

Plustar N.V.

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Compliance Manual

Version: 1.0

Effective Date: [To Be Assigned]

Prepared By: Compliance Department, Plustar N.V.

Confidentiality Level: Internal Use Only

Company Name: Plustar N.V.

Registered Address: Abraham de Veerstraat 9, Curacao

Industry: Online Gambling

Regulatory License: Curacao eGaming License

This manual outlines the anti-money laundering and counter-terrorist financing framework adopted by Plustar N.V. in compliance with applicable laws, regulations, and international standards. All personnel are required to adhere to the procedures defined herein.

Table of Contents

I. Preface

1.1 General Statements

1.2 What is Money Laundering?

1.3 What is Financing of Terrorism?

1.4 What is Financing of Proliferation of Weapons?

1.5 Targeted Financial Sanctions

II. The Risk-Based Approach

II.1 What is the Risk-Based Approach?

II.2 The Business and Customer Risk Assessments

1. II.2.1 Business Risk Assessment (BRA)

2. II.2.2 Customer Risk Assessment (CRA)

3. II.2.3 Risk Factors Specific to the Gambling Sector

II.3 Technological Developments Risk Assessment

III. Customer Due Diligence

III.1 Introduction

III.2 The CDD Measures

1. III.2.1 Identification and Verification of the Player

2. III.2.2 Identification and Verification of the Beneficial Owner

3. III.2.3 Purpose and Intended Nature of the Business Relationship

4. III.2.4 Ongoing Monitoring

III.3 Timing of CDD Measures

III.4 Enhanced Due Diligence

III.5 Simplified Due Diligence

III.6 Politically Exposed Persons

III.7 Existing Customer Reviews

III.8 Termination of the Business Relationship

III.9 Third-Party Reliance

IV. Reporting of Unusual Transactions

IV.1 Reporting Obligations

IV.2 Prohibition of Disclosure

IV.3 Record Keeping

V. Anti-Money Laundering Compliance Program

V.1 Introduction

V.2 Internal Policies, Procedures, and Controls

V.3 Appointment of Compliance Officer

V.4 Employee Screening and Training Program

V.5 Independent Audit Function

V.6 Examination by the Gaming Control Board

VI. Virtual Asset & Crypto Policy

VI.1 Introduction

VI.2 Scope of Application

VI.3 Crypto Transaction Risk Assessment

VI.4 VASP Interaction

VI.5 Cold Wallets & Custodians

VI.6 Internal Controls

VII. Transaction Monitoring and Risk Triggering Mechanisms

VII.1 Overview

VII.2 Monitoring Techniques

VII.3 Review Process

VII.4 Monitoring Tools

VIII. Enhanced Internal Controls & Compliance Oversight

VIII.1 Segregation of Duties

VIII.2 Compliance Officer Duties

VIII.3 Internal Audit

VIII.4 Incident Reporting Protocol

I. Preface

1.1 General Statements

This Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Compliance Manual outlines the internal framework adopted by Plustar N.V., a licensed online gambling operator registered in Curacao, to prevent its platform and services from being exploited for illicit financial activities.

The document is developed in accordance with applicable regulations, guidelines from the Curacao Gaming Control Board, and international standards established by the Financial Action Task Force (FATF). The policies and procedures herein are mandatory and binding upon all employees, departments, agents, and relevant third-party service providers of Plustar N.V.

1.2 What is Money Laundering?

Money laundering refers to the process of disguising the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. It generally involves three sequential stages:

- **Placement:** The introduction of criminal proceeds into the financial system.
- **Layering:** Complex transactions to obscure the origin of the funds.

- **Integration:** Reintroduction of the laundered money into the legitimate economy.

Plustar N.V. adopts mechanisms to identify and prevent activities that may constitute or facilitate any of the above stages.

I.3 What is Financing of Terrorism?

Financing of terrorism involves the provision or collection of funds with the intention that they be used to carry out terrorist acts. These funds may come from both illegal and legitimate sources. Unlike money laundering, the focus is not on the origin but on the intended use of funds.

Plustar N.V. maintains screening systems, customer profiling tools, and payment controls to mitigate risks of terrorist financing.

I.4 What is Financing of Proliferation of Weapons?

Proliferation financing refers to the act of providing funds or financial services that support the spread of weapons of mass destruction (WMD). International sanctions, including those issued by the United Nations Security Council (UNSC), are the primary tools used to combat such activities.

Plustar N.V. actively monitors customers and transactions to ensure compliance with applicable sanction regimes and blocks any activity suspected to contribute to WMD proliferation.

