

GAMEPLAY INTERNATIONAL B.V.

Reg. Number: 148409

Dr. H. Fergusonweg 1, Willemstad, Curaçao

AML/CTF/CPF POLICY

February 2025

Approved by the Board of Directors

Contents:

- 1. Statement**
- 2. Abbreviations & Definitions**
- 3. iGaming Landscape**
- 4. Money Laundering, Terrorism Financing & Proliferation Financing**
- 5. Sanctions Compliance**
- 6. Risk-Based Approach**
 - 6.1. Risk Factors**
 - 6.2. Technological Developments Risk Assessment**
- 7. Client Due Diligence**
 - 7.1. Detailed Customer Due Diligence Measures**
 - 7.2. Player Identification & Verification**
 - 7.3. Understanding the Relationship**
 - 7.4. Ongoing Monitoring & Compliance**
 - 7.5. Simplified & Enhanced Due Diligence**
 - 7.6. Timing of Customer Due Diligence Measures**
 - 7.7. Customer Due Diligence for Existing Clients**
 - 7.8. Termination of Business Relationships**
 - 7.9. Third-Party Reliance for Customer Due Diligence**
- 8. Suspicious Activity Reporting**
- 9. Compliance Officer**
- 10. Independent Audit**
- 11. Responsibilities of the Management**
- 12. Training & Record Keeping**

1. Statement

GAMEPLAY INTERNATIONAL B.V. is dedicated to the prevention of financial crimes, including money laundering, terrorism financing, and proliferation financing. To achieve this, the company has instituted a comprehensive Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (AML/CTF/CPF Policy), which ensures compliance with both national and international regulatory frameworks. This policy serves as a structured risk management approach covering essential operational areas such as customer interactions, product and service offerings, payment channels, geographic locations, and service delivery methods, aligning with the highest regulatory standards and ensuring strict adherence to all relevant legal obligations.

The Board of Directors (BoD) of GAMEPLAY INTERNATIONAL B.V. is responsible for the approval, enforcement, and oversight of this AML/CTF/CPF Policy. To maintain its effectiveness, the policy undergoes an annual review, with amendments introduced as necessary to reflect regulatory updates or operational adjustments. Additionally, a designated compliance officer is authorized to recommend immediate updates to the policy based on findings from internal or external AML audits, ensuring that any potential risks are promptly mitigated.

GAMEPLAY INTERNATIONAL B.V. strictly follows key international and Curaçao regulatory mandates concerning anti-money laundering, counter-terrorism financing, and counter-proliferation financing. Compliance with these regulations is an essential requirement for maintaining an iGaming license under the Curaçao jurisdiction. The legal framework governing these obligations includes:

- The National Ordinance on Identification When Rendering Services (NOIS) (N.G. 2017, no. 92) - Article 2(8) and Article 11(3)
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99) - Article 22mm(3)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)

The Curaçao Gaming Control Board (GCB) provides a structured compliance framework guiding casinos and online gambling operators in adhering to these regulations. This framework serves as the foundation for GAMEPLAY INTERNATIONAL B.V.'s internal policies and procedures aimed at reducing financial crime risks.

GAMEPLAY INTERNATIONAL B.V. complies with various regulatory provisions, including but not limited to:

- National Ordinance on Identification of Clients When Rendering Services (N.G. 2017, no. 92)
- National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
- Ministerial Decree (November 11, 2015) - Regulation Indicators Unusual Transactions (N.G. 2015, no. 73)

- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- National Decree on the Enforcement of the Kingdom Sanction Law (N.G. 2017, no. 2)
- National Decree (July 10, 2015) - Implementation of UN Security Council Resolutions (N.G. 2015, no. 29)
- National Decree (July 10, 2015) - Sanctions Ordinance Libya (N.G. 2015, no. 28)
- National Decree (July 10, 2015) - Extension of Validity Sanction Decrees 2018 (N.G. 2018, no. 34)
- The Penal Code (Code of Criminal Law) (N.G. 2011, no. 48)

These laws, in conjunction with regulations stemming from NOIS, NORUT, the Sanctions National Ordinance, and the Kingdom Sanction Law, form the core legal framework governing the Curaçao gaming sector's AML/CTF/CPF responsibilities.

Beyond compliance with local regulations, this policy integrates global best practices and follows guidelines established by key international organizations, including:

- Financial Action Task Force (FATF) Recommendations
- European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs)
- The Wolfsberg Principles

By incorporating these international frameworks, GAMEPLAY INTERNATIONAL B.V. reinforces its commitment to preventing financial crimes and ensuring its regulatory approach aligns with global standards.

The AML/CTF/CPF Policy of GAMEPLAY INTERNATIONAL B.V. is designed to meet the compliance requirements set by the Curaçao Gaming Control Board. All directors, officers, employees, and third-party compliance auditors are required to fully comply with and uphold the principles outlined in this policy. Through strict enforcement and continuous monitoring, GAMEPLAY INTERNATIONAL B.V. remains dedicated to fostering a secure and legally compliant gaming environment while preventing illicit financial activities within its operations.

2. Abbreviations & Definitions

AML (Anti-Money Laundering) – A set of laws, regulations, and procedures designed to prevent money laundering and other financial crimes.

CTF (Counter-Terrorism Financing) – The process of identifying and preventing financial transactions that support terrorist activities.

CPF (Counter-Proliferation Financing) – Measures aimed at stopping financial support for the spread of weapons of mass destruction.

KYC (Know Your Customer) – Procedures used to verify the identity of customers and monitor their financial activities.

CDD (Customer Due Diligence) – A process of verifying customer identity, assessing

risk, and monitoring transactions to detect potential illicit activity.

EDD (Enhanced Due Diligence) – Additional verification and risk assessment measures applied to high-risk individuals, businesses, or transactions.

UBO (Ultimate Beneficial Owner) – The individual who ultimately owns or controls an account or financial transaction.

SOF/SOW (Source of Funds/Source of Wealth) – Verification of the origin of financial assets to ensure they are not derived from criminal activities.

PEP (Politically Exposed Person) – An individual holding a high-profile political or public function who requires additional scrutiny due to increased financial crime risks.

SAR/STR (Suspicious Activity Report/Suspicious Transaction Report) – A report submitted to regulatory authorities when a transaction or financial activity appears suspicious or unusual.

FIU (Financial Intelligence Unit of Curaçao) – The national agency responsible for analyzing and processing reports on suspicious financial transactions.

BoD (Board of Directors) – The company's governing body responsible for compliance oversight, corporate governance, and regulatory adherence.

Compliance Officer – A senior official responsible for managing AML/CTF/CPF risks, ensuring compliance with financial crime regulations, and operating independently from gaming operations.

NOOGH (National Ordinance on Offshore Games of Hazard) – Curaçao's legislative framework governing offshore gaming activities.

OFAC (Office of Foreign Assets Control) – A U.S. Treasury Department agency that enforces economic sanctions against targeted individuals, entities, and countries.

FATF (Financial Action Task Force) – An international organization that develops and promotes global AML and CTF standards and monitors high-risk jurisdictions.

CFATF (Caribbean Financial Action Task Force) – A regional group of Caribbean, Central, and South American countries dedicated to combating money laundering and terrorist financing.

EU (European Union) – A political and economic union that enforces AML/CTF directives among its member states.

UK (United Kingdom) – A jurisdiction with AML/CTF regulations overseen by its financial and regulatory authorities.

US (United States) – A country with financial crime oversight conducted by agencies such as OFAC and FinCEN.

Risk-Based Approach (RBA) – A methodology for assessing and managing AML/CTF risks based on transaction types, customer profiles, and jurisdictions.

Blacklist – A list of individuals, businesses, or jurisdictions subject to financial restrictions due to regulatory concerns.

Sanctions – Legal restrictions imposed on specific countries, individuals, or entities due to financial crime, national security risks, or geopolitical concerns.

Automated Screening Tools (AST) – Software that screens customers against sanctions lists and flags high-risk individuals or transactions.

Economic Sanctions – Financial and trade restrictions imposed by governments or regulatory bodies to restrict illicit financial activity.

Curaçao Gaming Control Board (GCB) – The primary supervisory authority responsible for overseeing AML/CTF compliance in the gaming sector.

Know Your Business (KYB) – The process of verifying business entities, their ownership structures, and financial activities for compliance purposes.

Structuring – A money laundering technique that involves breaking large transactions into smaller amounts to evade reporting thresholds.

Layering – A method used to disguise the source of illicit funds by conducting multiple, complex transactions.

Integration – The final stage of money laundering, in which illicit funds are reintroduced into the legitimate economy.

Sanctions Evasion – Attempts to circumvent restrictions by disguising transactions involving sanctioned individuals, entities, or countries.

Financial Action Task Force (FATF) – A global authority that sets AML/CTF compliance standards and issues blacklists and greylists for high-risk countries.

First Line of Defense – Employees responsible for collecting customer information and identifying suspicious activity during onboarding and transaction processing.

Suspicious Transaction Report (STR) – A report submitted to regulatory authorities when a transaction raises AML/CTF concerns.

