

V 1.0

Rail Solutions Group BV

AML/CFT MANUAL

Confidential

Document / Revision History

	AML/CFT Manual
--	-----------------------

Revision #	Version Date	Description of Changes
1.0	30 May 2025	

Table of Contents

Introduction	3
1. Policy Statement	3
2. Purpose	3
3. Audience	3
4. Definitions	3
5. Policy Implementation.....	4
6. Compliance and Consequences of Non-Compliance	6
7. Related Information	6
8. Contact Information.....	6
9. Policy History	7
10. Policy URL	7
11. Administrative Details	7

Introduction

1. Policy Statement

This document outlines the Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Counter Proliferation Financing (CPF) policy of Rail Solutions Group BV ("the Company"). This policy serves as a cornerstone in the Company's efforts to prevent and mitigate the risks associated with money laundering, terrorist financing, and the proliferation of weapons of mass destruction. The policy applies to all operations, employees, and service providers of the Company, both online and in any affiliated physical locations. It is designed in alignment with the applicable laws in Curacao including the National Ordinance on the Identification of Clients when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, the Kingdom Sanction Act, and the Code of Criminal Law. The policy also incorporates the FATF 40 Recommendations, the latest guidance issued by the Curacao Gaming Control Board (GCB), and EU AML directives.

2. Purpose

The purpose of this policy is to define and implement robust internal measures, processes, and controls that help prevent the misuse of Rail Solutions Group BV's platforms for the purposes of money laundering, financing of terrorism, and financing of proliferation. The policy ensures compliance with local and international legal obligations and promotes the integrity, transparency, and accountability of Rail Solutions Group BV's services. It also enhances customer confidence and safeguards the company from reputational, legal, and financial risks.

3. Audience

This policy is mandatory and applies to all employees, officers, board members, subcontractors, consultants, third-party service providers, affiliates, and any other persons or entities operating on behalf of or in partnership with Rail Solutions Group BV.

4. Definitions

- **Money Laundering (ML):** The process of disguising the illicit origin of proceeds derived from criminal activities.
- **Terrorist Financing (TF):** Providing or collecting funds with the intention or knowledge that they will be used to carry out terrorist acts.
- **Proliferation Financing (PF):** The act of providing funds for the acquisition, development, or transport of nuclear, chemical, or biological weapons.
- **PEP (Politically Exposed Person):** Individuals who are or have been entrusted with prominent public functions, and their immediate family members and close associates.
- **CDD (Customer Due Diligence):** Procedures to collect and verify information about the identity of a customer.
- **EDD (Enhanced Due Diligence):** Additional scrutiny for customers who pose a higher risk of ML/TF/PF.
- **MLRO (Money Laundering Reporting Officer):** The appointed individual responsible for ensuring compliance with AML/CFT laws and regulations.

- **CRA (Customer Risk Assessment):** A methodology to assess the ML/TF risk associated with a customer.
- **BRA (Business Risk Assessment):** A systematic process to evaluate risks the company faces from its operations.
- **UTR (Unusual Transaction Report):** A report filed with the FIU when suspicious or unusual transactions are detected.

5. Policy Implementation

5.1 Business Risk Assessment (BRA)

A thorough and well-documented BRA is conducted annually, or upon significant change in the business model, services, or regulatory environment. The BRA examines the risks associated with:

- Types of customers (e.g., individuals with multiple sources of income, PEPs, casual customers)
- Geographic locations and jurisdictions
- Distribution channels (e.g., online vs physical establishments)
- Types of products and services (e.g., anonymous payment methods, peer-to-peer gaming)
- Methods of payment and technology (e.g., prepaid cards, e-wallets)

This assessment is approved by the Board of Directors and made available to regulatory authorities such as the GCB upon request. It incorporates the findings from the latest National Risk Assessment (NRA).

