

AML/CTF/CPF POLICY

**VELATUS N.V.
163778**

27/05/2025

Approved by the Board of Directors

A handwritten signature in blue ink, consisting of a large, stylized capital letter 'A' followed by a series of loops and a final downward stroke.

Compliance Officer: Haris Constantinou
compliance@velatus-nv.com
Scheduled Policy Review Date: May 2026

CONTENTS

1. POLICY STATEMENT	3
2. iGAMING ENVIRONMENT	4
3. MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING	4
4. SENIOR MANAGEMENT ROLE	9
5. RISK ASSESSMENT	10
5.1. CUSTOMER RISK	11
5.2. GEOGRAPHIC RISK	12
5.3. PRODUCT, SERVICE AND TRANSACTION RISKS	13
5.4. DISTRIBUTION CHANNEL RISKS	14
5.5. TECHNOLOGICAL RISKS	15
6. COMPLIANCE FUNCTION	17
6.1. APPOINTMENT OF MLRO/AMLCO	17
6.2. FUNCTIONS OF MLRO/AMLCO	17
6.3. RESPONSIBILITIES OF MLRO/AMLCO	17
7. CUSTOMER DUE DILIGENCE	19
7.1. COMPANY'S IDENTIFICATION AND VERIFICATION OF PLAYERS	19
7.2. BUSINESS RELATIONSHIP PURPOSE AND NATURE	20
7.3. TIMING OF CDD	21
7.4. EXISTING CUSTOMERS MONITORING	22
7.5. ENHANCED DUE DILIGENCE (EDD)	23
7.6. SIMPLIFIED DUE DILIGENCE (SDD)	23
7.7. POLITICALLY EXPOSED PERSONS (PEPs)	24
7.8. RELIANCE ON THIRD PARTIES AND TECHNOLOGICAL TOOLS PROVIDERS	24
7.9. RELATIONSHIP TERMINATION	24
8. SANCTIONS	25
9. SUSPICIOUS ACTIVITY & TRANSACTION REPORTING	26
10. AML/CTF/CPF AUDIT	28
11. TRAINING AND RECORD KEEPING	30
12. ANNEXES	31
12.1. KEY ABBREVIATIONS	31
12.2 KEY DEFINITIONS	32

1. POLICY STATEMENT

The Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) Policy (referred to as the AML/CTF/CPF Policy) has been crafted to ensure full compliance with the guidelines set forth by the Curaçao Gaming Control Board, the designated authority overseeing AML/CTF/CPF measures in Curaçao. All directors, officers, employees, counterparties, and third-party consultants associated with Velatus N.V. are committed to adhering to the principles and obligations established in this Policy.

The Board of Directors of Velatus N.V. is responsible for approving the annual framework for the development, implementation, and monitoring of this AML/CTF/CPF Policy. Updates to the Policy may occur periodically to reflect changes in regulations or operational practices. Additionally, urgent modifications may be proposed by a designated compliance officer based on internal reviews or third-party AML audit findings, particularly when addressing new risks or their potential impacts.

This AML/CTF/CPF Policy is designed to mitigate risks related to money laundering and terrorist financing. It establishes a robust compliance framework aligned with local and international regulatory standards. The policy addresses specific risk areas, including customer behavior, payment methods, product offerings, geographic regions, and delivery channels, through a standardized and systematic approach.

In alignment with the legal and regulatory framework of Curaçao, the Policy incorporates key national legislation, such as the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (PB 1993, no. 63) (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), and the National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99), including amendments effective May 16, 2024. It also adheres to the National Ordinance on Identification when Rendering Services (NOIS, N.G. 2017, no. 92), the Sanctions National Ordinance (SNO, N.G. 2014, no. 55), and the Kingdom Sanction Act (N.G. 2016, no. 54).

Additionally, this Policy integrates international best practices, including the Financial Action Task Force (FATF) Recommendations, the European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs), and principles established by the Wolfsberg Group. These standards ensure that Velatus N.V. meets its obligations both locally and globally while maintaining the highest industry compliance standards.

2. iGAMING ENVIRONMENT

Velatus N.V. is a company incorporated under the laws of Curaçao, holding registration number 163778. The company operates the website <https://1xbet.asia/en> under the oversight of a Curaçao online gaming license (license number OGL/2024/1593/0817), issued by the Curaçao Gaming Control Board. This license mandates full compliance with regional regulations and the jurisdictional restrictions established by the Curaçao regulatory framework.

As per these regulatory requirements, Velatus N.V. is prohibited from offering gaming services in restricted jurisdictions, including but not limited to the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. The company ensures that its operations are confined to jurisdictions where online gambling is legally permitted and does not target regions where such activities are prohibited.

The nature of the e-gaming and betting industry presents specific risks related to money laundering. These include, but are not limited to, identity theft, fraudulent activities, structuring and layering of transactions to obscure the origin of funds, and potential collusion between customers, employees, or third-party payment providers to circumvent internal compliance mechanisms. Velatus N.V. remains vigilant in addressing these challenges through stringent anti-money laundering measures and robust internal controls to protect the integrity of its operations.

3. MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

Money Laundering:

Money laundering is a pivotal component of financial crimes and often operates across international borders. It facilitates a range of illegal activities, such as tax evasion, sanctions evasion, fraud, corruption, illegal arms trade, drug trafficking, extortion, and kidnapping. At its core, money laundering seeks to obscure the origins, identity, and destination of illicitly obtained funds, thereby integrating them into the legitimate financial system.

Key Stages of Money Laundering:

1. Placement:

The initial stage involves introducing unlawful funds into the financial system. This may occur through depositing cash into bank accounts, purchasing high-value goods, or engaging in financial transactions. The primary goal is to initiate the process of blending illicit money with legitimate funds.

2. Layering:

During this phase, complex layers of transactions are created to disguise the money's origin. These may include transferring funds between multiple accounts, converting currencies, or investing in diverse financial instruments. This stage complicates tracking the funds' origins by creating a confusing transactional audit trail.

3. Integration:

The final stage sees the laundered funds reintegrated into the economy. This may involve acquiring luxury assets, investing in legitimate businesses, or other lawful financial activities, making the funds appear as though they were legally earned. By this stage, tracing the money back to its criminal roots becomes significantly more difficult.

Online gambling platforms, including casinos, are susceptible to exploitation at any stage of money laundering. Consequently, operators must implement robust measures to prevent anonymous activities and detect suspicious transactions effectively.

Terrorist Financing and Its Link to Money Laundering

Terrorist financing refers to the provision of financial resources to support terrorist operations. Unlike money laundering, such funds may originate from both lawful and unlawful sources. However, similar laundering techniques are employed to obscure their end use. For example, prepaid cards may be utilized to procure materials for terror-related activities. Regular training for employees on the latest typologies and methods of terrorist financing is essential to address this risk proactively.

Risk Management and Mitigation Strategies

Velatus N.V. adopts a proactive approach to manage and mitigate the risks associated with money laundering and terrorist financing. Key measures include:

- Identity Verification and Fraud Prevention:
Rigorous customer due diligence (CDD) is employed, ensuring accurate verification of customer documentation, age, and geographic location.
- Monitoring High-Risk Behaviors:
Systems are in place to detect unusual patterns such as multiple accounts operated by a single individual or significant transaction volumes inconsistent with a player's profile.

- **Addressing Illicit Fund Deposits:**
Mechanisms to identify deposits derived from unlawful activities or misuse of the platform as a temporary holding space for criminal proceeds.
- **Controlling Player-to-Player Transfers:**
Monitoring for inappropriate use of peer-to-peer transfer features to exchange or withdraw funds without engaging in legitimate gambling activities.

This approach is complemented by continuous risk assessments tailored to emerging threats and comprehensive employee training. These practices form the foundation of Velatus N.V.'s AML compliance framework, ensuring adherence to regulatory requirements and fostering a secure operational environment.

Terrorist Financing:

Terrorist financing involves the allocation of financial resources to support terrorist activities, which can range from small-scale operations to large-scale attacks. This financing can stem from both legitimate and illegal sources, each presenting unique challenges in identifying and preventing its use. The overarching goal of terrorist financing is to enable acts of terrorism, undermining national and global security.