Egmont Group of FIUs – An international network of Financial Intelligence Units that facilitates cooperation and intelligence-sharing in financial crime investigations.

The Wolfsberg Group – An association of major global banks that develops best practices for private banking AML compliance.

Money Laundering Reporting Officer (MLRO) – The designated officer responsible for overseeing AML policies, conducting transaction monitoring, and submitting SARs/STRs.

Audit Logs – Records maintained for compliance and regulatory review, documenting AML/CTF efforts and stored for a minimum of five years.

Reporting Mechanism Audit – A process that ensures SARs and other compliance reports meet legal standards and are properly documented.

Unusual Transaction – A financial activity that deviates from normal transaction patterns and may indicate illicit activity.

Transaction Monitoring – The real-time analysis of financial transactions to identify suspicious behavior and detect money laundering risks.

High-Risk Third Country – A jurisdiction identified by FATF or the European Commission as having insufficient AML/CTF controls.

Comprehensive Sanctions – The strictest level of sanctions, prohibiting all financial dealings with a sanctioned country, individual, or entity.

Sanctions Compliance and Screening – The process of verifying customers and transactions against international sanctions lists to prevent illicit financial activity.

Operational Restrictions – Limitations imposed on businesses that fail to comply with AML/CTF regulations, including license suspensions and financial penalties.

Risk Appetite – The level of risk an organization is willing to accept within its AML/CTF compliance framework.

Beneficial Owner – The individual who ultimately controls or benefits from a financial transaction or legal entity.

Financial Crime Prevention Framework – A structured program designed to mitigate money laundering, terrorist financing, and other financial crimes.

Customer File Review – A compliance practice where customer records are

periodically examined to ensure adherence to KYC, CDD, and regulatory requirements.

Senior Management Oversight – The responsibility of executive leadership to ensure that AML/CTF/CPF programs are effectively implemented and continuously improved.

Training and Awareness Programs – Educational initiatives designed to ensure employees understand AML/CTF risks, compliance obligations, and reporting procedures.

Ongoing Monitoring – A continuous review of customer transactions and risk profiles to identify potential financial crime risks.

Regulatory Reviews – Assessments conducted by supervisory authorities to verify that a company's AML/CTF policies and practices meet legal requirements.

Corrective Action Plans – Compliance strategies implemented in response to audit findings or regulatory enforcement actions.

Periodic Independent Audits – External reviews of a company's AML/CTF/CPF compliance framework to identify gaps and improve regulatory adherence.

Internal Control Mechanisms – Policies and procedures designed to safeguard against financial crime risks and ensure compliance with AML regulations.

Real-Time Risk Assessment – The use of technology and compliance teams to assess and respond to potential money laundering threats as transactions occur.

Confidentiality in Reporting – The requirement to protect information related to SARs/STRs, preventing unauthorized disclosure or tipping off of customers.

3. iGaming Landscape

GAMEPLAY INTERNATIONAL B.V. is a legally registered entity in Curaçao that operates the website <https://bizbet.io/en>. The company holds an online gaming license issued by the Curaçao Gaming Control Board (OGL/2024/511/0630), ensuring full compliance with licensing regulations and regional restrictions set by Curaçao regulatory authorities. These regulations strictly prohibit remote gaming licensees from offering services in specific jurisdictions, including the United States, Australia, the Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. As a result, GAMEPLAY INTERNATIONAL B.V. operates exclusively in legally authorized markets and does not target customers in regions where online gambling is restricted or prohibited.

As with other e-gaming and betting operators, GAMEPLAY INTERNATIONAL B.V. faces potential money laundering risks, such as identity theft, fraudulent activities, structuring, layering, and the possibility of collusion among employees, customers, or third-party payment providers seeking to circumvent internal security measures. To mitigate these risks, the company has established a robust AML/CTF/CPF framework, implementing strict security protocols and due diligence measures to prevent illicit financial activities within its operations.

4. Money Laundering, Terrorism Financing & Proliferation Financing

Money Laundering:

Money laundering plays a critical role in financial crimes, often involving international transactions and operations. It is associated with a range of illegal activities, including tax fraud, corruption, sanctions evasion, drug trafficking, illicit arms trade, extortion, and kidnapping. The primary purpose of money laundering is to obscure the illegal origins of financial gains, making it difficult to trace their source, ownership, and ultimate destination.

The Three Stages of Money Laundering

1. **Placement** – This initial phase involves introducing illegally obtained funds into the financial system. This can occur through bank deposits, acquiring high-value assets, or conducting various financial transactions. The objective at this stage is to begin integrating illicit proceeds into the legitimate economy.
2. **Layering** – During this stage, funds are transferred through multiple transactions to create complexity and obscure their origins. This may involve moving money between multiple accounts, converting funds into different currencies, or investing in financial instruments. The intent is to make tracing the transactions back to their criminal source increasingly difficult.
3. **Integration** – In the final phase, laundered funds are reintroduced into the legal economy. This may involve purchasing luxury assets, investing in cash-intensive businesses, or engaging in other seemingly lawful financial activities. At this stage, the illicit funds appear legitimate, making them harder to identify and track.

Money laundering can take place at various points within financial transactions, and online gambling platforms are particularly vulnerable to exploitation. This highlights the necessity of preventing anonymous transactions and promptly identifying suspicious activity.

Terrorist Financing and Its Link to Money Laundering

Terrorist financing refers to the movement of funds intended to support terrorist activities. Unlike traditional money laundering, these funds may come from lawful sources but are processed in a manner that mirrors laundering techniques. For example, prepaid cards are often used to finance terrorist operations by purchasing supplies for attacks.

To mitigate such risks, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) ensures that employees receive continuous training on emerging trends and evolving threats associated with terrorist financing.

Risk Management and Compliance Measures

To proactively combat money laundering risks, GAMEPLAY INTERNATIONAL B.V. has implemented comprehensive compliance measures to identify, assess, and mitigate potential threats. These include:

- Fraud Prevention and Identity Verification – Conducting customer due diligence (CDD) through document verification, age authentication, and location validation.
- Monitoring Multiple Accounts and High-Value Transactions – Identifying irregular account behavior, such as the use of multiple accounts or frequent large transactions.
- Detecting Suspicious Deposits – Screening for funds that may originate from illicit activities and ensuring the platform is not misused as a temporary holding space for such transactions.
- Player-to-Player Transfers – Monitoring transactions between users to detect potential misuse for laundering illicit funds or fraudulent cash-outs.

These measures represent key components of the company's AML compliance efforts; however, new risks may emerge over time. To ensure continued effectiveness, GAMEPLAY INTERNATIONAL B.V. conducts regular risk assessments tailored to evolving threats and provides ongoing training to its employees. This reinforces the company's commitment to a robust Anti-Money Laundering (AML) compliance framework.

Terrorism Financing:

Terrorism financing involves the provision of financial support to terrorist organizations or activities, utilizing both lawful and unlawful financial sources. These funds are essential for carrying out operations, ranging from minor logistical support to large-scale attacks.

Sources of Terrorism Financing

The funding sources for terrorist activities can generally be categorized into two groups:

- Legitimate Sources – Terrorists often exploit legal financial systems, including businesses, charitable donations, and other lawful transactions, to redirect funds covertly. In some instances, charitable organizations and commercial enterprises are misused as intermediaries to conceal and reroute financial resources.
- Illicit Sources – Criminal activities such as fraud, smuggling, drug trafficking, extortion, and money laundering serve as primary means of generating funds while obscuring their origins.

Methods of Fund Transfers

Terrorist networks employ various channels to transfer and distribute funds, including:

- Formal Financial Institutions – Traditional banking systems and financial services are sometimes manipulated using advanced techniques such as layering and structuring. These methods involve breaking large transactions into smaller amounts to avoid raising suspicion and bypass financial monitoring mechanisms.
- Informal Money Transfer Systems – Alternative financial networks, such as the hawala system, operate outside conventional banking regulations, making it difficult for authorities to detect and trace suspicious transactions.

Indicators of Terrorism Financing

Certain financial behaviors and transaction patterns may signal potential terrorist financing, including:

- Unusual financial activities that deviate from an individual's or business's normal behavior.
- Frequent or high-value transactions linked to regions associated with terrorist activity.
- Financial dealings involving individuals or organizations flagged on international sanctions or watchlists.
- Large cash deposits, transactions involving high-risk industries, or activities designed to evade detection by financial institutions.

Regulatory Compliance and Countermeasures

To mitigate the risks associated with terrorism financing, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) has established a robust Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) compliance framework, which includes:

- Customer Due Diligence (CDD) – Conducting thorough identity verification, assessing the source of funds, and evaluating potential risks.
- Transaction Monitoring – Continuously analyzing financial transactions to detect patterns indicative of suspicious activities.
- Reporting Suspicious Activities – Promptly notifying the relevant authorities whenever transactions raise red flags related to terrorism financing.