I.5 Targeted Financial Sanctions

Targeted Financial Sanctions (TFS) are restrictive measures imposed by international or domestic authorities to prohibit transactions with specific individuals, entities, or countries. These sanctions are primarily related to terrorism, proliferation, or human rights violations.

Plustar N.V. adheres to all relevant TFS obligations by:

- Conducting name screening against updated sanctions lists
- Freezing assets where required

- Notifying regulatory bodies when necessary

The effectiveness of these measures relies on systematic application of screening tools and prompt response protocols by the compliance department.

II. The Risk-Based Approach

II.1 What is the Risk-Based Approach?

The Risk-Based Approach (RBA) is a methodology that enables Plustar N.V. to allocate AML/CTF resources efficiently and effectively by identifying, assessing, and understanding the money laundering and terrorist financing risks the business faces. Resources are then directed in accordance with the level of risk.

The RBA forms the cornerstone of effective risk management and regulatory compliance. It allows for:

- Proportional implementation of controls
- Prioritization of higher-risk customers, products, services, and geographies
- Reduction of burdens on low-risk relationships

II.2 The Business and Customer Risk Assessments

II.2.1 Business Risk Assessment (BRA)

The Business Risk Assessment evaluates the overall exposure of Plustar N.V. to money laundering and terrorism financing. It considers operational practices, product offerings, payment channels, geographic markets, and customer demographics.

Key BRA factors include:

- Nature of services (online gambling)
- Use of cryptocurrencies (BTC, ETH, USDT)

- Geographic scope and exclusion of high-risk countries
- Delivery channel risk (fully remote onboarding)

The BRA is reviewed annually or upon any significant change in business operations.

II.2.2 Customer Risk Assessment (CRA)

Customer Risk Assessments are performed on all clients upon registration and periodically during the business relationship. The risk model considers:

1. Jurisdiction of residence
2. Source of funds and wealth
3. Occupation and transaction profile
4. Behavioral indicators (e.g., frequent high-value deposits)

Clients are categorized into low, medium, or high risk, triggering corresponding levels of due diligence.

II.2.3 Risk Factors Specific to the Gambling Sector

The gambling industry presents sector-specific risks, including:

1. Rapid transaction flows that may obscure illicit patterns
2. Customer anonymity due to remote registration
3. Use of third-party payment processors

Plustar N.V. addresses these risks by enforcing robust identity verification, limiting deposit methods, and monitoring behavioral anomalies.

II.3 Technological Developments Risk Assessment

Plustar N.V. continually monitors and assesses the risks associated with new technologies, particularly in payment innovations and platform features. This includes:

1. Adoption of automated systems for fraud detection
2. Integration of machine learning for transaction analysis
3. Controls on smart contract-based crypto assets

Emerging threats are evaluated through cross-departmental risk reviews and technology audits.

III. Customer Due Diligence

III.1 Introduction

Customer Due Diligence (CDD) is a critical component of Plustar N.V.'s AML/CTF framework. It involves the collection and evaluation of identifying information about each customer to assess their risk profile, verify their identity, and determine the legitimacy of their transactions. CDD is implemented during onboarding and maintained throughout the customer lifecycle.

III.2 The CDD Measures

III.2.1 Identification and Verification of the Player

All customers must undergo a full Know Your Customer (KYC) process before gaining access to gambling services. The following information is required:

1. Full legal name
2. Date of birth
3. Nationality and country of residence
4. Government-issued photo identification
5. Proof of address

Verification is performed through document validation, liveness checks (where applicable), and third-party verification databases.

III.2.2 Identification and Verification of the Beneficial Owner

In the case of corporate or proxy accounts, the beneficial owner(s) of the funds must also be identified and verified. This includes:

1. Ownership structure documentation
2. Identification of natural persons owning 25% or more
3. Screening against sanction lists and PEP databases

III.2.3 Purpose and Intended Nature of the Business Relationship

Customers must declare the purpose of account usage, such as:

1. Personal recreational gambling
2. Frequency and scale of intended deposits
3. Preferred payment channels

Discrepancies between stated intentions and actual behavior trigger further review.

III.2.4 Ongoing Monitoring

All customer activity is subject to ongoing monitoring, including:

1. Transaction pattern analysis
2. Frequency of login and usage
3. Abrupt changes in gambling behavior
4. Involvement of previously unseen jurisdictions

Unusual or suspicious behavior is escalated to the Compliance Officer.

III.3 Timing of CDD Measures

CDD measures must be completed:

1. Prior to account activation
2. Upon suspicion of money laundering or terrorist financing
3. Upon changes to key customer details
4. Periodically for high-risk customers

Failure to complete CDD within required timelines results in account suspension.