Funds used for terrorist financing may originate from lawful income, including business proceeds, charitable donations, or other legitimate financial activities. However, such legitimate channels are often exploited to disguise the true intent behind the financial transactions. On the other hand, illegal sources such as drug trafficking, smuggling, fraud, extortion, and other criminal enterprises also contribute significantly to the financing of terrorism. These illicit revenues are often laundered to obscure their origins before being funneled into terrorist operations.

Terrorist groups employ various methods to move their funds, leveraging both formal and informal financial systems. Traditional banking channels and financial institutions are sometimes used, with techniques like layering and structuring designed to evade detection and obscure the money trail. Alternatively, informal value transfer systems, such as hawala networks, offer a way to transfer funds outside regulated financial systems, making them particularly difficult to monitor and trace.

Recognizing the signs of terrorist financing is crucial in combating this threat. Transactions that deviate significantly from normal behavior, such as large or frequent transfers involving high-risk regions, may indicate the involvement of terrorist financing. Similarly, engagement in financial activities without a clear economic purpose or those conducted in high-risk sectors could also raise red flags. Vigilance in identifying these anomalies is a key part of any robust counter-terrorism financing framework.

To address these risks, institutions must adopt comprehensive regulatory and compliance measures. Anti-money laundering policies serve as a cornerstone, requiring financial institutions to implement thorough customer due diligence (CDD) processes, monitor transactions continuously, and report any suspicious activities promptly. Compliance with global sanctions lists, such as those maintained by the United Nations Security Council or the Office of Foreign Assets Control (OFAC), is also essential in preventing transactions linked to terrorist organizations or activities.

International organizations like the Financial Action Task Force (FATF) play a significant role in setting standards to combat terrorist financing. FATF emphasizes the importance of strong policies to identify and report suspicious activities, while entities like OFAC enforce sanctions against individuals and organizations involved in terrorism. In the European Union, directives aim to prevent the misuse of financial systems, requiring member states to implement effective anti-money laundering measures. Similarly, the United Nations Security Council imposes sanctions and maintains lists of individuals and entities associated with terrorism, forming a critical part of the global effort to disrupt terrorist financing networks.

National regulations further complement these international frameworks, mandating financial institutions to conduct due diligence, monitor financial activities, and report any unusual transactions. By adhering to these regulations and guidelines, institutions contribute to the global fight against terrorism, reducing the resources available to terrorist groups and protecting the integrity of financial systems.

Proliferation Financing:

Proliferation financing refers to the financial support provided for the development, acquisition, or production of weapons of mass destruction (WMDs), including nuclear, chemical, and biological weapons, as well as their delivery systems. Such financing poses severe risks to global security, and Velatus N.V. is fully committed to ensuring that it is not involved in any activities related to the financing of WMDs. As a licensed casino operator in Curaçao, Velatus N.V. follows the regulations set by the Curaçao Gaming Control Board (GCB) and complies with international standards aimed at mitigating the risks associated with proliferation financing.

Proliferation financing can originate from both legitimate and illicit sources. Legitimate sources may include funds from businesses, investments, or charitable donations, which could be exploited to channel money toward the development of WMDs. Velatus N.V. takes significant precautions to ensure that any transactions involving international trade or high-risk regions undergo thorough scrutiny. This helps prevent any misuse of financial activities that could potentially support the creation of dangerous weapons. At the same time, illicit sources such as smuggling, fraud, and money laundering can also contribute to the financing of WMDs. Velatus

N.V. remains vigilant in identifying and preventing these illicit financial activities through a robust monitoring system designed to detect suspicious transactions and activities early on.

The financial channels used for proliferation financing can be both formal and informal. Formal financial systems, such as banks and payment processors, are frequently exploited to transfer funds. These transactions may involve complex layering techniques that obscure the true origin and destination of the money. To address this risk, Velatus N.V. employs advanced transaction monitoring systems that can identify unusual patterns and flag any transactions that appear designed to conceal their purpose. In addition to formal systems, informal financial networks such as trade-based financing or alternative remittance systems (like hawala) can also be used for proliferation financing. These informal systems are much harder to trace since they operate outside the scope of regulated financial institutions. Velatus N.V. takes steps to actively monitor transactions that involve high-risk jurisdictions or goods that could potentially be used in the development of WMDs. This ensures compliance with Curaçao regulations as well as international sanctions.

Velatus N.V. has put in place a comprehensive monitoring system designed to detect potential proliferation financing activities. For example, the company closely watches transactions that involve dual-use goods—items that can serve both civilian and military purposes. Such transactions are carefully examined to ensure they do not inadvertently support WMD development. In addition, Velatus N.V. remains alert to business activities that appear to lack legitimate commercial purposes or that are structured in ways that suggest an attempt to evade detection. Any unusual or large transactions that seem inconsistent with a customer's usual business behavior are flagged for further investigation. Additionally, the company monitors transactions for any signs of money laundering, as these can sometimes be indicative of misdirected funds intended for legitimate uses but actually supporting proliferation activities.

To further mitigate the risks of proliferation financing, Velatus N.V. conducts enhanced customer due diligence (CDD). This process involves thoroughly verifying the identities of customers, particularly those engaged in international trade or operating in industries that may present a higher risk for proliferation financing. The company ensures that all transactions are legitimate and that no funds are being diverted toward activities related to WMDs. Velatus N.V. also uses state-of-the-art transaction monitoring systems to detect irregular patterns in financial transactions, particularly those involving high-risk regions or significant cross-border payments. Any suspicious activity triggers further scrutiny to ensure that the funds are not being used for illicit purposes.

Velatus N.V. is committed to ensuring full compliance with local and international sanctions. The company adheres to sanctions programs implemented by the United Nations, the European Union, and the U.S. Office of Foreign Assets Control (OFAC). These sanctions are specifically designed to prevent financial resources from

reaching entities or individuals involved in the development or proliferation of WMDs. Velatus N.V. ensures that none of its transactions involve sanctioned individuals, organizations, or countries. All transactions are meticulously monitored to ensure compliance with these global efforts to prevent the financing of dangerous weapons.

In addition to Curaçao's regulations, Velatus N.V. also aligns with international best practices in combating proliferation financing. The company follows recommendations set by the Financial Action Task Force (FATF), which provides guidelines for identifying and preventing the misuse of financial systems for proliferation financing. These recommendations ensure that Velatus N.V.'s compliance program remains in line with global standards and is effectively preventing the misuse of its platform for illegal financial activities.

By following both local Curaçao regulations and global standards, Velatus N.V. ensures its operations are free from any involvement in the financing of weapons of mass destruction. Through robust monitoring systems, enhanced customer due diligence, and strict compliance with international sanctions, the company actively contributes to global efforts to prevent the spread of WMDs and support international security.

4. SENIOR MANAGEMENT ROLE

The senior management of Velatus N.V. plays a central role in identifying, assessing, and managing the risks associated with money laundering, terrorist financing, and proliferation financing. The Board of Directors mandates that a designated AML/CTF Officer provide regular updates on any significant changes or issues within the control environment. This officer is also tasked with preparing an annual report that evaluates the effectiveness of the company's risk management systems and controls, ensuring that potential risks in these areas are properly mitigated.

To maintain a proactive approach to risk management, senior management ensures that all relevant policies and procedures undergo comprehensive reviews at least once a year. These reviews are informed by monthly risk assessments, enabling the company to identify weaknesses in its internal controls and risk management practices promptly. If any deficiencies are identified, the AML/CTF Officer has the authority to propose corrective actions for Board approval, further strengthening the company's commitment to effective compliance and risk management.

In alignment with global best practices, senior management is also responsible for overseeing the implementation of a robust employee training program. This program is aimed at enhancing staff awareness of AML, CTF, and CPF risks, ensuring that employees—particularly those in key positions—are well-equipped to identify and appropriately respond to suspicious activities and potential threats.