Furthermore, the company strictly adheres to various international and national regulatory frameworks, including:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Curaçao Gaming Control Board (GCB) regulatory requirements
- Office of Foreign Assets Control (OFAC) sanctions and watchlists
- United Nations Security Council (UNSC) sanctions list
- European Union (EU) anti-terrorism financing regulations
- U.S. List of Foreign Terrorist Organizations

These regulatory measures ensure that GAMEPLAY INTERNATIONAL B.V. does not inadvertently facilitate financial transactions that could support terrorist organizations.

Global Counter-Terrorism Financing Initiatives

To align with international standards, GAMEPLAY INTERNATIONAL B.V. complies with established counter-terrorism financing frameworks, including:

- Financial Action Task Force (FATF) – An international body that sets guidelines for detecting and preventing financial crimes related to terrorism and money laundering.
- Office of Foreign Assets Control (OFAC) – A U.S. government agency responsible for enforcing economic sanctions and maintaining the Specially Designated Nationals (SDN) list, which includes entities linked to terrorism.
- European Union (EU) Regulations – Mandating strict AML/CTF measures across member states to prevent financial exploitation by terrorist groups.
- United Nations (UN) Sanctions – Imposing global restrictions and maintaining watchlists of individuals and organizations associated with terrorism financing.

By implementing stringent compliance policies and adhering to international regulations, GAMEPLAY INTERNATIONAL B.V. reinforces its ability to identify, prevent, and report terrorism financing activities, ensuring a secure and legally compliant operational environment.

Proliferation Financing:

Proliferation financing refers to the financial support, facilitation, or provision of resources for activities related to the development, acquisition, and distribution of weapons of mass destruction (WMDs) and their delivery systems. This form of financial crime poses a significant global security risk and is strictly prohibited under both international regulations and Curaçao's legal framework. As a licensed iGaming operator, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) is committed to identifying, assessing, and mitigating the risks associated with proliferation financing. This commitment is embedded within the company's broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework, ensuring full regulatory adherence and the integrity of its financial transactions.

Compliance with Curaçao iGaming Regulations

The Curaçao Gaming Control Board (GCB) enforces strict regulatory requirements to prevent financial crimes, including proliferation financing. These regulations require all licensed iGaming operators, including GAMEPLAY INTERNATIONAL B.V., to take active measures in identifying, mitigating, and reporting potential threats linked to WMD proliferation. By complying with these regulations, the company aligns itself with global financial security standards, ensuring that its platform is not exploited for illicit financial activities.

Risk Assessment and Proliferation Financing Prevention

To effectively counter the risks associated with proliferation financing, GAMEPLAY INTERNATIONAL B.V. conducts comprehensive risk assessments on an ongoing basis. These assessments focus on identifying customers and financial transactions that may be linked to high-risk jurisdictions known for weak proliferation controls. In particular, the company examines transactions involving goods, services, or entities associated with proliferation networks and evaluates financial patterns that resemble established proliferation financing methods. By continuously refining its risk assessment strategies, the company enhances its ability to detect and prevent any attempts to misuse its platform for illicit financial purposes.

Enhanced Customer Due Diligence (CDD) Measures

As part of its stringent compliance framework, GAMEPLAY INTERNATIONAL B.V. implements enhanced customer due diligence (CDD) procedures, particularly for customers and transactions categorized as high-risk. These procedures include screening all customers against international sanctions lists, including those maintained by the United Nations Security Council (UNSC), the Financial Action Task Force (FATF), and the European Union (EU). Additionally, the company thoroughly investigates any transactions that deviate from typical customer behavior and closely monitors potential affiliations with organizations flagged for involvement in proliferation-related activities. These proactive measures ensure that the company effectively identifies and prevents high-risk transactions from occurring within its platform.

Transaction Monitoring and Suspicious Activity Reporting

To detect financial activities that may be linked to proliferation financing, GAMEPLAY INTERNATIONAL B.V. employs sophisticated transaction monitoring systems designed to analyze patterns of financial behavior. These systems continuously scan financial transactions, flagging any movements that exhibit characteristics of proliferation financing. When suspicious activity is identified, it is immediately reviewed by compliance officers, who conduct further investigations before submitting Suspicious Activity Reports (SARs) to the Curaçao Financial Intelligence Unit (FIU). This ensures that regulatory authorities are promptly informed of any potential proliferation financing risks, enabling swift enforcement actions against any entities attempting to exploit the financial system.

Sanctions Screening and Regulatory Compliance

Strict adherence to Curaçao and international sanctions regulations is a core component of GAMEPLAY INTERNATIONAL B.V.'s compliance program. The company systematically screens all financial transactions and business relationships against regularly updated sanctions lists, including those under the Kingdom Sanction Act and United Nations Security Council Resolutions. Transactions involving individuals, entities, or jurisdictions subject to WMD-related sanctions are automatically flagged and blocked, preventing illicit financial flows from infiltrating the platform. Additionally, the company

maintains detailed records of all sanctions screenings and compliance actions, ensuring full transparency and accountability during regulatory audits.

Training and Awareness for Employees

Recognizing the importance of informed decision-making in preventing proliferation financing, GAMEPLAY INTERNATIONAL B.V. ensures that all employees receive specialized training on financial crime risks, with a particular focus on proliferation financing threats. This training enables employees to recognize key red flags, such as unusual financial transactions or suspicious business affiliations, and equips them with the knowledge required to respond appropriately to potential threats. Additionally, the company's training programs are regularly updated to reflect the latest developments in Curaçao's evolving regulatory landscape, ensuring that compliance personnel remain vigilant against emerging risks.

Collaboration with Regulatory Authorities

In its commitment to upholding financial integrity, GAMEPLAY INTERNATIONAL B.V. actively collaborates with regulatory bodies and enforcement agencies, including the Curaçao Gaming Control Board (GCB), the Financial Intelligence Unit (FIU), and other relevant authorities. This collaboration involves sharing intelligence on potential threats, providing timely reports on suspicious activities, and actively participating in industry-wide initiatives aimed at strengthening the iGaming sector's defenses against proliferation financing risks. By fostering strong regulatory partnerships, the company plays a vital role in preventing its platform from being misused for unlawful financial activities.

Commitment to Global Security and Compliance

As a responsible iGaming operator, GAMEPLAY INTERNATIONAL B.V. remains unwavering in its dedication to preventing proliferation financing activities within its platform. The company's adherence to Curaçao's latest iGaming regulations and international compliance frameworks ensures that it upholds the highest standards of financial security, transparency, and legal compliance. These efforts not only safeguard the integrity of the company's financial operations but also contribute to global initiatives aimed at disrupting financial networks linked to WMD development and distribution. By maintaining rigorous compliance controls, the company strengthens its role as a trusted and responsible participant in the international financial system.

5. Sanctions Compliance

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) is firmly committed to adhering to international sanctions regulations as part of its broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) policies. The company enforces a comprehensive sanctions compliance

framework to prevent any financial dealings with sanctioned individuals, entities, or jurisdictions. Through rigorous due diligence procedures, all clients and financial transactions are meticulously screened to ensure full regulatory compliance and mitigate any risks associated with sanctions violations.

Transaction Monitoring and Regulatory Reporting

A key aspect of the company's AML/CTF/CPF compliance strategy is the continuous monitoring of financial transactions to identify any indications of sanctions breaches. Automated transaction screening systems analyze financial movements in real time, detecting irregularities that may suggest involvement with sanctioned parties. Whenever suspicious activity or potential non-compliance is identified, the company immediately flags the transaction for further review and, if necessary, reports the case to relevant regulatory authorities.

To reinforce its commitment to sanctions compliance, GAMEPLAY INTERNATIONAL B.V. provides ongoing training programs for its employees, ensuring they remain informed about the latest sanctions regulations, enforcement policies, and evolving compliance requirements. This proactive approach ensures that staff members are well-equipped to identify, report, and prevent any potential sanctions violations.

Automated Sanctions Screening and Compliance Actions

To ensure full compliance with national and international sanctions regulations, GAMEPLAY INTERNATIONAL B.V. has implemented real-time sanctions screening mechanisms across all client interactions and financial transactions. These automated compliance systems continuously verify transactions against the latest global sanctions lists, minimizing the risk of regulatory breaches. The company's internal database is regularly updated with newly issued sanctions to maintain a robust and up-to-date compliance framework.

If a sanctions match or suspicious financial activity is detected, the company takes immediate action, including freezing accounts, blocking transactions, and conducting enhanced investigations. Any confirmed violations are promptly reported to the appropriate regulatory authorities, ensuring a zero-tolerance approach to sanctions breaches.

Ongoing Policy Reviews and Regulatory Adherence

To keep pace with evolving regulatory requirements, GAMEPLAY INTERNATIONAL B.V. conducts regular reviews and updates of its sanctions compliance framework. This ensures that the company remains aligned with the latest domestic and international sanctions policies. As part of this commitment, the company actively monitors and enforces compliance with the following sanctions lists:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Curaçao Gaming Control Board (GCB) announcements

- European Union (EU) sanctions regulations
- United Kingdom Office of Financial Sanctions Implementation (UK OFSI) sanctions
- United Nations Security Council (UNSC) Consolidated List
- U.S. List of Foreign Terrorist Organizations
- Office of Foreign Assets Control (OFAC) sanctions framework

By proactively monitoring these global sanctions directives, GAMEPLAY INTERNATIONAL B.V. ensures that its platform remains compliant, secure, and protected from unlawful financial activities.