III.4 Enhanced Due Diligence

Enhanced Due Diligence (EDD) applies to high-risk customers and includes:

1. More in-depth source of funds analysis
2. Senior management approval for onboarding
3. Continuous review cycles

Risk triggers for EDD include:

1. Politically Exposed Person (PEP) status
2. Adverse media coverage
3. High transaction volumes or value

III.5 Simplified Due Diligence

Simplified Due Diligence (SDD) may be applied in limited scenarios where risk is objectively low. For example:

1. Customers residing in low-risk countries
2. Occasional and low-value transactions

Even under SDD, identity verification is still required.

III.6 Politically Exposed Persons

Plustar N.V. performs screening to detect PEPs. Where a PEP is identified:

1. Enhanced Due Diligence applies
2. Source of wealth and funds must be documented
3. Continuous monitoring is mandatory

III.7 Existing Customer Reviews

Plustar N.V. conducts periodic reviews of existing customers to ensure:

1. Records are up to date
2. Risk levels are still valid
3. No new suspicious activity has emerged

The frequency of review depends on the assigned risk tier.

III.8 Termination of the Business Relationship

A business relationship is terminated when:

1. The customer fails to meet CDD requirements
2. The relationship is deemed too high-risk
3. Regulatory or legal obligation necessitates closure

All terminations must be documented and, if appropriate, reported.

III.9 Third-Party Reliance

Plustar N.V. may rely on third parties to perform elements of CDD, provided that:

1. The third party is regulated and subject to AML requirements
2. Results are shared immediately upon request
3. Ultimate responsibility remains with Plustar N.V.

IV. Reporting of Unusual Transactions

IV.1 Reporting Obligations

Plustar N.V. is obligated to report any transaction that appears suspicious or inconsistent with a customer's known profile or declared purpose of use. Reporting duties are mandatory under applicable anti-money laundering regulations and must be executed without delay.

Key obligations include:

1. Immediate internal escalation of any flagged activity
2. Filing of Suspicious Transaction Reports (STRs) with the designated regulatory authority
3. Full documentation of facts, context, and decision-making rationale

All employees are trained to recognize indicators of suspicious transactions and report them through the internal compliance channel.

IV.2 Prohibition of Disclosure

Employees and officers of Plustar N.V. are strictly prohibited from informing any customer or third party that a suspicious transaction is being reported or that a compliance investigation is underway. This confidentiality obligation applies before, during, and after the reporting process.

Violations of this non-disclosure requirement may result in regulatory penalties and internal disciplinary action.

IV.3 Record Keeping

To ensure regulatory compliance and facilitate potential investigations, Plustar N.V. maintains detailed records related to AML activities, including:

1. Customer identification documents (retained for at least 5 years after relationship termination)
2. Transaction records, including payment method, time, amount, and counterparties
3. Internal compliance reviews and STR filings

Records are stored securely and are accessible only to authorized personnel. Systems are periodically tested to ensure data integrity, confidentiality, and retrievability.

V. Anti-Money Laundering Compliance Program

V.1 Introduction

Plustar N.V. maintains a comprehensive and risk-sensitive AML Compliance Program in accordance with local regulations and FATF guidelines. This program serves as the operational foundation for detecting, deterring, and reporting suspicious financial activities.

The program incorporates robust policies, procedures, controls, and governance mechanisms to ensure continuous compliance and adaptation to evolving threats.

V.2 Internal Policies, Procedures, and Controls

The Compliance Department oversees the implementation of:

1. Written policies outlining AML/CTF responsibilities and protocols
2. Standard operating procedures for CDD, transaction monitoring, and recordkeeping
3. Internal control systems that detect policy breaches or inconsistencies

All policies are reviewed annually and updated as needed.

V.3 Appointment of Compliance Officer

Plustar N.V. has formally designated a qualified Compliance Officer (CO) responsible for:

1. Overseeing AML/CTF program execution

VI. Virtual Asset & Crypto Policy

VI.1 Introduction

As part of its service offering, Plustar N.V. accepts selected virtual assets as payment options. This policy outlines the risk controls and governance measures in place to manage exposure to cryptocurrencies such as Bitcoin (BTC), Ethereum (ETH), and Tether (USDT).