Moreover, senior management is charged with ensuring that the company's internal control framework is both effective and comprehensive. This includes ensuring proper segregation of duties, clear authorization procedures, continuous monitoring, and thorough documentation practices. To evaluate the continued effectiveness of the AML/CTF/CPF program, regular independent audits and assessments are conducted. These evaluations help identify areas for improvement and ensure ongoing compliance with both local regulations and international standards.

5. RISK ASSESSMENT

The company adopts a risk-based approach (RBA) as a central principle in its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) policies, aiming to allocate resources efficiently to mitigate the most significant risks. This approach is especially critical under the new Curaçao gaming legislation, which emphasizes the importance of a robust RBA to maintain compliance and safeguard the integrity of the gaming sector. The Law on Offshore Games (LOK), which replaces the previous National Ordinance on Offshore Games of Hazard (NOOGH), enforces stricter AML/CTF requirements. Under this framework, the company is required to adopt a comprehensive RBA to identify, assess, and effectively mitigate the risks related to money laundering and terrorist financing.

The cornerstone of the RBA is the company's risk assessment process. The company conducts regular, thorough risk assessments to identify potential risks linked to customers, products, services, and geographic locations. For example, customer risk is evaluated based on factors such as whether the customer is a Politically Exposed Person (PEP), comes from a high-risk jurisdiction, or has a complex business structure. Products and services offered by the casino are also assessed for risk, with particular attention given to those with high transaction volumes or anonymous features. Additionally, the geographic location of customers and operations is considered, identifying high-risk jurisdictions characterized by weak AML/CTF regimes, significant corruption, or a history of terrorist activities.

Once risks are identified, the company implements appropriate mitigation measures that are proportional to the level of risk. These measures include enhanced due diligence (EDD) for high-risk customers and transactions, transaction monitoring systems to detect suspicious activities, and stringent customer verification processes to ensure the legitimacy of transactions. EDD includes gathering additional information about a customer's source of funds, beneficial ownership, and the purpose of their transactions. The company uses advanced algorithms to monitor transactions for patterns indicative of money laundering or terrorist financing, setting alerts for suspicious activities.

Ongoing monitoring and periodic reviews are essential components of the company's risk-based approach. Continuous transaction monitoring ensures that any unusual or suspicious activities are promptly identified. The company updates customer profiles regularly, reflecting new information and transaction histories. Furthermore, the company reviews its AML policies and procedures periodically to ensure they remain aligned with evolving risks and regulatory requirements, making updates when necessary.

Effective reporting and record-keeping are also integral to the RBA. The company ensures that all suspicious activities are reported to the relevant authorities, such as the Financial Intelligence Unit (FIU), in a timely manner. Detailed records are maintained for all customer identification, transaction data, and risk assessments, and these records are kept for the required minimum period, as specified by local legislation. These records are readily accessible for inspection by regulatory authorities to ensure full compliance with applicable laws.

In line with the new Curaçao gaming legislation, the company also implements specific programs for AML, CTF, and Counter-Proliferation Financing (CPF). These programs incorporate the RBA and are tailored to the size, nature, and complexity of the business. Regular training and awareness programs are provided to employees, focusing on the risk-based approach and equipping staff to identify and mitigate AML/CTF/CPF risks effectively. Additionally, the company conducts independent audits to assess the effectiveness of its AML/CTF/CPF programs and the implementation of the RBA.

The company is particularly aware of risks specific to the gambling sector. These risks are addressed through a thorough business and customer-specific risk assessment in key areas such as customer risk, geographical risk, product and service risk, and distribution channel risk.

5.1. Customer Risk

Customer risk is a significant concern in the gambling sector, as certain individuals or groups pose a higher risk for money laundering or terrorist financing. These high-risk customers may include those with multiple income sources, inconsistent income patterns, or involvement in high-spending activities. Additionally, Politically Exposed Persons (PEPs) or individuals using third parties to gamble or purchase chips may also present higher risks. To mitigate these risks, the company performs comprehensive customer due diligence (CDD), with enhanced scrutiny applied to high-risk individuals, including PEPs and large spenders. Ongoing monitoring ensures that customer profiles are regularly updated to reflect any changes in their risk status, and third-party transactions are subject to strict validation.

Customer risk is a critical component of the company's Anti-Money Laundering (AML) strategy. Each customer is assessed to determine the level of due diligence

required, based on factors such as income structure, financial activity, and political exposure.

Customers may be categorized as high-risk due to:

- Multiple income sources, which complicate the verification of legitimate fund origins.
- Irregular or unpredictable financial behavior, making it difficult to establish a risk baseline.
- Politically Exposed Persons (PEPs), due to their proximity to public funds and increased corruption risk.
- Disproportionate spending, where financial activity significantly exceeds declared income.
- Use of multiple gaming accounts, which may indicate attempts to obscure transactional behavior or avoid detection.

To mitigate these risks:

- Standard CDD is applied to low-risk customers with a single, verified income source.
- Enhanced Due Diligence (EDD) is required for high-risk customers, with increased scrutiny of financial documents and transaction patterns.
- Transaction thresholds are used to flag deviations from typical customer behavior.

5.2. Geographic Risk

Geographical risk is another key factor, as the country of origin of funds or the location of customers can influence the risk level. High-risk countries are often those with weak AML/CTF frameworks, significant corruption, or a history of terrorism. The company evaluates the risks associated with each jurisdiction by regularly reviewing credible sources such as FATF's high-risk country list, the U.S. Department of State's INCSR, and the EU's sanctions lists. Stricter due diligence measures are applied to customers from high-risk regions, and these jurisdictions are closely monitored to mitigate the potential threats they pose.

Geographic risk assessment helps determine whether a customer's location or the source of their funds presents increased exposure to financial crime, based on jurisdictional weaknesses or international sanctions.

Higher-risk jurisdictions are identified by:

- Lack of effective AML/CTF frameworks
- High levels of corruption
- Links to sanctioned entities or WMD proliferation

VELATUS N.V. refers to a range of authoritative sources, including:

- Financial Action Task Force (FATF) lists of high-risk countries
- Caribbean Financial Action Task Force (CFATF) advisories
- U.S. Department of State International Narcotics Control Strategy Reports (INCSR)
- European Commission's list of third countries with AML/CFT deficiencies
- Office of Foreign Assets Control (OFAC) sanctions lists
- Transparency International's Corruption Perceptions Index (CPI)

Based on these inputs, the company applies:

- Jurisdiction-based risk classification (low, medium, or high)
- EDD for clients from high-risk countries
- Restrictions on financial activity involving sanctioned jurisdictions
- Ongoing review of geographic risk matrices, ensuring alignment with current global assessments

5.3. Product, Service and Transaction Risks

The nature of the gaming industry makes it inherently vulnerable to exploitation by criminals. Certain payment methods, such as prepaid cards or virtual assets that offer anonymity, are high-risk factors. Transactions such as large deposits, withdrawals, or peer-to-peer transfers also pose potential risks, especially when they involve third parties or anonymous customers. The company addresses these risks by implementing strict identity verification procedures, validating the source of funds for large transactions, and ensuring that casino accounts are used solely for gambling purposes. The company also regulates peer-to-peer platforms and monitors transactions for any signs of fraudulent or illegal activity.

VELATUS N.V. acknowledges that certain gaming products and financial instruments are more susceptible to misuse for ML and TF purposes. The company regularly assesses its service offerings to detect potential vulnerabilities.

Risk-prone features include:

- High-volume transaction services, which may facilitate rapid movement and layering of funds.
- Anonymous payment methods, such as:
 - Prepaid cards
 - Virtual assets (e.g., cryptocurrencies or digital tokens)
- Peer-to-peer transfers, allowing players to move funds without engaging in gaming.
- Misuse of accounts, where funds are deposited and withdrawn with minimal gaming activity.

- Third-party financial tools, such as using someone else's bank card or e-wallet.