Preventing Sanctions Evasion and Strengthening Compliance Measures

Beyond direct sanctions compliance, GAMEPLAY INTERNATIONAL B.V. is dedicated to detecting and preventing any attempts to circumvent sanctions regulations. The company's enhanced due diligence procedures focus on identifying concealed or indirect transactions designed to bypass restrictions. Any identified evasion tactics are immediately reported to the appropriate authorities, triggering further investigative measures.

To address such risks, GAMEPLAY INTERNATIONAL B.V. takes decisive corrective actions, which may include transaction suspensions, comprehensive account reviews, and heightened monitoring protocols. Additionally, the company enforces regular compliance audits to ensure adherence to the highest regulatory standards.

By maintaining a proactive approach to sanctions enforcement, GAMEPLAY INTERNATIONAL B.V. ensures full compliance with international financial regulations, reinforcing its commitment to transparency, security, and responsible gaming operations. Through continuous policy enhancements and staff training initiatives, the company safeguards its platform from sanctions violations, financial crime, and regulatory non-compliance.

6. Risk-Based Approach

Risk Assessment and Mitigation Strategies

A fundamental aspect of GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409)'s compliance framework is its comprehensive risk assessment process, which operates under a risk-based approach (RBA). This methodology involves an in-depth evaluation of risks associated with customers, products, services, and geographic locations, ensuring that the company maintains a proactive stance in identifying and mitigating potential vulnerabilities. By conducting regular assessments, the company strengthens its ability to detect, analyze, and respond to emerging threats, thereby ensuring compliance with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations.

Implementation of Risk Mitigation Measures

Once risks are identified, GAMEPLAY INTERNATIONAL B.V. employs targeted risk mitigation strategies, adjusting its approach based on the level of risk exposure. The company applies tailored compliance measures to safeguard its platform against financial crimes, including money laundering, terrorist financing, and proliferation financing.

One of the key risk mitigation strategies is Enhanced Due Diligence (EDD), which involves conducting thorough investigations on high-risk customers and transactions. This process includes obtaining additional details on the source of funds, verifying beneficial ownership structures, and assessing financial backgrounds. By implementing rigorous due diligence, the company enhances its ability to detect and prevent illicit financial activities.

To further strengthen its compliance framework, GAMEPLAY INTERNATIONAL B.V. employs sophisticated transaction monitoring systems designed to identify suspicious financial activities in real time. These systems utilize automated alerts that flag unusual transaction patterns, helping detect behaviors consistent with money laundering, fraud, or terrorist financing. By setting specific alert thresholds, the company ensures that any irregular financial activities are promptly reviewed and investigated.

Additionally, strict customer verification procedures are enforced, particularly for high-risk individuals and entities. Robust identity verification measures involve authentication through trusted data sources and continuous monitoring of flagged individuals to detect emerging risks. This ensures that high-risk customers undergo comprehensive scrutiny before engaging in financial transactions on the platform.

Continuous Monitoring and Policy Updates

To ensure ongoing compliance with regulatory requirements, GAMEPLAY INTERNATIONAL B.V. conducts regular reviews of transaction data and risk profiles. This continuous monitoring process enables the company to detect emerging suspicious activities, update customer risk classifications, and refine AML/CTF/CPF policies in response to evolving threats and regulatory changes. The company remains committed to maintaining a dynamic compliance program that adapts to new risks as they arise.

Accurate Reporting and Record-Keeping

A key element of the company's risk-based compliance program is precise reporting and record management. GAMEPLAY INTERNATIONAL B.V. ensures that suspicious transactions are promptly reported to the appropriate authorities, in accordance with regulatory guidelines. Additionally, detailed records of customer identification, financial transactions, and risk assessments are securely maintained for the legally mandated period. These records are readily available for regulatory audits and inspections, demonstrating the company's commitment to transparency and legal compliance.

Commitment to a Secure and Compliant Operational Environment

By implementing these proactive risk mitigation strategies, GAMEPLAY INTERNATIONAL B.V. reinforces its dedication to maintaining a secure, transparent, and fully compliant operational environment. Through ongoing monitoring, policy enhancements, and adherence to international AML/CTF/CPF standards, the company upholds the integrity of its platform while safeguarding against financial crimes. This commitment ensures compliance with evolving regulatory requirements and strengthens the company's role as a responsible and trustworthy iGaming operator.

6.1. Risk Factors

Customer Risk and Risk-Based Assessments

Customer risk refers to the potential exposure to money laundering (ML) and terrorism financing (TF) risks arising from engaging with specific individuals. As part of its risk-based compliance approach, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) evaluates customer profiles, financial activities, and sources of wealth to determine potential vulnerabilities.

Certain categories of customers pose a higher risk of financial crime exposure, including those with multiple sources of income, making it more complex to verify the legitimacy of funds. Individuals with irregular or fluctuating income streams may also present increased risks, as their financial patterns can be unpredictable and difficult to assess. Politically Exposed Persons (PEPs) are subject to heightened scrutiny due to their influence over public funds and potential involvement in corruption-related offenses.

Other high-risk customer types include high-spending individuals, whose expenditures may be inconsistent with their declared income, as well as disproportionate spenders, who appear to spend significantly beyond their financial means. Additionally, customers utilizing multiple gaming accounts present a compliance challenge, as they can attempt to obscure gambling activities and avoid detection by financial monitoring systems.

To mitigate risks, GAMEPLAY INTERNATIONAL B.V. has implemented transaction thresholds that align with typical financial behaviors observed among its customer base. Low-risk customers typically have a single, verifiable source of income, whereas higher-risk customers, including those with multiple income sources or irregular transaction patterns, are subject to enhanced monitoring and due diligence measures.

Product, Service, and Transaction Risks

Certain gaming products, services, and transaction methods are more susceptible to exploitation for money laundering and terrorism financing. Criminal networks often target vulnerable financial mechanisms within the gaming industry, particularly those that enable

individuals to manipulate game outcomes or engage in financial transactions that obscure the origin of illicit funds.

Funds from criminal activities, such as credit/debit card fraud, drug trafficking, or theft, may be funneled into gambling platforms to launder illicit proceeds. Anonymous payment methods, including prepaid cards and virtual assets (such as cryptocurrencies or digital tokens), pose a significant risk due to their lack of traceability.

Misuse of player accounts is another concern, as some customers may use their gaming accounts as temporary holding spaces for deposits and withdrawals without engaging in actual gambling activities. Peer-to-peer gaming, where players can transfer funds among themselves, also increases the potential for illicit financial transactions.

Additionally, criminals may attempt to exploit third-party financial instruments, such as bank accounts or payment cards registered under another person's name. The transfer of funds between different gaming accounts further complicates transaction tracking, increasing the risk of financial crime.

The use of financial services tied to gaming, such as credit issuance, currency exchanges, and multi-operator gaming networks, poses another set of risks. Players may open multiple gaming accounts under different identities or transfer funds across platforms to evade detection.

To address these risks, GAMEPLAY INTERNATIONAL B.V. maintains strict monitoring of gaming transactions, applies enhanced due diligence (EDD) procedures, and ensures compliance with global AML/CTF/CPF standards.

Geographical Risk

Geographical risk arises from the location of players and the origin of their financial resources, which can indicate potential exposure to money laundering, terrorism financing, or proliferation financing risks. Certain jurisdictions pose a higher risk due to weak AML/CFT frameworks, high corruption levels, or international sanctions. Countries associated with terrorist organizations or the proliferation of weapons of mass destruction (WMDs) are subject to stricter monitoring and enforcement measures.

To assess geographical risk exposure, GAMEPLAY INTERNATIONAL B.V. relies on trusted regulatory sources and independent global organizations, including:

- Financial Action Task Force (FATF) reports, which identify high-risk jurisdictions subject to enhanced monitoring.
- Caribbean Financial Action Task Force (CFATF) statements, highlighting financial crime concerns in the region.
- U.S. Department of State International Narcotics Control Strategy Reports (INCSR), which assess jurisdictions linked to financial crime and money laundering.
- The European Commission's list of high-risk third countries, identifying jurisdictions with strategic AML/CFT deficiencies.

- Office of Foreign Assets Control (OFAC) sanctions lists, which impose financial restrictions on countries associated with terrorism or illicit financing activities.
- Reports from reputable global organizations, such as Transparency International's Corruption Perceptions Index (CPI), ranking countries based on corruption risks.

To effectively manage geographical risk, GAMEPLAY INTERNATIONAL B.V. employs a structured risk classification system, categorizing countries into high-risk and low-risk groups. This enables the company to apply enhanced due diligence (EDD) measures for customers from high-risk jurisdictions, restrict transactions involving sanctioned countries, and regularly update monitoring systems to reflect evolving risk assessments. By adopting a data-driven approach, the company ensures compliance with AML/CTF/CPF regulations, thereby reducing financial crime exposure while maintaining a secure and transparent gaming environment.