5.2 Customer Risk Assessment (CRA)

CRA is carried out prior to establishing a business relationship. Each player is assigned a risk score (low, medium, high) based on:

- Source of funds and wealth
- Country of residence and nationality
- Use of third-party funding sources
- Unusual betting or transactional behavior
- Use of high-risk payment methods or distribution channels

Risk categorization dictates the level of CDD measures required. CRA is updated whenever there are significant changes in the customer's behavior or profile.

5.3 Customer Acceptance Policy (CAP)

CAP defines criteria for accepting or rejecting customers. It includes:

- Refusal to establish business relationships with customers who cannot provide full identity documents
- Mandatory screening of all customers against UN, EU, and Curacao sanctions lists
- Obligatory rejection or termination of relationships with customers who are sanctioned or refuse to comply with AML/CFT checks

- Mandatory EDD and senior management approval for onboarding PEPs
- Requirements to identify and verify the beneficial owner for corporate accounts

5.4 Customer Due Diligence (CDD)

CDD procedures apply when:

- The NAF. 4,000 transaction threshold is reached
- There is suspicion of ML/TF/PF
- There are doubts about the adequacy of previously collected data

CDD involves:

- Full identification: name, residential address, DOB, nationality, ID number
- Verification through government-issued ID and secondary proof of address
- PEP and sanctions screening prior to establishing a relationship and periodically thereafter
- Beneficial owner identification and verification
- Collection of information on the purpose and expected nature of the business relationship

In cases of suspicion, operations are suspended until satisfactory information is obtained.

5.5 Ongoing Monitoring

Ongoing monitoring includes:

- Real-time transaction analysis and flagging of anomalous behavior
- Periodic updating of customer identification information
- Re-verification upon expiry of ID documents
- Review of customer risk profile based on account behavior and geographic movement

Triggers for enhanced monitoring include:

- High-volume or high-frequency transactions
- Repeated use of third-party accounts
- Dormant accounts becoming active with large bets or deposits

5.6 Reliance on Third Parties

The Company may rely on third-party institutions for conducting CDD only if:

- They are subject to equivalent AML/CFT regulations
- They agree to provide CDD data immediately upon request
- They have a formal written agreement with the Company

Rail Solutions Group BV remains ultimately responsible for CDD compliance.

5.7 Reporting of Unusual Transactions

The MLRO must file a UTR with FIU Curacao under the following conditions:

- Transactions that exceed NAf. 5,000 in value
- Suspicion of criminal activity or terrorist financing
- Customer linked to PEP lists or sanctions

All reporting is confidential and follows a no-tipping-off policy. Reports are filed through the official portal at https://portal.fiucuracao.cw/goAMLWeb_PRD/Account/LogOn

5.8 AML Compliance Program

Rail Solutions Group BV maintains a formal AML/CFT compliance program which includes:

- Appointment of an MLRO with direct access to all customer data and the authority to block accounts
- Board-approved AML/CFT policy and internal procedures
- Employee awareness programs and mandatory training
- An internal and independent audit system to test program efficacy
- A mechanism to regularly review and enhance internal controls, especially in light of technological changes

6. Compliance and Consequences of Non-Compliance

One Failure to comply with this policy may result in:

- Internal disciplinary action, including termination
- Civil and criminal liability
- Regulatory fines and sanctions

All personnel are accountable for adhering to this policy and must report any breaches to the MLRO.

7. Related Information

- National Ordinance on the Identification of Clients (NOIS)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Sanctions National Ordinance & Kingdom Sanction Act
- FATF 40 Recommendations
- GCB AML/CFT Guidance (January 2025)
- EU AML Directives

8. Contact Information

For questions or clarifications: MLRO – Rail Solutions Group BV

Email: support@betnimbus.com

Website: www.betnimbus.com

9. Policy History

- Initial Release: May 2025
- This policy supersedes all previous AML/CFT documentation.

10. Policy URL

Relevant policies will be available online at: www.betnimbus.com

11. Administrative Details

Approving Officer:

Chief Compliance Officer or MLRO, Rail Solutions Group B.V.

Responsible Office:

Compliance Department, Rail Solutions Group B.V.

Next Review Date:

Every 3 years, or annually if relevant changes are made.