Person. In situations where there are concerns about the legitimacy of a customer's funds and they were unable or unwilling to provide sufficient evidence to alleviate these concerns, the account will be closed. Additionally, if the concerns are significant enough, the matter may be escalated to the AML Compliance Person for consideration of a report to be made to the relevant authorities. This is in line with AML and counter-terrorist financing regulations and helps to prevent the Company from being used as a tool for illicit activities. Once the enhanced due diligence investigation is completed and the sources of funds are deemed legitimate, the account will be signed off to a level of activity corresponding to the amounts of income evidenced by the findings of the investigation. The account will then remain active but subject to ongoing monitoring to ensure continued compliance with AML regulations.

V. Ownership

This Program is owned and managed by the Legal Department and the AML Compliance Person. The AML Compliance Person's role is to ensure the Company has established strong controls and procedures to prevent and/or report instances of money laundering, terrorist financing, or other crimes across all of its operations. Additionally, the AML Compliance Officer is responsible for supervising the training of all Company employees with regard to recognizing, monitoring, and identifying money laundering activities.

VI. Governance & Oversight

This Policy shall be reviewed by the Legal Department and MyPrize's AML Compliance Person on a regular basis, and at least annually, in order to ensure that the policy is up to date and reflects all changes to the Company's AML Obligations or the Regulations. Additionally, the Legal Department shall monitor relevant changes within the Company and communicate significant

changes to Key Personnel responsible for trade-related activities. The drafting of any update or revision of this Policy shall be performed or approved by the Legal Department, which shall be responsible for the distribution of all updates and revisions to Employees. Periodic and unscheduled audits may be conducted to ensure the continuing compliance with the Policy and with applicable laws and regulations.

VII. Compliance and Consequences of Non-Compliance

Failure to comply with AML legislation may result in sanctions being brought against employees such as fines and imprisonment or the Company including criminal prosecutor, and/or fines. These could affect the Company's ability to operate as well as seriously damage the Company's reputation. The typical types of offenses below may vary between jurisdictions.

Employees can be found guilty of money laundering if they (a) fail to report, (b) tip off, and/or prejudice an investigation, and/or (c) assist in the act of money laundering.

A. **Failing to Report Money Laundering** is committed if the following elements are met: (i) the employee knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering, or is attempting to launder money; (ii) the information or other matter, on which that knowledge or suspicion is based came to his/her attention in the course of his/her trade, profession, business or employment; and (iii) the employee does not disclose the information to the AML Compliance Person and the AML Compliance Person does not disclose to FinCEN as soon as reasonably expected.

Separate and in addition to the foregoing, an employee may also be liable for failure to meet record keeping and client identification responsibilities and requirements, failure to provide assistance or provide information during a compliance examination, or disclosing the fact that a unusual transaction report was made, or disclosing the contents of such a report with the intent to prejudice a criminal investigation.

B. **"Tip Off"** shall be defined as revealing to a third party that an internal or FinCEN report has been filed. Similarly, "prejudicing an investigation" involves disclosing to a third party that law enforcement is either investigating or preparing to investigate an individual. Disclosing to a suspected money launderer that a disclosure has been made will almost certainly undermine any subsequent investigation,

C. **"Assist"**

An employee commits an offense if he or she: (i) enters an arrangement which he or she knows, or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person; (ii) acquires, uses or has possession of criminal property; and (iii) conceals, disguises, converts, transfers or removes criminal property.

VIII. Related Documents / Resources

- i. KYC Policy
- ii. Sanctions Policy
- iii. Unsupported Jurisdictions List
- iv. Prohibited Jurisdictions List

IX. Questions / Contact Information

Please use the following contact information with any questions in regard to the Policy.

Frank Nonnenmacher – Head of Compliance

Email: Frank@mytechnologyco.com

In witness whereof, Clover Leaf B.V. has caused this Policy to be duly executed this 16th day of May 2025



By: e-Management N.V. as Director of Clover Leaf B.V.

Clover Leaf B.V. - AML Policy

Final Audit Report

2025-05-28

Created:	2025-05-28
By:	Sharella Bitoria (sharella.bitoria@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA8k0gLkFT0E91fuHMOMNRP9wsEdNDJhN3

"Clover Leaf B.V. - AML Policy" History

-  Document created by Sharella Bitoria (sharella.bitoria@hbmgroup.com)
2025-05-28 - 8:10:20 PM GMT
-  Document emailed to Herman Oosten (herman.oosten@hbmgroup.com) for signature
2025-05-28 - 8:10:24 PM GMT
-  Email viewed by Herman Oosten (herman.oosten@hbmgroup.com)
2025-05-28 - 8:36:17 PM GMT
-  Document e-signed by Herman Oosten (herman.oosten@hbmgroup.com)
Signature Date: 2025-05-28 - 8:36:32 PM GMT - Time Source: server
-  Document emailed to Annesol Melaria (annesol.melaria@hbmgroup.com) for signature
2025-05-28 - 8:36:33 PM GMT
-  Email viewed by Annesol Melaria (annesol.melaria@hbmgroup.com)
2025-05-28 - 9:16:53 PM GMT
-  Document e-signed by Annesol Melaria (annesol.melaria@hbmgroup.com)
Signature Date: 2025-05-28 - 9:17:11 PM GMT - Time Source: server
-  Agreement completed.
2025-05-28 - 9:17:11 PM GMT