Distribution Channel Risks and Mitigation Measures

The channels through which GAMEPLAY INTERNATIONAL B.V. interacts with its customers also present potential risks related to money laundering, terrorist financing, and fraud. Anonymity-driven distribution channels, particularly those that facilitate anonymous transactions or interactions, increase the likelihood of financial crime unless properly regulated.

To mitigate these risks, the company has implemented enhanced verification controls for anonymous transactions, ensuring that all financial interactions are properly authenticated. The use of technological solutions, such as biometric authentication and advanced identity verification tools, further reduces the likelihood of fraud and non-face-to-face transaction manipulation.

By enforcing rigorous monitoring protocols and implementing secure authentication mechanisms, GAMEPLAY INTERNATIONAL B.V. strengthens its compliance with international regulations, ensuring that its gaming operations remain transparent, secure, and free from financial crime.

6.2. Technological Developments Risk Assessment

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) is committed to preventing the exploitation of technological advancements for financial crimes, including money laundering (ML) and terrorist financing (TF). As emerging technologies continuously reshape the iGaming landscape, the company maintains rigorous controls and proactive risk management strategies to mitigate any associated vulnerabilities. By integrating comprehensive risk assessment procedures, GAMEPLAY INTERNATIONAL B.V. ensures that new business practices, products, services, and delivery mechanisms do not compromise its regulatory compliance obligations.

Risk Identification and Assessment Procedures

To safeguard against the misuse of technological innovations, the company conducts thorough risk assessments whenever:

- A new product or service is introduced into the platform.
- A new business practice is implemented to enhance operational efficiency or customer engagement.
- A new service delivery method becomes available, such as innovative payment solutions or digital account management tools.
- A new or evolving technology is integrated into existing or future gaming products, including blockchain-based transactions, artificial intelligence (AI)-driven services, or advanced cybersecurity measures.

Before deploying any technological innovation, the company performs a comprehensive evaluation to determine whether it introduces potential security vulnerabilities that could be exploited for financial crimes. This assessment process involves identifying, analyzing, and documenting risks, ensuring compliance with both local and international AML/CTF regulatory requirements. By maintaining detailed records of all risk evaluations, GAMEPLAY INTERNATIONAL B.V. strengthens its ability to detect, respond to, and mitigate technology-related financial crime threats.

Implementation of Risk Mitigation Measures

When risks are identified, GAMEPLAY INTERNATIONAL B.V. takes immediate, proactive steps to address potential threats and strengthen its financial crime prevention framework. These mitigation measures include:

- Enhancing security controls to prevent the misuse of new technologies for fraudulent activities. This may involve multi-factor authentication (MFA), biometric verification, data encryption, and AI-driven fraud detection systems.
- Strengthening transaction monitoring systems to identify anomalies in financial activities. By employing automated compliance tools, the company can detect irregular transaction patterns and flag potential money laundering or terrorist financing attempts.
- Updating AML/CTF compliance policies to align with emerging technological risks. As digital financial services evolve, the company ensures that its policies remain dynamic and adaptable to counter new cybercrime tactics and financial crime methodologies.

By continuously evaluating and adapting to rapid technological advancements, GAMEPLAY INTERNATIONAL B.V. upholds its commitment to a secure, compliant, and resilient gaming environment. This proactive approach not only safeguards the integrity of the company's financial operations but also reinforces its compliance with international AML/CTF standards, ensuring that innovative technologies do not compromise security or regulatory obligations.

7. Client Due Diligence

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) is fully committed to complying with regulatory requirements that prohibit anonymous and fraudulent accounts. As part of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework, the company enforces robust identity verification procedures to establish legitimate business relationships with its players.

By implementing rigorous CDD protocols, the company enhances its ability to detect and prevent financial crimes, including money laundering, terrorist financing, and proliferation financing. A comprehensive due diligence program enables GAMEPLAY INTERNATIONAL B.V. to assess potential risks effectively, ensuring full compliance with regulatory obligations while maintaining a secure and transparent gaming environment.

All suspicious activities identified during the CDD process are promptly reported to the Financial Intelligence Unit (FIU). If necessary, cases are further escalated to the Public Prosecutor's Office to facilitate legal action against financial crime offenders. Through these proactive compliance measures, GAMEPLAY INTERNATIONAL B.V. reinforces its commitment to responsible gaming, financial security, and regulatory adherence.

7.1. Detailed Customer Due Diligence Measures

Player Identification and Verification

As part of its Customer Due Diligence (CDD) framework, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) enforces rigorous identity verification protocols to ensure a secure and compliant gaming environment. The company applies the following measures:

- Verification of player identities through official, independent, and reliable sources, such as government-issued documents or regulatory databases.
- Determination of the Ultimate Beneficial Owner (UBO) for legal entities to understand ownership structures and control mechanisms.
- Assessment of the business relationship's purpose and intent, ensuring transparency in player interactions.
- Ongoing due diligence and transaction monitoring, verifying that financial activities align with expected customer behavior and assigned risk profiles. When necessary, additional verification of the source of funds is conducted to confirm legitimacy.

Confidentiality and Compliance in Reporting

To prevent tipping off customers, GAMEPLAY INTERNATIONAL B.V. strictly prohibits its employees from disclosing when a Suspicious Activity Report (SAR) has been submitted to the Financial Intelligence Unit (FIU). If performing CDD procedures could alert the customer to an ongoing investigation, the company may opt to bypass the standard verification process and immediately report the suspicious activity to the relevant authorities.

7.2. Player Identification & Verification

Required Identification Information

To verify a player's identity, GAMEPLAY INTERNATIONAL B.V. collects the following details:

- Full legal name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Official identification number (e.g., passport, national ID, or driver's license)

For low-risk customers, basic identification details are sufficient. However, for high-risk individuals, additional verification measures are applied to mitigate the risk of money laundering and terrorist financing.

Risk Assessment and Verification Process

Upon registration, each player undergoes an initial risk assessment based on the information provided. This risk profile is continuously updated as more data becomes available. The identity verification process includes:

- Review of government-issued photo identification (passport, national ID, or driver's license).
- Supporting documents for address verification, such as a recent utility bill or bank statement (issued within the last six months).
- Address confirmation through official correspondence, including letters, emails, or phone verification.
- Advanced security checks, including biometric verification, database cross-referencing, IP tracking, and validation of financial sources.

In cases where the collected data is insufficient, GAMEPLAY INTERNATIONAL B.V. may require additional verification steps, such as:

- A live selfie with the ID document to confirm authenticity.
- Verification of the first deposit through a regulated financial institution.

Through these robust CDD measures, GAMEPLAY INTERNATIONAL B.V. strengthens its ability to detect and prevent financial crime while maintaining strict AML/CTF/CPF compliance.

7.3. Understanding the Relationship

As part of its Customer Due Diligence (CDD) procedures, GAMEPLAY INTERNATIONAL B.V. seeks to fully understand the purpose and nature of its business relationships with players. While the primary objective of the relationship—gambling activities—is typically clear, the company gathers sufficient data to identify unusual or suspicious financial behavior.

For higher-risk clients, the company implements Enhanced Due Diligence (EDD) procedures, which include:

- Detailed documentation on the source of wealth, verifying the legitimacy of funds.
- Assessment of expected gaming and financial activity, ensuring alignment with the player's financial profile.
- Cross-referencing with independent databases to validate the accuracy of provided information.

For low- and medium-risk players, a simplified verification process is applied, requiring:

- A basic declaration outlining their employment or business details.
- Additional verification measures only if suspicious patterns are detected.

By categorizing customers based on risk levels, GAMEPLAY INTERNATIONAL B.V. ensures that due diligence efforts remain proportionate, preventing financial crime while upholding regulatory standards.

7.4. Ongoing Monitoring & Compliance

As part of its AML/CTF/CPF compliance program, GAMEPLAY INTERNATIONAL B.V. continuously monitors player identities and transactions to detect and prevent money laundering, terrorist financing, and proliferation financing.

Key Monitoring Measures

- Regular updates and verification of player information, particularly for high-risk individuals.

- Transaction monitoring to detect irregular financial patterns or suspicious activities.
- Enhanced Due Diligence (EDD) for transactions meeting or exceeding NAF 4,000, including linked transactions that cumulatively surpass this threshold.
- Real-time risk detection using advanced monitoring systems, which analyze financial transactions for potential red flags. If suspicious activity is identified, an immediate investigation is conducted, and if necessary, the Financial Intelligence Unit (FIU) is promptly notified.

By integrating automated risk detection with manual oversight, GAMEPLAY INTERNATIONAL B.V. enhances its ability to identify, prevent, and report financial crimes. This proactive compliance strategy reinforces the company's commitment to regulatory adherence, financial security, and operational transparency.

7.5. Simplified & Enhanced Due Diligence

Simplified Due Diligence (SDD)

When the risk of money laundering (ML) or terrorist financing (TF) is assessed to be low, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) may apply Simplified Customer Due Diligence (SDD) measures. These streamlined procedures reflect the reduced risk level while ensuring full compliance with AML/CTF/CPF regulations.