Mitigating measures implemented include:

- Verifying all payment sources during onboarding and throughout the customer relationship.
- Accepting payments only through regulated financial service providers.
- Conducting real-time transaction monitoring using automated detection systems.
- Applying EDD protocols to suspicious or atypical activity.
- Training staff to detect and escalate unusual transaction behavior immediately.

5.4. Distribution Channel Risks

Distribution channel risks relate to the type of communication used to establish business relationships. Channels that allow anonymity or non-face-to-face communication with customers increase the risk of identity theft or impersonation. Third parties that serve as intermediaries without being subject to AML/CTF requirements also present a risk. To mitigate these risks, the company ensures proper identification and verification of customers through secure channels, preventing impersonation fraud and ensuring that third parties involved in the transaction are fully vetted.

The way VELATUS N.V. interfaces with its clients—especially through digital and remote channels—also influences its risk exposure. Channels lacking robust verification mechanisms may be exploited to bypass compliance safeguards.

Common vulnerabilities include:

- Non-face-to-face onboarding, increasing the risk of identity fraud.
- Anonymous or partially anonymous platforms, where customer credentials cannot be easily validated.
- Use of third-party intermediaries not subject to regulatory oversight.

To counteract these risks, the company enforces:

- Biometric and two-factor authentication tools during registration and login processes.
- Automated identity verification systems that screen and validate personal data against trusted databases.
- Strict prohibition of anonymous payments or interactions without full verification.
- Ongoing monitoring of all transaction channels to detect unusual access or usage patterns.

By implementing these comprehensive measures and adhering to both local regulations and international standards, the company ensures that its operations effectively mitigate the risks of money laundering, terrorist financing, and proliferation financing, while maintaining the integrity of the gaming sector.

5.5. Technological Risks

VELATUS N.V. is dedicated to ensuring that innovation and the adoption of new technologies do not introduce vulnerabilities that could be exploited for financial crime. As the iGaming industry evolves through digital transformation, the company proactively assesses the risks posed by emerging technologies to ensure full compliance with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) obligations.

The company's strategy centers around embedding technological risk awareness into its compliance framework. This involves detailed assessments of all new systems, services, and operational tools prior to implementation, with a view to identifying any features that could be manipulated for illicit purposes.

Risk Identification and Assessment Procedures

VELATUS N.V. conducts comprehensive risk assessments whenever technological advancements are introduced to the platform. These evaluations are aimed at ensuring that no new product, service, or operational feature undermines the company's ability to detect, prevent, and report financial crimes.

Risk assessments are triggered in the following situations:

- **Launch of new products or services** within the gaming platform.
- **Deployment of new operational practices** aimed at enhancing user experience or internal efficiency.
- **Adoption of novel service delivery mechanisms**, such as:
 - Mobile wallet integrations
 - Real-time account access tools
 - Alternative payment interfaces
- **Integration of advanced technologies**, including:
 - Blockchain transactions
 - Artificial Intelligence (AI)–based services
 - Machine learning algorithms for behavioral analytics
 - Enhanced cybersecurity infrastructure

Prior to rollout, each innovation undergoes a documented evaluation to:

- Identify inherent and residual risks.
- Determine the potential for misuse by criminal actors.
- Ensure compatibility with existing AML/CTF/CPF controls.

- Align with both Curaçaoan and international regulatory standards.

By maintaining audit trails of all assessments, VELATUS N.V. reinforces internal accountability and regulatory transparency.

Implementation of Risk Mitigation Measures

Once risks are identified, the company responds with immediate, proportionate, and forward-looking mitigation strategies. These are designed to protect both the company and its customers from the misuse of technology in financial crime schemes.

Risk mitigation measures include:

- **Reinforcement of Security Protocols**, such as:
 - Multi-factor authentication (MFA)
 - Biometric verification methods
 - End-to-end data encryption
 - AI-powered fraud detection tools
- **Enhancement of Transaction Monitoring Systems:**
 - Automated tools to detect anomalies in real time
 - Pattern recognition algorithms to flag suspicious activities
 - Threshold-based alerts for high-risk transactional behavior
- **Policy Adaptation and Regulatory Alignment:**
 - Regular updates to internal AML/CTF policies
 - Integration of new threat typologies (e.g., deepfake fraud, account takeovers)
 - Alignment with emerging international regulatory guidance

These steps ensure that innovation never comes at the expense of regulatory security or operational integrity.

Ongoing Oversight and Compliance

VELATUS N.V. acknowledges that technological risk is not static. To maintain resilience, the company continuously monitors both internal systems and external technological trends. Regular reviews are conducted to:

- Reassess the risk posture of implemented technologies.
- Update controls in response to emerging threats or vulnerabilities.
- Ensure that compliance policies evolve in line with digital advancements.

This dynamic approach ensures that the company's infrastructure remains both secure and compliant, even as the digital environment becomes increasingly complex.

By integrating technology risk assessments into every stage of its innovation lifecycle, VELATUS N.V. ensures that advancements enhance—not compromise—its AML/CTF/CPF objectives. This proactive stance strengthens the integrity of its gaming platform and reflects a long-term commitment to regulatory excellence in a rapidly evolving sector.

6. COMPLIANCE FUNCTION

6.1. Appointment of MLRO/AMLCO

The company designates a qualified individual to serve as the Money Laundering Reporting Officer (MLRO) or Anti-Money Laundering Compliance Officer (AMLCO). The appointment of the MLRO/AMLCO is a vital component of the company's Anti-Money Laundering (AML) framework. This decision is made by senior management to ensure that the role is both independent and holds the necessary authority to carry out its functions. The individual selected for this position must have relevant experience and expertise in AML compliance, along with the seniority required to oversee the implementation and enforcement of the company's AML policies and procedures. This appointment is formalized through a documented letter that defines the scope of the role and the reporting structure within the organization.

6.2. Functions of the MLRO/AMLCO

The MLRO/AMLCO is entrusted with several critical functions to ensure the effective operation of the company's AML program. Their primary responsibility is to oversee the implementation of the AML policies and procedures, ensuring full compliance with all relevant local and international regulations. As the central point of contact for all AML-related matters, the MLRO/AMLCO is responsible for reviewing and approving the company's AML policies to ensure they align with the current regulatory standards and address emerging risks. They also supervise the company's AML training program, ensuring all employees are sufficiently educated about AML requirements and their roles in maintaining compliance.

6.3. Responsibilities of the MLRO/AMLCO

The MLRO/AMLCO plays an integral role within the company's AML framework, with significant responsibilities in various key areas:

- **Monitoring and Reporting:**

The MLRO/AMLCO is responsible for continuously monitoring transactions and client activities to detect and investigate any suspicious activities. This includes the obligation to file Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) whenever necessary. The MLRO/AMLCO must also ensure that accurate records of all reports are maintained.

- **Policy Development:**

One of the core responsibilities of the MLRO/AMLCO is to develop, update, and adapt the company's AML/CTF/CPF policies and procedures to comply with the latest Curaçao gaming legislation and international best practices. This ensures that the company's AML framework effectively addresses emerging risks and any changes in regulatory requirements.

- **Training and Awareness:**

The MLRO/AMLCO ensures that all employees receive appropriate training on AML/CTF/CPF obligations. This training educates staff on identifying and reporting suspicious activities and enhances their understanding of the company's internal controls. The MLRO/AMLCO regularly reviews and updates training materials to ensure that they reflect the latest legal and regulatory changes.

- **Liaison with Authorities:**

The MLRO/AMLCO serves as the main liaison with regulatory bodies, law enforcement, and other relevant authorities on AML/CTF/CPF matters. This includes responding to requests for information, participating in regulatory inspections or audits, and ensuring the company is fully compliant with all external requirements.

- **Compliance Oversight:**

The MLRO/AMLCO conducts periodic reviews and audits of the AML/CTF/CPF program to assess its effectiveness and ensure ongoing compliance with legal requirements. They must also address any deficiencies identified in these reviews and propose corrective actions to improve the AML framework.

- **Documentation and Record-Keeping:**

The MLRO/AMLCO is responsible for maintaining comprehensive records of all AML/CTF/CPF activities, including SARs, internal reports, training sessions, and updates to policies. These records must be stored in compliance with legal retention requirements and must be accessible to regulatory authorities upon request.