VI.2 Scope of Application

This policy applies to all cryptocurrency transactions conducted via the Plustar N.V. platform. It includes:

1. Deposits and withdrawals in BTC, ETH, USDT
2. Internal controls for handling crypto payments
3. Customer risk assessments tied to crypto use

VI.3 Crypto Transaction Risk Assessment

Crypto transactions present distinct risks due to:

1. Anonymity of blockchain addresses
2. Global reach without jurisdictional boundaries
3. Rapid and irreversible transfers

To address these risks, Plustar N.V.:

1. Flags high-volume or unusual crypto transactions for manual review
2. Prohibits crypto transactions originating from sanctioned countries or high-risk jurisdictions
3. Logs transaction hashes and wallet addresses for traceability

VI.4 VASP Interaction

Currently, Plustar N.V. does not maintain formal relationships with Virtual Asset Service Providers (VASPs). However, if such engagement occurs in the future, the following conditions will apply:

1. Only VASPs regulated in FATF-compliant jurisdictions may be engaged
2. Due diligence must be performed on the VASP's AML/CTF framework
3. Records of all VASP-related transactions must be retained for five years

VI.5 Cold Wallets & Custodians

Plustar N.V. does not utilize cold storage or custodial services for holding customer crypto funds. All crypto received is:

1. Processed directly to operational wallets
2. Managed with multi-factor authentication and internal authorization procedures

Any future implementation of custodial wallets must include:

1. Segregation of customer assets
2. Daily reconciliation
3. Access controls and activity logs

VI.6 Internal Controls

To manage crypto-specific risks, the company has implemented:

1. Transaction limits based on customer risk tier
2. Real-time alerts for suspicious address activity
3. Manual review queue for deposits exceeding predefined thresholds
4. Crypto reporting integrated into overall AML transaction monitoring

The Compliance Officer is responsible for overseeing crypto-related policies and initiating periodic reviews based on threat landscape changes.

VII. Transaction Monitoring and Risk Triggering Mechanisms

VII.1 Overview

Transaction monitoring is an essential control element in Plustar N.V.'s AML/CTF program. The goal is to detect, assess, and respond to suspicious transactions and behavior that deviate from expected customer patterns or established risk thresholds.

The system is designed to combine automated alerts and manual investigations, ensuring both efficiency and depth of review.

VII.2 Monitoring Techniques

The following techniques are employed:

1. **Rule-Based Alerts:** Parameters are set for transaction frequency, volume, jurisdiction, and source of funds. Breaches of these rules trigger alerts.
2. **Behavioral Profiling:** The system builds dynamic profiles of customer behavior to detect anomalies.
3. **Geolocation Checks:** Transactions are flagged when originating from high-risk or blacklisted jurisdictions.
4. **Crypto Traceability Checks:** Blockchain activity is monitored using analytics tools to assess origin and flow.

VII.3 Review Process

Once an alert is generated:

1. The transaction is reviewed by a compliance analyst.

2. Additional information is retrieved if necessary (e.g., source of funds, customer communication).
3. A decision is made to:
 1. Close the alert (false positive)
 2. Escalate for further internal investigation
 3. File a Suspicious Transaction Report (STR) with the authorities

Case files are documented thoroughly to ensure traceability and auditability.

VII.4 Monitoring Tools

Plustar N.V. uses a combination of proprietary systems and third-party AML monitoring solutions. Key features include:

1. Real-time transaction analytics dashboards
2. Risk scoring engines based on customer profile and activity
3. Alert escalation tracking and resolution workflows

Tools are reviewed and calibrated quarterly to account for emerging threats, regulatory updates, and business changes.

VIII. Enhanced Internal Controls & Compliance Oversight

VIII.1 Segregation of Duties

Plustar N.V. maintains strict segregation of duties (SoD) across key functions to prevent conflicts of interest, unauthorized access, and operational misuse. The following principles are applied:

1. No single employee has end-to-end control over any transaction or process

2. The Finance Department executes payments but cannot override compliance flags
3. Compliance personnel are not involved in revenue-generating functions

All role assignments are reviewed annually and upon staff changes.

VIII.2 Compliance Officer Duties

The Compliance Officer (CO) is the designated individual with overall responsibility for:

1. Implementation and enforcement of the AML/CTF framework
2. Reporting STRs and regulatory notifications
3. Advising management on compliance risks and exposures
4. Approving high-risk client onboarding and reviews
5. Overseeing crypto-related compliance workflows

The CO is supported by deputies and granted access to all necessary systems and records.

VIII.3 Internal Audit

Internal audit is a critical oversight function designed to evaluate:

1. Policy effectiveness and procedural compliance
2. Control adequacy and systems reliability
3. Historical cases and resolution effectiveness

Audit cycles are scheduled at least annually and result in formal reports to executive management, with follow-up tracking for corrective actions.

VIII.4 Incident Reporting Protocol

All employees are obligated to report AML/CTF-related incidents, including:

1. Attempted or suspected fraud

2. Internal policy violations
3. Systemic control failures

Reports may be submitted via secure internal portals or directly to the Compliance Officer.

All reports are:

1. Logged and acknowledged upon receipt
2. Investigated independently
3. Escalated as required based on severity

Confidentiality and protection of whistleblowers are strictly upheld.