Examples of Simplified Due Diligence Measures

- Limited Data Collection – If the risk assessment confirms low ML/TF risk, only basic identity information may be collected, including:
 - Full legal name
 - Date of birth
 - Permanent residential address
- Delayed Verification – In lower-risk cases, verification of identity and beneficial ownership may occur after the business relationship has been established.
- Risk-Based Verification – The level of verification may be adjusted depending on the risk level:
 - In low-risk cases, reliance on alternative reputable data sources may be permitted, even those without photographic identification.
 - Minimal identity verification may be applied if there is sufficient assurance that the customer's identity is legitimate.
- Reduced Frequency of Information Updates – Players categorized as low risk may be subject to less frequent identity verification updates.
- Lower-Intensity Transaction Monitoring – Transactions involving low-risk customers may be monitored less frequently, provided they remain within reasonable monetary thresholds.

Limitations of SDD

SDD cannot be applied in cases where:

- There is a suspicion of ML/TF activity.
- The customer falls into a higher-risk category, in which case Standard Due Diligence (CDD) or Enhanced Due Diligence (EDD) is required.

By applying SDD only in appropriate cases, GAMEPLAY INTERNATIONAL B.V. maintains a risk-sensitive approach while ensuring regulatory compliance and financial security.

Enhanced Due Diligence (EDD)

As part of its risk-based compliance framework, GAMEPLAY INTERNATIONAL B.V. applies Enhanced Due Diligence (EDD) to higher-risk customers. This process includes stricter verification and monitoring to identify, prevent, and assess financial crime risks. The company intensifies monitoring of business relationships to detect unusual activity or suspicious transactions.

When EDD is Required

EDD is mandatory in situations where the risk of ML or TF is higher, including:

- Residents of high-risk jurisdictions – Customers from countries with weak AML/CFT regulations, high corruption levels, or international sanctions require additional scrutiny.
- Politically Exposed Persons (PEPs) – Due to their influence and access to public funds, PEPs pose an increased financial crime risk, necessitating enhanced identity verification and transaction monitoring.
- Use of anonymous financial products – Transactions involving prepaid cards, virtual assets (cryptocurrencies), or other anonymity-enhancing methods require stricter oversight.
- New financial technologies – Any new business practices or financial technologies, such as cryptocurrency transactions or blockchain-based gaming services, must be assessed for potential financial crime risks before implementation.

EDD Measures Implemented by GAMEPLAY INTERNATIONAL B.V.

To ensure compliance with AML/CTF/CPF regulations, EDD measures are proportionate to the risk identified and include:

- Collection of additional customer information, including employment details, previous addresses, and publicly available data.
- Detailed assessment of the business relationship, requiring additional documentation to understand the customer's intent.
- Verification of the source of funds and wealth, ensuring legitimate financial origins (e.g., personal savings, employment income, property sales, inheritances).

- In-depth review of large or unusual transactions, ensuring consistency with expected financial behavior.
- Senior management approval before initiating or continuing a relationship with a high-risk customer.
- Real-time transaction monitoring, with automated alerts on high-risk transactions.
- Ensuring the first deposit originates from a regulated financial institution, registered in the customer's name.
- Ongoing source of funds verification, requiring periodic updates for high-risk customers.

By enforcing these strict measures, GAMEPLAY INTERNATIONAL B.V. strengthens its financial security framework, ensuring full compliance with international AML/CTF/CPF standards while mitigating financial crime risks.

7.6. Timing of Customer Due Diligence Measures

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) applies Customer Due Diligence (CDD) measures promptly and effectively, ensuring full compliance with AML/CTF/CPF regulations.

CDD Implementation Based on Transaction Thresholds

At the time of account registration, the company collects and verifies the minimum required personal details of each player, including:

- Full name
- Permanent residential address
- Date of birth
- Politically Exposed Person (PEP) screening
- Sanctions screening

As part of its risk-based approach, the company verifies customer identities before processing financial transactions equal to or exceeding NAF 4,000. This verification process applies to:

- Single transactions that reach or exceed NAF 4,000.
- Multiple linked transactions (deposits, withdrawals, and peer-to-peer transfers) that cumulatively reach NAF 4,000.

To maintain a proactive compliance approach, GAMEPLAY INTERNATIONAL B.V. continuously monitors all player transactions and calculates the threshold daily, ensuring that all transactions since the business relationship was established are considered.

Upon reaching the NAF 4,000 threshold, the company conducts a comprehensive customer risk assessment, reviewing all relevant data and completing any outstanding CDD obligations.

Proactive Customer Due Diligence Implementation

GAMEPLAY INTERNATIONAL B.V. prioritizes early completion of CDD verification, conducting full identity checks at the time of account registration rather than waiting until a financial threshold is met. This reduces the risk of illicit funds entering the gaming system before thorough due diligence has been completed.

Transaction Restrictions While CDD is Pending

If a player reaches the NAF 4,000 threshold before completing full CDD verification, the company applies restrictions to maintain compliance:

- If the threshold is reached due to a deposit, the player cannot deposit or withdraw additional funds but may continue playing with existing account funds.
- If the threshold is reached due to a withdrawal request, the company freezes the account, preventing further gaming activity until verification is complete.

Handling Non-Compliance with CDD Requirements

If a player fails to provide the required CDD documentation within 30 days of reaching the NAF 4,000 threshold, GAMEPLAY INTERNATIONAL B.V. takes the following actions:

- Terminates the business relationship with the player.
- Reports the transaction to the Financial Intelligence Unit (FIU) if there is a presumption of money laundering (ML) or terrorist financing (TF).
- If no suspicion of ML/TF exists, the company returns the funds to the original deposit source (same bank account or digital wallet).
- If ML/TF suspicion is present, the company follows internal procedures to determine whether the funds should be blocked, ensuring full compliance with AML/CTF regulations.

Managing Tipping-Off Risks

Recognizing that blocking an account may raise suspicion, the company carefully evaluates each situation to ensure that necessary compliance actions are taken without violating AML/CTF regulations. Internal procedures guide how cases are handled to prevent inadvertent tipping-off while ensuring regulatory compliance.

By implementing these timely CDD measures, GAMEPLAY INTERNATIONAL B.V. maintains regulatory compliance, reduces financial crime risks, and ensures the security and transparency of its operations across both online and land-based gaming environments.

7.7 Customer Due Diligence for Existing Clients

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) applies Customer Due Diligence (CDD) measures not only to new customers but also to existing ones, ensuring continued compliance through ongoing monitoring and risk assessment. The company maintains a risk-based approach, regularly reviewing its CDD procedures to ensure they align with regulatory obligations and effectively mitigate financial crime risks.

Review of Existing Customer CDD Compliance

- Ongoing Due Diligence – The company continuously applies CDD measures to existing customers, with a particular focus on transaction monitoring and risk reassessment.
- Risk-Sensitive Approach – For existing customers where prior CDD procedures were inadequate or incomplete, the company:
- Conducts retrospective CDD, prioritizing higher-risk customers.
- Performs periodic CDD updates to align with AML/CTF/CPF regulations.

When CDD is Reapplied to Existing Customers

GAMEPLAY INTERNATIONAL B.V. reassesses existing customers when:

- A customer's risk profile changes significantly (e.g., sudden large transactions, change in jurisdiction, PEP status).
- Regulatory updates or legal requirements mandate a reassessment of customer data.
- An existing customer engages in transactions equal to or exceeding the NAF 4,000 threshold, triggering full CDD verification.

Compliance for Previously Unverified Customers

If a customer was previously onboarded without formal CDD procedures, the company:

- Implements full CDD measures, prioritizing high-risk customers.
- Conducts customer verification at appropriate intervals, using a risk-sensitive approach.

By ensuring that existing customer relationships comply with AML/CTF/CPF regulations, GAMEPLAY INTERNATIONAL B.V. reinforces its commitment to financial security and prevents money laundering and terrorist financing risks.

7.8 Termination of Business Relationships

If a player fails to comply with CDD requirements or engages in suspicious activities, GAMEPLAY INTERNATIONAL B.V. takes necessary steps to terminate the business relationship, ensuring compliance with AML/CTF/CPF regulations.

Conditions for Termination

A player's account is terminated if they:

- Engage in suspicious financial activities.
- Fail to provide adequate CDD documentation within the required timeframe.
- Are identified as posing a high risk for money laundering (ML) or terrorist financing (TF).

Process for Termination

- Senior management reviews and approves the termination decision.
- Upon termination, the company conducts a final review of the player's account activities.
- If any suspicious transactions are detected, the company submits a report to the Financial Intelligence Unit (FIU).
- All records related to the terminated account are securely stored for a minimum of five years, in compliance with regulatory requirements.

By enforcing strict termination policies, GAMEPLAY INTERNATIONAL B.V. maintains a secure and transparent gaming environment while mitigating financial crime risks.

7.9. Third-Party Reliance for Customer Due Diligence

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) may engage third parties to perform specific aspects of Customer Due Diligence (CDD); however, this reliance is subject to strict regulatory oversight to ensure full compliance with AML/CTF/CPF requirements. Despite delegating certain CDD functions, the company retains ultimate responsibility for ensuring that all CDD measures are properly implemented and adhered to. To maintain compliance, the company ensures immediate access to all customer identification details provided by the third party upon request. Additionally, formal agreements with these third-party providers are established, outlining clear obligations for data provision, adherence to AML regulations, and periodic compliance testing.