By carrying out these functions and responsibilities, the MLRO/AMLCO plays a critical role in safeguarding the company against the risks of money laundering and terrorist financing. They ensure that the company remains fully compliant with Curaçao's AML/CTF/CPF regulations and follows best practices to mitigate these risks.

7. CUSTOMER DUE DILIGENCE

The company's CDD process includes several key steps to ensure effective identification and risk management:

1. Identification and Verification of Players:

The company ensures that each player's identity is verified using legitimate, reliable, and independent documents, data, and systems. This includes verifying identification for all customers before they are allowed to participate in the casino's services.

2. Ultimate Beneficial Ownership:

For legal entities, the company identifies and verifies the ultimate beneficial owner (UBO) to ensure full transparency about who controls or benefits from the account. The ownership and control structure of any legal entities must be understood and documented.

3. Understanding the Purpose and Nature of the Business Relationship:

The company takes steps to understand the purpose of the customer's relationship with the casino and the typical nature of their business activities. This helps in assessing the legitimacy of the relationship and monitoring for any potential unusual activity.

4. Ongoing Monitoring and Due Diligence:

The company conducts ongoing monitoring of business relationships, regularly reviewing customer transactions to ensure they align with the company's understanding of the player and their risk profile. If necessary, the source of funds will also be reviewed, particularly for high-risk customers.

Casino staff are required to maintain confidentiality regarding any reports made to the FIU. If there is a suspicion of money laundering or terrorism financing, and conducting further due diligence could alert the player, staff are instructed to refrain from notifying the player and instead file a report directly with the FIU. This approach helps prevent tipping off the player and ensures the integrity of the investigation.

7.1. Company's Identification and Verification of Players

The company employs a thorough identification and verification process to establish the identity of its players and ensure compliance with regulatory requirements. Identification involves gathering personal details to confirm the player's identity, while verification confirms the authenticity of the provided information using reliable documents or data. The extent of the information required varies based on the assessed risk level associated with the player.

At a minimum, the company collects the following details for player identification:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number

For low-risk situations, the company may require only the first three details. However, for high-risk scenarios, additional information is requested to mitigate the risks associated with money laundering and terrorism financing.

The company's customer risk assessment procedure helps determine the potential for unusual activity in a player's business relationship. Initially, a provisional risk rating is assigned based on the collected data. This rating is revised as more information is obtained, ensuring that appropriate Customer Due Diligence (CDD) measures are applied.

Verification of identity is a critical step in confirming that the player is who they claim to be. This typically involves:

- A government-issued and valid photo ID (e.g., passport, ID card)
- Additional documents like a utility bill or bank statement (no older than six months) to confirm the address
- Verification of the residential address through letters, email, or phone
- Using biometric checks, cross-referencing with databases, IP addresses, and funding methods

If there are concerns regarding the quality or completeness of the information provided, the company may request additional documentation, such as a selfie of the player holding their ID or require the player to make a deposit through a regulated financial institution in a reputable jurisdiction.

7.2. Business Relationship Purpose and Nature

As part of the CDD process, the company works to understand the purpose and nature of its relationships with players. While the nature of the relationship is generally clear due to the services provided, the company collects sufficient information to evaluate potential risks and detect any unusual or suspicious activity.

In cases where necessary, the company gathers documentation regarding the source of wealth and the expected levels of activity to ensure the legitimacy of the player's income and justify the account's activity. For low and medium-risk players, a declaration containing employment or business details and salary information may suffice. For higher-risk clients, the company obtains reliable and independent

sources of wealth documentation to verify the legitimacy of the player's financial activities. This helps establish the player's behavior model for monitoring and assessing their risk profile.

7.3. Timing of CDD

VELATUS N.V. applies Customer Due Diligence (CDD) measures promptly and consistently, ensuring full alignment with applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. The company integrates a risk-based approach to determine the appropriate timing for CDD implementation, with a focus on early verification and ongoing monitoring.

At the time of account registration, the company collects and verifies key personal information from each customer. This includes the full legal name, residential address, and date of birth, in addition to screening for Politically Exposed Person (PEP) status and checking against applicable sanctions lists. These foundational checks are carried out to establish a legitimate and verifiable business relationship before financial activity begins.

In accordance with VELATUS N.V.'s compliance protocols, CDD is not only conducted at the outset of the relationship but is also triggered by financial thresholds. Specifically, if a customer engages in a single transaction amounting to NAF 4,000 or more, or if multiple transactions cumulatively reach or exceed that value, a full CDD process must be completed. The company maintains a proactive monitoring system that aggregates daily transactional activity per customer, ensuring that all financial movements—regardless of frequency—are assessed in relation to the threshold.

Once the threshold is reached, a comprehensive customer risk assessment is performed. This includes verifying the completeness and accuracy of existing records, conducting additional checks if necessary, and ensuring that any pending CDD obligations are fulfilled without delay. To mitigate risk even further, VELATUS N.V. encourages the completion of full identity verification at the time of registration, rather than waiting for the financial threshold to be crossed. This strategy reduces the opportunity for illicit funds to enter the gaming system prior to due diligence being completed.

In cases where the NAF 4,000 threshold is reached and CDD has not yet been finalized, certain restrictions are applied to preserve compliance. If the threshold is triggered by a deposit, the customer is blocked from making additional deposits or withdrawals but may continue to use existing funds within the gaming platform. If the threshold is met through a withdrawal request, the customer's account is temporarily suspended—halting all gameplay and financial activity—until CDD verification is complete.

Failure to provide the necessary documentation within 30 days of reaching the threshold results in the termination of the business relationship. If there is any suspicion of money laundering or terrorist financing, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU). Where no such suspicion exists, any remaining funds are returned to the customer via the original deposit method. However, if there is reason to believe that the funds are linked to criminal activity, internal procedures are followed to determine whether a fund freeze or further escalation is warranted.

VELATUS N.V. also pays careful attention to avoiding any potential tipping-off during this process. Account freezes and terminations are handled with discretion, and internal protocols guide staff to ensure that regulatory obligations are met without compromising the confidentiality of the investigation. By enforcing these timely and structured CDD practices, the company safeguards its platform, promotes transparency, and remains fully compliant with both national and international financial regulations.

7.4. Existing Customers Monitoring

VELATUS N.V. applies Customer Due Diligence (CDD) not only at the point of onboarding but also throughout the full lifecycle of every client relationship. This ongoing process is rooted in a risk-based compliance framework that allows the company to continuously monitor for financial crime indicators and reassess customer profiles as necessary. By doing so, VELATUS N.V. ensures that all client activity remains consistent with current AML, CTF, and CPF regulatory expectations.

Ongoing due diligence is carried out through the regular monitoring of customer transactions and behavioral patterns, with a particular focus on identifying anomalies or changes in risk level. This enables the company to detect potential threats early and adapt its level of scrutiny accordingly. If previous CDD measures were found to be incomplete or no longer sufficient—especially for accounts established before regulatory standards were enhanced—VELATUS N.V. initiates retrospective due diligence. High-risk clients are prioritized in this process, ensuring that the company addresses the most urgent vulnerabilities first.

Periodic reviews are conducted to keep client data up to date, especially in light of changes to risk exposure or external regulatory developments. Reapplication of CDD measures becomes necessary when a client undergoes a material change in profile. For example, a sudden spike in transaction volume, a shift in geographic location, or the identification of PEP status would all warrant reassessment. Additionally, any customer whose transactional activity meets or exceeds the NAF 4,000 threshold—whether through single or cumulative transactions—is subject to full identity verification and a renewed risk assessment.

Where customers were initially onboarded without the application of formal CDD—such as under legacy policies—VELATUS N.V. takes corrective action by conducting comprehensive verification checks. Again, the level of attention applied is determined by the assessed risk, with high-risk individuals undergoing enhanced due diligence procedures. Regular intervals for CDD updates are also established to ensure ongoing compliance, especially as regulatory standards evolve.

Through this ongoing diligence, VELATUS N.V. ensures that all customer relationships are maintained in accordance with both domestic legislation and international AML/CTF/CPF best practices. This commitment supports the integrity of the company's operations, reduces exposure to financial crime, and demonstrates a proactive compliance posture to regulators and stakeholders alike.

7.5. Enhanced Due Diligence (EDD)

The company's AML/CTF/CPF policy includes stringent Enhanced Due Diligence (EDD) measures for high-risk situations. EDD is mandatory for transactions that exceed the NAF 4,000 threshold, as well as when there is suspicion of money laundering or terrorism financing. In these cases, the company conducts a deeper investigation into the player's background, including verifying the source of funds and wealth, examining transaction patterns, and frequently updating identification details.

For higher-risk individuals, including Politically Exposed Persons (PEPs), their family members, and close associates, the company conducts thorough risk assessments and continuous monitoring. Independent and reliable sources of information are obtained to confirm the legitimacy of the player's financial activities. These robust measures provide a higher level of scrutiny, ensuring the company's compliance with regulatory standards and protecting the integrity of gaming operations.

7.6. Simplified Due Diligence (SDD)

For low-risk scenarios, the company's AML/CTF/CPF policy incorporates Simplified Due Diligence (SDD) measures. SDD is applied when the risk of money laundering or terrorism financing is minimal, allowing for a more streamlined process. In these cases, the company collects only basic identification details, such as full name, date of birth, and residential address. While ongoing monitoring continues, the frequency and intensity of reviews are lower compared to higher-risk situations.

Should any suspicious activity arise or if a player's risk profile changes, the company will promptly escalate the situation by applying enhanced due diligence measures. SDD ensures compliance with regulatory standards while facilitating a smoother and more efficient experience for low-risk players.

7.7. Politically Exposed Persons (PEPs)

The company's AML/CTF/CPF policy includes specific measures for managing relationships with Politically Exposed Persons (PEPs). PEPs, along with their family members and close associates, are subject to heightened scrutiny due to the increased risk of involvement in money laundering and corruption. When a PEP is identified, Enhanced Due Diligence (EDD) measures are immediately implemented.

This includes obtaining senior management approval before establishing or continuing the business relationship, thoroughly understanding the source of the PEP's funds and wealth, and conducting continuous, rigorous monitoring of all transactions. Detailed risk assessments are carried out regularly to detect any suspicious activities, ensuring the company's operations remain compliant with regulatory requirements and uphold the integrity of the gaming environment.

7.8. Reliance on Third Parties and Technological Tools Providers

The company's policy also covers the use of third-party providers for due diligence (CDD) and technological tools. When outsourcing elements of the CDD process or utilizing third-party technological solutions, the company ensures that these providers comply with the same rigorous AML/CTF/CPF standards. Prior to engaging any third-party provider, the company conducts thorough due diligence to verify that they have robust compliance protocols and a proven track record in AML/CTF/CPF adherence.

Regular audits and assessments are conducted to ensure ongoing compliance with the company's AML/CTF/CPF requirements. Contracts with third-party providers must include clauses ensuring cooperation with regulatory inquiries and the provision of relevant data. By ensuring that external partners meet the same high standards, the company enhances its AML/CTF/CPF framework without compromising security and compliance.

7.9. Relationship Termination

If a player is found to be engaged in suspicious activities or fails to provide sufficient information during the due diligence process, the company reserves the right to terminate the business relationship. Such decisions must be supported by documented evidence and approved by senior management. Upon termination, the company will thoroughly review all account activities and report any suspicious transactions to the Financial Intelligence Unit (FIU) immediately. The player's access to casino services will be revoked, and their accounts will be closed in accordance with regulatory guidelines.

Furthermore, the company ensures that all records related to the terminated relationship are securely stored for at least five years, in compliance with legal

retention requirements. This approach helps the company remain vigilant against money laundering and terrorist financing while maintaining compliance with the latest regulatory standards.

8. SANCTIONS

The company's Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) policy mandates strict adherence to both national and international sanctions. We are fully committed to implementing comprehensive procedures that ensure compliance with all applicable sanctions imposed by regulatory bodies and authorities globally. This includes conducting thorough due diligence on all clients and transactions to avoid dealings with individuals, entities, or jurisdictions subject to sanctions. Our policy requires continuous monitoring and immediate reporting of any suspicious activities that could violate these sanctions.

The company ensures that all transactions and client engagements are rigorously screened against updated Sanctions Lists to prevent involvement with sanctioned individuals or entities. This process involves the use of automated systems for real-time checks and maintaining a dynamic database that reflects the most current sanctions information. If any matches or suspicious activities are identified, they must be reported to the relevant authorities without delay. In such cases, appropriate actions, such as freezing accounts or blocking transactions, will be implemented to mitigate compliance risks. Regular reviews and updates of our sanctions compliance procedures will be conducted to ensure alignment with evolving legislation and to maintain robust AML/CTF/CPF practices.

Our sanctions compliance framework includes reference to various sanctions lists and regulations, such as:

- **The Sanctions National Ordinance (SNO, N.G. 2014, no. 55) and the Kingdom Sanction Act (N.G. 2016, no. 54), as well as GCB (Curaçao Gaming Control Board) announcements**
- **EU Sanctions**
- **UN Security Council Consolidated List**
- **UK OFSI Sanctions**
- **US List of Foreign Terrorist Organizations**
- **OFAC Sanctions**

The company's due diligence processes are designed to detect any indirect or covert attempts to engage with sanctioned parties or jurisdictions. Any identified evasion tactics, such as attempts to circumvent sanctions by using third-party intermediaries,

will be promptly reported to the relevant authorities. Immediate corrective actions, including suspending transactions and reviewing affected accounts, will be taken to mitigate any risk.

To ensure ongoing vigilance and compliance with the latest legislative requirements and best practices in preventing sanctions evasion, the company conducts regular audits and provides continuous training for staff. This ensures that all personnel are fully equipped to understand and comply with the latest sanctions regulations, safeguarding the integrity of our operations and reducing any associated risks.

9. SUSPICIOUS ACTIVITY AND TRANSACTION REPORTING

VELATUS N.V. is firmly committed to the identification and reporting of activities that may be indicative of money laundering (ML) or terrorist financing (TF). The company upholds a strong internal culture of vigilance, requiring all staff members to remain alert to red flags—such as unusual client behavior, large or irregular financial movements, or interactions involving jurisdictions considered high-risk. Any concerns that arise must be reported immediately to the designated Compliance Officer, who is responsible for conducting a thorough review and determining whether further internal action or external reporting to the appropriate regulatory authorities is necessary.

Transactions that deviate significantly from a customer's normal financial behavior are considered potentially unusual and merit further examination. Such anomalies may include large or uncharacteristic deposits or withdrawals, transactions involving unknown third parties, or financial operations lacking a clear legal or economic justification. VELATUS N.V. uses automated monitoring systems to help detect such deviations. When an alert is triggered, the information is escalated to the Compliance Officer for deeper analysis.

The following categories of transactions, whether completed or attempted, are considered indicators of potential ML/TF risk and may trigger internal review or formal reporting obligations:

- Transactions that have already been reported to law enforcement or prosecutorial authorities due to concerns related to money laundering or terrorism financing are automatically considered unusual and subject to additional scrutiny.
- Dealings involving individuals or entities subject to sanctions under the Sanctions National Ordinance (N.G. 2014 no. 55), or any party listed by the

competent authorities as sanctioned, are also classified as unusual and may be subject to escalation and reporting.

- Financial transactions equal to or exceeding the threshold of NAF 5,000—whether executed in a single instance or accumulated through multiple smaller transactions within a single gaming day—are treated as unusual and warrant closer examination. This applies regardless of the payment method, whether via cash, electronic transfer, check, or any other means. Such transactions may include significant deposits or withdrawals, purchases of gaming tokens or credits, and payout requests at or above this value.

Where reasonable suspicion exists—based on behavioral cues, contextual risks, or transactional indicators—that a financial activity may be connected to money laundering or the financing of terrorism, the transaction must be treated as presumptively suspicious and escalated without delay.