Even when CDD procedures are outsourced, GAMEPLAY INTERNATIONAL B.V. remains directly responsible for conducting independent risk assessments, determining Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring

to detect any suspicious activities. Third-party providers engaged in CDD processes must be regulated entities subject to AML/CTF laws and regulatory supervision. Furthermore, the third party must maintain an independent business relationship with the customer, separate from its relationship with GAMEPLAY INTERNATIONAL B.V. To mitigate jurisdictional risks, the company conducts a comprehensive risk assessment of the third party's country of operation, ensuring compliance with international risk intelligence reports.

There is a distinction between third-party reliance and outsourcing. In third-party reliance, the external provider conducts specific CDD elements independently, but GAMEPLAY INTERNATIONAL B.V. remains fully accountable for compliance. In outsourcing scenarios, the third party applies CDD procedures strictly under the company's internal policies and regulatory framework, with full oversight remaining with GAMEPLAY INTERNATIONAL B.V. Regular quantitative and qualitative assessments are conducted to evaluate the effectiveness of the service provider, ensuring that customer risk assessments and business relationship decisions remain solely within the company's control.

By enforcing strict oversight and regulatory compliance in third-party CDD processes, GAMEPLAY INTERNATIONAL B.V. effectively mitigates risks while ensuring a secure, transparent, and legally compliant gaming operation.

8. Suspicious Activity Reporting

GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) is committed to the detection and reporting of unusual financial activities that may indicate potential money laundering (ML) or terrorist financing (TF). Suspicious activity typically involves deviations from a customer's normal transaction behavior, including frequent high-value transactions, structured deposits and withdrawals, or dealings with high-risk jurisdictions. To maintain a proactive compliance approach, all employees undergo AML/CTF training and are required to immediately report any suspicious transactions or behavior patterns to the designated Compliance Officer.

Role of the Compliance Officer

The Compliance Officer plays a critical role in investigating flagged transactions and behaviors to determine whether they pose AML/CTF risks. Their responsibilities include conducting detailed reviews of unusual financial activities, ensuring they align with recognized risk indicators, and assessing whether a transaction lacks economic or legal justification. If an activity is deemed suspicious, the Compliance Officer files a Suspicious Activity Report (SAR) with the Financial Intelligence Unit (FIU), as required under Curaçao's AML/CTF regulatory framework.

Definition and Examples of Unusual Activity

A suspicious transaction is any financial activity that significantly deviates from a customer's usual behavior or does not align with legitimate business practices. Examples include unexpectedly large transactions that are inconsistent with a player's typical spending or deposit patterns, frequent high-value transactions, or multiple small transactions structured to evade reporting thresholds. Additionally, dealings with unknown entities or financial activities linked to high-risk jurisdictions with weak AML/CTF controls may indicate potential financial crime. Other red flags include unjustified transactions, such as large deposits followed by immediate withdrawals, suggesting an attempt to disguise illicit funds.

To enhance detection capabilities, GAMEPLAY INTERNATIONAL B.V. employs sophisticated transaction monitoring systems that analyze financial behavior in real-time. Transactions flagged for suspicious activity are immediately escalated to the Compliance Officer for further review.

Confidentiality in Reporting Suspicious Activity

The company enforces strict confidentiality regarding Suspicious Activity Reports (SARs) to protect the integrity of ongoing investigations. Employees and authorized personnel are strictly prohibited from disclosing any information related to SARs to the affected client, their associates, or unauthorized personnel inside or outside the company.

Maintaining confidentiality is crucial to:

- Prevent tipping-off – Disclosing an investigation could enable suspects to alter their behavior, destroy evidence, or evade detection, undermining enforcement efforts.
- Ensure effective regulatory action – Authorities must be able to conduct thorough investigations without interference, allowing for the proper enforcement of AML/CTF regulations.

All SAR-related communications are handled exclusively by the Compliance Officer and designated authorized personnel, ensuring a secure and compliant reporting process.

Consequences of Breaching Confidentiality

Any breach of SAR-related confidentiality is regarded as a serious violation of the company's AML/CTF policies. Consequences for such breaches include internal disciplinary action, which may result in termination of employment, as well as legal penalties under Curaçao's AML/CTF laws for both the individual responsible and the company.

By enforcing strict confidentiality measures and adhering to regulatory reporting protocols, GAMEPLAY INTERNATIONAL B.V. ensures that its AML/CTF compliance framework remains effective, secure, and legally compliant. Through these measures,

the company reinforces its commitment to financial security and the global fight against money laundering and terrorist financing.

9. Compliance Officer

The Compliance Officer plays a critical role in protecting GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) from risks related to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). As the central figure in the company's AML/CTF compliance framework, the Compliance Officer is responsible for developing, implementing, and overseeing all aspects of the anti-financial crime program, ensuring full compliance with Curaçao's regulatory requirements and international AML/CTF laws.

A core responsibility of the Compliance Officer is the design and oversight of the company's AML compliance program. This includes creating and enforcing AML policies, ensuring that all procedures are aligned with local and global financial crime regulations, and conducting regular reviews to assess the effectiveness of compliance controls. The officer continuously updates policies to reflect regulatory changes and advises senior management on necessary improvements.

To strengthen AML/CTF awareness, the Compliance Officer organizes training programs for employees, ensuring they remain knowledgeable about financial crime risks and compliance requirements. Staff members receive regular updates on new regulations, industry best practices, and key risk indicators associated with money laundering and terrorist financing.

The Compliance Officer also plays a key role in transaction monitoring and reporting. This involves analyzing transactions to identify suspicious activities, assessing financial movements against the Ministerial Decree on Unusual Transactions, and ensuring internal reports of suspicious activity are complete and accurate. Any flagged activities undergo further investigation, and when necessary, the Compliance Officer submits Suspicious Activity Reports (SARs) to the Financial Intelligence Unit (FIU). Additionally, they determine when blocking or freezing of accounts is required, ensuring compliance with anti-tipping-off regulations to prevent suspects from altering their financial behavior.

To ensure continuous compliance, the Compliance Officer is responsible for enhancing the AML/CTF framework, making necessary adjustments based on regulatory developments and evolving financial crime risks. By staying informed about global AML/CTF trends, they recommend improvements to the company's financial crime prevention measures and provide periodic compliance reports to management, detailing risk assessments and progress updates.

By proactively monitoring transactions, training staff, and refining compliance policies, the Compliance Officer ensures that GAMEPLAY INTERNATIONAL B.V. maintains a strong defense against financial crime. Their work is essential in protecting the company

from regulatory breaches, safeguarding its integrity, and ensuring full compliance with Curaçao's AML/CTF regulations within the iGaming sector.

10. Independent Audit

To ensure full compliance with Curaçao's new gaming regulations, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) undergoes an independent audit focused on Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF). This comprehensive assessment evaluates the company's financial crime prevention framework, identifies areas for enhancement, and ensures alignment with evolving legal and regulatory requirements. The Curaçao Gaming Control Board oversees the audit process, ensuring that all licensed operators maintain robust compliance measures.

The primary objective of the annual AML/CTF/CPF audit is to evaluate the effectiveness of the company's compliance measures while confirming adherence to regulatory obligations. Through regular audits, GAMEPLAY INTERNATIONAL B.V. proactively identifies and mitigates financial crime risks, integrates industry best practices, and strengthens its internal risk management systems. The audit encompasses a wide range of compliance areas, including risk assessments, transaction monitoring, staff training, and reporting procedures, ensuring the company maintains full compliance with AML/CTF/CPF standards.

Engagement of an Independent Auditor

To maintain objectivity and transparency, GAMEPLAY INTERNATIONAL B.V. engages an independent external auditor or, in specific cases, an internal audit team with specialized expertise in AML/CTF/CPF regulations. This auditor operates separately from the AML Compliance team to eliminate potential conflicts of interest. The company carefully evaluates the auditor's qualifications, industry experience, and credibility, ensuring they meet the approval standards set by the Curaçao Gaming Control Board. The Gaming Control Board formally approves the selected auditor, reinforcing the regulatory expectations for compliance.

Scope of the AML/CTF/CPF Audit

The audit adheres to international compliance standards and follows specific AML/CTF/CPF guidelines established by the Curaçao Gaming Control Board. The review process includes an in-depth examination of the company's financial crime prevention framework, covering key compliance areas such as:

- **Evaluation of AML/CTF/CPF Policies and Procedures** – The auditor assesses whether the company's AML policies are current, effective, and compliant with the latest regulatory updates. The review also ensures that internal controls efficiently mitigate financial crime risks.