To safeguard the integrity of the reporting process, VELATUS N.V. enforces strict confidentiality regarding Suspicious Activity Reports (SARs). Employees are expressly prohibited from disclosing any information related to SARs to the customer in question or to any unauthorized individuals. This measure is critical to preventing the risk of tipping off the subject of an investigation, interfering with regulatory inquiries, or compromising legal proceedings.

All information related to suspicious activity is managed with the utmost discretion. Only the Compliance Officer and select, authorized members of the compliance function are permitted to access or discuss such matters. Staff are trained to understand their confidentiality obligations and the serious consequences of any breach.

Any violation of this confidentiality requirement is treated as a major compliance infraction and may result in disciplinary action, up to and including termination of employment. These safeguards ensure that the company's reporting mechanism remains effective, secure, and compliant with AML/CTF/CPF standards.

By fostering a reporting culture grounded in discretion, accountability, and regulatory alignment, VELATUS N.V. reinforces its commitment to combating financial crime and protecting the integrity of its operations.

10.AML/CTF/CPF AUDIT

In accordance with the new Curaçao gaming legislation, the company is required to undergo an independent audit of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) measures. This chapter outlines the framework for conducting such audits, detailing the role of independent auditors and the examination process conducted by the Curaçao Gaming Control Board (GCB).

The primary goal of the independent annual AML/CTF/CPF audit is to assess the effectiveness and compliance of the company's AML/CTF/CPF policies and procedures. This audit is crucial to ensure the organization adheres to the latest legal standards and best practices in mitigating risks related to money laundering and terrorism financing. The audit will encompass a thorough review of the AML/CTF/CPF program, including risk assessments, transaction monitoring systems, staff training programs, and reporting mechanisms.

To ensure impartiality and thoroughness, the company engages an independent and adequately resourced internal audit team or external auditor. The chosen auditor must be certified, have expertise in AML/CTF/CPF compliance, and be independent of the organization's AML compliance staff to avoid any conflicts of interest. The selection process must be transparent, taking into account the auditor's experience, qualifications, and industry reputation. The auditor must also be approved by the Curaçao Gaming Control Board to ensure they meet the regulatory requirements outlined in Curaçao's gaming legislation.

The independent audit is conducted in compliance with international auditing standards and the specific requirements set by the Curaçao Gaming Control Board. Key procedures involved in the audit include, but are not limited to:

- **Review of AML/CTF/CPF Policies and Procedures:**
Ensuring that the company's policies are up-to-date and compliant with legal requirements.
- **Assessment of the Risk Management Framework:**
Evaluating the adequacy of risk assessments and the effectiveness of mitigation strategies in place.
- **Examination of Transaction Monitoring Systems:**
Verifying the effectiveness of systems designed to detect and report suspicious activities.
- **Evaluation of Staff Training Programs:**
Assessing the comprehensiveness and effectiveness of the training provided to employees regarding AML/CTF/CPF obligations.

- **Audit of Reporting Mechanisms:**
Reviewing the company's processes for reporting suspicious transactions and compliance-related issues.
- **Review of Customer Files:**
Ensuring compliance with Know Your Customer (KYC), Know Your Business (KYB), and Customer Due Diligence (CDD) procedures.

Upon completing the audit, the independent auditor will prepare a detailed report that outlines their findings, recommendations, and any identified deficiencies. This report must be submitted to both the company's senior management and the Curaçao Gaming Control Board. The company is required to respond to the audit findings and implement corrective actions within a specified timeframe. Follow-up audits may be conducted to ensure that corrective measures have been effectively implemented and that compliance with regulatory standards is maintained.

The Curaçao Gaming Control Board (GCB) oversees the AML/CTF/CPF compliance of all licensed entities, including reviewing independent audit results and conducting its own examinations to verify compliance with regulatory requirements. The GCB has the authority to request additional documentation, conduct onsite inspections, and review the implementation of audit recommendations.

The examination process by the GCB follows several key steps:

- **Review of Audit Reports:**
The Board reviews the auditor's report to assess compliance with AML/CTF/CPF regulations and to identify areas of concern.
- **Onsite Inspections:**
The Board may perform onsite inspections to verify the accuracy of the audit findings and ensure that corrective actions have been implemented effectively.
- **Interviews and Documentation Review:**
The Board may conduct interviews with key personnel and review relevant documentation to ensure a comprehensive understanding of the company's AML/CTF/CPF practices.

Entities found to be non-compliant with AML/CTF/CPF regulations, based on the audit findings or the Board's examination, may face regulatory sanctions. These sanctions can range from fines and operational restrictions to suspension or revocation of the gaming license. The company is committed to working closely with the Gaming Control Board to take corrective actions where required, ensuring full compliance and preventing future violations.

11. TRAINING AND RECORD KEEPING

The company maintains a comprehensive Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) training program for all employees. The primary goal of this training is to equip employees with the knowledge and skills necessary to detect, prevent, and report money laundering and terrorism financing activities. This training ensures that employees are well-versed in their legal obligations, can recognize suspicious activities, and understand the internal procedures for reporting such activities. A well-trained workforce is vital for the effective implementation of AML/CTF/CPF policies and plays a significant role in maintaining the integrity and reputation of the gaming industry.

The training program is tailored to the specific roles and responsibilities of employees and is provided to all staff, including but not limited to:

- Senior management
- Compliance officers
- Customer-facing staff
- Operational staff
- Any employees involved in financial transactions or customer interactions

Initial Training and Ongoing Refresher Courses

Upon hire, all new employees undergo initial AML/CTF/CPF training. Additionally, all employees receive refresher training at least annually to ensure they remain up-to-date with any changes in legislation or internal procedures. Employees in roles that involve higher exposure to money laundering or terrorism financing risks may be required to undergo more frequent training sessions.

Training Topics

The training program covers a broad range of topics to ensure comprehensive knowledge and understanding, including:

- An overview of AML/CTF/CPF laws and regulations in Curaçao
- Internal AML/CTF/CPF policies and procedures
- Employee roles and responsibilities in AML/CTF/CPF compliance
- Customer identification and verification procedures (KYC/CDD)
- How to recognize and report suspicious activities and transactions
- Record-keeping and documentation requirements
- Consequences of non-compliance for individuals and the organization
- Recent trends and typologies in money laundering and terrorism financing

Training Delivery Methods

To maximize the effectiveness and accessibility of the training program, it is delivered through various methods, including:

- In-person workshops and seminars
- Online courses and webinars
- Interactive e-learning modules
- Case studies and practical exercises
- Role-playing scenarios

A combination of these methods is recommended to accommodate different learning styles and reinforce key concepts.

Qualified Trainers

Training is conducted by qualified professionals with expertise in AML/CTF/CPF compliance. Internal compliance officers may lead the training, or the company may engage external consultants and training providers. It is essential that trainers stay updated with the latest legal requirements and industry best practices to ensure that training content remains current, relevant, and accurate.

Record Keeping

The company adheres to stringent record-keeping practices to comply with AML/CTF/CPF regulations. We maintain comprehensive and accurate records, including customer identification details, transaction information, suspicious activity reports (SARs), training logs, and audit records. These records are securely stored for a minimum of five years, as required by law, and are protected by encryption and access controls to prevent unauthorized access. Regular security audits ensure the integrity and security of the stored data.

The records are organized and easily retrievable to facilitate prompt access by authorized personnel and regulatory authorities. Internal monitoring and periodic audits are conducted to verify compliance with record-keeping requirements. Effective record-keeping is essential for ensuring regulatory compliance, supporting audits, and preserving the integrity of the gaming industry. By maintaining these rigorous practices, the company ensures that it is prepared for regulatory inspections and audits and is fully aligned with AML/CTF/CPF obligations.

12. ANNEXES

12.1. Key Abbreviations:

- **AML** – Anti-Money Laundering

- **BoD** – Board of Directors of the Company
- **CFATF** – The Caribbean Financial Action Taskforce (an organization of 24 states in the Caribbean Basin, Central and South America)
- **Compliance Officer** – A senior management member responsible for detecting and deterring ML/TF/CPF risks, independent from the games operations
- **CTF** – Counter-Terrorism Financing
- **CPF** – Counter-Proliferation Financing
- **CDD** – Customer Due Diligence
- **EDD** – Enhanced Due Diligence
- **FIU** – The Financial Intelligence Unit Curaçao, as referenced in Art. 2 of the **Norut**
- **KYB** – Know Your Business
- **KYC** – Know Your Customer
- **SOF/SOW** – Source of Funds/Wealth
- **UBO** – Ultimate Beneficial Owner
- **SAR/STR** – Suspicious Activity Report/Suspicious Transaction Report
- **PEP** – Politically Exposed Person
- **UN** – United Nations
- **EU** – The European Union
- **UK** – The United Kingdom
- **US** – The United States
- **OFAC** – Office of Foreign Assets Control
- **FATF** – Financial Action Task Force
- **NOOGH** – The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, P.B. 1993, no. 63)

12.2. Key Definitions

- **Money Laundering**
The process of concealing or disguising illicitly obtained funds to make them appear legitimate, involving the placement, layering, and integration phases.
- **AML Policy**
A policy designed to prevent money laundering and terrorist financing. It includes written internal policies, procedures, and controls managed by an AML compliance team led by a Money Laundering Reporting Officer (MLRO), who oversees AML training and arranges independent program audits.
- **Anti-Money Laundering and Counter-Financing of Terrorism Program**
Programs developed to combat money laundering and terrorist financing. These include internal policies, procedures, and controls, and are monitored by the AML compliance team led by the MLRO, who is also in charge of AML training and program audits.
- **Money Laundering Reporting Officer (MLRO)**
The individual responsible for overseeing anti-money laundering activities,

filing suspicious transaction reports, and implementing AML strategies and policies.

- **Alert**
A notification indicating that an analysis is needed due to discrepancies flagged by predefined red flags and typologies.
- **The Curaçao Gaming Control Board (GCB)**
The supervisory authority for AML/CTF compliance for the entire gaming sector in Curaçao.
- **Automated Screening Tool (AST)**
Software used to automate the screening of customers, including checking against sanctions lists.
- **Beneficial Owner**
The individual who ultimately owns or controls an account through which a transaction is executed.
- **Blacklist**
An internal list of names (including entities, individuals, and locations) screened to detect any sanctions exposure, in addition to government and vendor-maintained sanctions lists. The FATF blacklist specifically lists countries deemed noncooperative in combating money laundering and terrorist financing.
- **Comprehensive Sanctions**
Sanctions that ban all transactions and activities with a sanctioned country, except in rare, specific cases.
- **Criminal Proceeds**
Property obtained, directly or indirectly, through the commission of a crime.
- **Customer**
An individual who opens an account and engages in transactions with the company.
- **Customer Relationship**
All interactions with a prospective customer during onboarding and throughout their use of the company's services and products.
- **Know Your Customer (KYC)**
Policies and procedures for verifying the identity of a customer and understanding their typical activity to identify any unusual or suspicious behavior.
- **Know Your Employee (KYE)**
Policies and procedures for understanding employees to detect conflicts of interest, money laundering, past criminal activity, and suspicious behavior.
- **Due Diligence**
The process of investigating and examining an individual or legal entity before engaging in a business transaction. This is done prior to initiating any transaction or business relationship.
- **Customer Due Diligence (CDD)**
Internal controls used to verify a customer's identity, predict transaction types,

and assess risks like money laundering and sanctions. CDD also helps guard against fraud and ensures compliance with relevant laws.

- **Enhanced Due Diligence (EDD)**

Additional measures applied to higher-risk customers to better understand their nature, business, and transactions compared to standard or lower-risk customers.

- **High-Risk Third Country**

A country flagged by the European Commission and FATF due to significant deficiencies in its AML/CFT regime, posing threats to the financial system of the Union. It is also categorized as high risk by the company according to its risk assessment.

- **Economic Sanctions**

Trade or financial restrictions imposed by one or more countries to influence behavior or policy. These can include tariffs, trade restrictions, and financial limitations.

- **Mandatory Sanctions Lists**

Sanctions lists required to be screened against, such as those from UN Security Council Resolutions. Local sanctions may also be mandatory depending on the country.

- **Egmont Group of Financial Intelligence Units**

An international network of financial intelligence units (FIUs) that promotes the development of FIUs and cooperation in information exchange, training, and expertise to combat money laundering and terrorism financing.

- **Embargo**

An official ban on trade or commercial activity with a specific country or product, such as grain or oil.

- **European Union (EU)**

An economic and political union of European countries established by the Treaty of Maastricht in 1992. The EU's directive on preventing the use of the financial system for money laundering and terrorist financing, first adopted in 1991 and updated periodically, mandates EU member states to address these risks.

- **Exclusions List**

A list of names confirmed by the compliance team to not match any names on sanctions lists, thus excluded from the screening process.

- **Financial Action Task Force (FATF)**

An international body formed in 1989 to promote global anti-money laundering and counter-terrorist financing measures. It sets standards and publishes typology reports on current money laundering and terrorist financing trends.

- **Greylist**

A list of countries or entities identified as having strategic deficiencies in their AML/CFT regimes. These entities have not made adequate progress to address FATF's concerns.

- **Financial Intelligence Unit (FIU)**
A national agency responsible for receiving, analyzing, and forwarding reports on suspicious transactions to appropriate authorities.
- **First Line of Defense**
The initial level within a sanctions compliance program, consisting of relationship managers and customer-facing employees who are responsible for gathering sufficient information for effective customer screening.
- **Inherent Risk**
The level of risk present before applying any controls to mitigate it. Categories include customers, products, services, countries, and delivery channels.
- **Investigation**
The process of gathering and analyzing information about an individual or entity in response to a potential sanctions violation alert, starting with simple checks and possibly escalating to more detailed actions.
- **Layering**
The phase in the money laundering process where illegal proceeds are distanced from their source through complex financial transactions to obscure their origin.
- **Minor**
An individual under 18 years of age.
- **Monitoring**
The process of reviewing customer activity for unusual patterns or transactions that deviate from expected norms, often using software to detect anomalies.
- **Office of Foreign Assets Control (OFAC)**
A US Treasury Department agency that administers and enforces economic sanctions against foreign entities and individuals. It manages the Specially Designated Nationals (SDN) list.
- **Politically Exposed Person (PEP)**
An individual holding a prominent public function in a foreign country, including heads of state, senior officials, and their close associates. PEP definitions can vary by jurisdiction.
- **Red Flag**
A warning indicator that signals a potentially suspicious situation, transaction, or activity.
- **Regulatory Agency**
A government body responsible for supervising financial institutions, issuing regulations, conducting examinations, and enforcing penalties.
- **Risk Appetite**
The level of risk a firm is willing to accept in pursuit of its objectives, reflecting its risk management philosophy and influencing resource allocation.
- **Risk Assessment**
A tool used to identify and evaluate the extent of potential risks a business might face.

- **Risk-Based Approach**
A method of assessing and managing risks associated with different types of business, clients, and transactions to enhance the effectiveness of an AML program.
- **Second Line of Defense**
The part of the sanctions compliance program responsible for monitoring, reviewing, and ensuring the effectiveness of controls established by the first line of defense. It includes the compliance function, human resources, and technology departments.
- **Senior Management**
An individual with sufficient knowledge and authority within the company to make decisions affecting its money laundering and terrorist financing risk exposure.
- **Structuring**
The practice of making small transactions to avoid recordkeeping requirements or AML alerts.
- **Sanctions**
Punitive measures imposed to induce a change in behavior or policy, including trade, financial, diplomatic, and movement restrictions.
- **Sanctions Evasion**
The deliberate act of hiding or obscuring the involvement of sanctioned entities or individuals in transactions to avoid detection and penalties.
- **Sanctions Due Diligence (SDD)**
A process focusing on sanctions-specific risks,