- Risk Management Assessment – The company's risk assessment methodology is evaluated to determine whether it effectively identifies and addresses high-risk transactions, customers, and jurisdictions.
- Transaction Monitoring and Reporting Review – The audit verifies whether the company's transaction monitoring systems effectively detect, flag, and report suspicious activities. Additionally, the auditor evaluates the company's compliance with Suspicious Activity Report (SAR) filing obligations with the Financial Intelligence Unit (FIU).
- Staff Training Evaluation – The company's AML/CTF training program is reviewed to ensure that employees receive adequate instruction on financial crime compliance, risk detection, and reporting obligations.
- Customer File Review and Due Diligence Compliance – A randomized review of customer files is conducted to verify adherence to Know Your Customer (KYC), Know Your Business (KYB), and Customer Due Diligence (CDD) requirements. This ensures that the customer onboarding process aligns with regulatory identity verification and risk assessment standards.
- Reporting Mechanism Audit – The procedures for submitting SARs and other compliance reports are analyzed to confirm that they meet the legal standards set by Curaçao's FIU and Gaming Control Board.

Audit Findings and Corrective Actions

Following the completion of the audit, the independent auditor prepares a detailed report outlining their findings, recommendations, and any identified compliance issues. This report is then submitted to senior management and the Curaçao Gaming Control Board. If any deficiencies or weaknesses are identified, GAMEPLAY INTERNATIONAL B.V. implements corrective actions within a designated timeframe to rectify compliance gaps. In certain cases, follow-up audits may be conducted to confirm that the necessary improvements have been effectively applied.

Regulatory Oversight by the Curaçao Gaming Control Board

As the regulatory authority overseeing AML/CTF/CPF compliance, the Curaçao Gaming Control Board conducts its own independent examinations to verify that all licensed operators comply with AML regulations. The Board has the authority to request additional documentation, conduct inspections, and evaluate the company's implementation of audit recommendations.

The Gaming Control Board's regulatory examination includes:

- Audit Report Review – A detailed analysis of the auditor's findings to assess compliance levels and address any unresolved concerns.
- Interviews and Documentation Analysis – Compliance Officers, senior management, and key personnel may be interviewed to verify the company's AML implementation efforts and ensure strict adherence to legal obligations.

Potential Consequences of Non-Compliance

If GAMEPLAY INTERNATIONAL B.V. is found to be non-compliant based on audit findings or regulatory examinations, the company may face significant penalties, including:

- Fines imposed by the Curaçao Gaming Control Board.
- Operational restrictions, limiting gaming activities until full compliance is restored.
- Suspension or revocation of the gaming license in cases of severe or repeated violations.

To prevent compliance failures, GAMEPLAY INTERNATIONAL B.V. works closely with the Gaming Control Board, ensuring that all corrective actions are implemented and that regulatory expectations are met at all times.

Commitment to AML/CTF/CPF Compliance

By undergoing regular independent audits and maintaining strict regulatory oversight, GAMEPLAY INTERNATIONAL B.V. demonstrates its commitment to financial crime prevention, transparency, and regulatory compliance. The audit process serves as a proactive measure to enhance the company's AML/CTF/CPF framework, ensuring that risks are effectively mitigated and that the highest integrity standards are upheld within the iGaming industry.

11. Responsibilities of the Management

Senior management at GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) plays a crucial role in assessing and mitigating Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) risks. The Board of Directors (BoD) ensures effective oversight by requiring the appointed AML/CTF/CPF Officer to submit regular reports detailing significant changes, risk developments, and updates to the company's compliance framework. Additionally, the AML/CTF/CPF Officer provides an annual assessment evaluating the effectiveness of the company's safeguards against financial crime risks, ensuring continuous enhancement of compliance measures.

As part of its regulatory obligations, senior management conducts annual reviews of company policies and procedures, ensuring they remain effective, relevant, and aligned with evolving legal requirements. These reviews are informed by monthly risk assessments, which help identify potential vulnerabilities within the company's internal controls and risk management systems. If deficiencies are detected, the AML/CTF/CPF Officer presents recommendations for improvements to the Board for approval, reinforcing the company's commitment to a robust compliance framework.

Senior management also oversees the development and implementation of comprehensive employee training programs, ensuring staff—particularly those in high-risk positions—are well-equipped to recognize and respond to suspicious activities. These ongoing training initiatives keep employees informed about AML/CTF/CPF risks, emerging regulatory changes, and best practices in financial crime prevention.

To maintain strong internal controls, senior management ensures that role segregation, defined authorization protocols, and continuous monitoring remain in place. Documentation is maintained in accordance with regulatory standards, ensuring transparency in all financial transactions. To further reinforce compliance, the company conducts regular independent audits and assessments, offering an unbiased evaluation of its AML/CTF/CPF program. These audits help identify areas for improvement, allowing the company to proactively address compliance challenges and strengthen its financial crime prevention framework.

12. Training & Record Keeping

Employee Training

At GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409), a comprehensive training program in Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) is in place to ensure that all employees possess the necessary knowledge and skills to detect and prevent financial crimes. This training is an integral component of the company's compliance framework, ensuring that employees understand legal obligations, recognize suspicious activities, and follow proper reporting procedures. A well-informed workforce plays a vital role in the effective implementation of AML/CTF/CPF policies, strengthening both the company's integrity and the credibility of the gaming industry as a whole.

The training program is role-specific, meaning that employees receive education tailored to the risks associated with their responsibilities. It is mandatory for all employees, regardless of their position within the company. Senior management is trained in policy implementation and strategic compliance oversight, while compliance officers receive in-depth instruction on regulatory requirements and transaction monitoring. Customer-facing staff, operational teams, and finance personnel are also trained to identify red flags, enforce Customer Due Diligence (CDD) measures, and manage transaction reviews effectively. As every employee contributes to the company's compliance efforts, participation in AML/CTF/CPF training is essential.

New employees complete comprehensive AML training upon joining the company, ensuring they are fully aware of compliance policies from the outset. Additionally, all employees participate in mandatory refresher courses at least once per year to stay updated on evolving AML/CTF/CPF regulations and industry best practices. Employees in high-risk roles, such as compliance officers and customer verification personnel,

undergo more frequent, specialized training sessions to reinforce key compliance principles and address emerging threats.

The training curriculum covers a wide range of topics to ensure employees develop a thorough understanding of financial crime risks and prevention measures. Employees receive instruction on AML/CTF/CPF laws applicable in Curaçao, alongside the company's internal policies and procedural requirements. The training emphasizes proper customer identification and verification through Know Your Customer (KYC) and Customer Due Diligence (CDD) protocols, equipping staff with the ability to identify suspicious activity, such as unusual transaction patterns, structured deposits and withdrawals, and transactions involving high-risk jurisdictions. Employees also receive guidance on record-keeping requirements, the consequences of non-compliance, and emerging trends in financial crime prevention.

To enhance engagement and knowledge retention, the company employs a variety of training methods, including in-person workshops, online courses, and e-learning modules. These sessions incorporate case studies, role-playing exercises, and transaction simulations, enabling employees to apply their knowledge in real-world compliance scenarios. This combination of instructional approaches ensures that employees fully understand their responsibilities and can effectively contribute to the company's AML/CTF/CPF compliance program.

Training sessions are led by qualified AML professionals, including internal compliance officers and external consultants with expertise in financial crime prevention. These experts ensure that training materials remain up to date with the latest regulatory developments, risk trends, and enforcement actions. By maintaining a structured and evolving AML/CTF/CPF training program, GAMEPLAY INTERNATIONAL B.V. fosters a culture of compliance, enabling employees to play an active role in detecting and preventing financial crimes, while ensuring full adherence to regulatory obligations.

Record Keeping

GAMEPLAY INTERNATIONAL B.V. maintains a comprehensive record-keeping framework to ensure full compliance with AML/CTF/CPF regulations. The company prioritizes data security, accessibility, and regulatory adherence, ensuring that all relevant records are properly maintained and safeguarded.

To comply with Curaçao's financial regulations, the company retains key documentation for a minimum of five years, including customer identification records, transaction data, suspicious activity reports (SARs), training records, and internal audit logs. These records serve as critical reference points for regulatory audits and investigations, promoting transparency and facilitating cooperation with financial authorities.

Data security is a core aspect of the company's record-keeping strategy. All records are encrypted and stored using secure access controls to prevent unauthorized access or tampering. Access to sensitive compliance data is strictly limited to authorized personnel, and all user activity is logged and monitored to ensure accountability. To further strengthen security, regular audits are conducted to verify record integrity and identify

potential vulnerabilities, reinforcing the company's commitment to data protection and confidentiality.

To streamline record management, the company employs a structured classification and retrieval process, allowing for efficient access to documentation when required. This ensures that authorized employees and regulatory bodies can promptly retrieve information during audits, compliance reviews, or investigations. In addition to secure data storage, the company implements continuous internal monitoring and periodic external audits to ensure that record-keeping practices remain aligned with evolving AML/CTF/CPF regulations.

By maintaining structured and secure records, GAMEPLAY INTERNATIONAL B.V. ensures compliance with legal and regulatory requirements, strengthens internal auditing processes, and enhances operational transparency. These diligent record-keeping practices contribute to the integrity of the gaming industry, reinforcing the company's commitment to compliance, accountability, and ethical business conduct.



(SMES)

Solutions for Management
and Employment Support N.V.

20-02-2025