

Business Risk Assessment for Trendy Games B.V. (FridayBet.com)

Executive Summary

Trendy Games B.V., operating the FridayBet.com online gaming platform under a Curaçao license, has conducted a comprehensive **Business Risk Assessment (BRA)** to evaluate and mitigate risks related to money laundering (ML), terrorist financing (TF), fraud, and cyber threats. This BRA focuses **exclusively on fiat payment channels** (no cryptocurrency is permitted) and uses a **risk-based approach (RBA)** with quantitative scoring to identify inherent risks, assess the effectiveness of mitigation measures, and determine residual risk levels. Key risk domains include the company's **Products & Services, Customer base, Delivery Channels, Geographic exposure, Transaction flows, Technology infrastructure, and Human Factors**. Each domain has been analyzed for ML/TF vulnerabilities, fraud exposure, and cyber-security threats.

Overall, Trendy Games B.V. maintains a **moderate residual risk profile** after applying robust controls and safeguards. High inherent risks – inevitable in a global online gambling operation – are systematically reduced through strong Know-Your-Customer (KYC) procedures, transaction monitoring systems, staff training, and cybersecurity protocols. The new **2025 Curaçao Gaming Authority (CGA) regulatory regime** and relevant Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) laws (including the **National Ordinance Reporting Unusual Transactions (NORUT)** and the “**Regeling Indicatoren**” for unusual transaction indicators) have been carefully considered. Trendy Games is fully committed to compliance with these requirements and the FATF Recommendations, and this BRA is designed to satisfy the expectations of both regulators and banking partners. Key findings include:

- **Inherent Risk:** Online casino and sports betting services carry high inherent ML/TF risk (due to potential misuse of gambling to launder illicit funds) and fraud risk (e.g. payment fraud, identity theft), exacerbated by a global customer base and non face-to-face delivery channel.
- **Mitigation Measures:** The company employs a multi-layered mitigation strategy: rigorous customer due diligence, automated transaction monitoring and fraud detection, geo-restrictions to block high-risk jurisdictions, secure technology and cybersecurity defenses, and ongoing employee training and oversight.
- **Residual Risk:** After applying controls, most risk categories are **moderate** or **low-moderate**. The highest residual risk area is **Geographic Exposure**, given the varied risk levels of markets served (mitigated by strict exclusion of certain high-risk regions). All residual risks are within the company's risk appetite and are deemed manageable with current controls.
- **Regulatory Compliance:** Trendy Games' risk management program aligns with the 2025 CGA framework and AML ordinances, ensuring all **FATF-aligned obligations** (customer identification, record-keeping, ongoing monitoring, and reporting of unusual/suspicious activities) are met. The Business Risk Assessment and accompanying **Customer Risk Assessment (CRA)** scoring methodology demonstrate a proactive stance in preventing ML/TF.

- **Ongoing Review:** The BRA will be reviewed and updated at least annually, or sooner if material changes occur (e.g. expansion to new markets or products), ensuring continuous improvement and responsiveness to emerging risks.

This report provides a detailed breakdown by risk category, a structured customer risk scoring model, and an updated residual risk matrix. It is formatted to facilitate review by regulators (CGA) and financial institutions, reflecting Trendy Games B.V.'s commitment to transparency and robust risk management.

Company Overview & Regulatory Framework

Company Profile: Trendy Games B.V. is an online gaming operator licensed in Curaçao, offering a **diverse portfolio of gambling services** through its platform FridayBet.com. The product suite includes: **sports betting** (pre-match and live betting on global sports), **RNG casino games** (slots and virtual table games powered by Random Number Generators), and **live casino games** (real-time table games with live dealers). Operations are global in reach, serving customers online in multiple jurisdictions **excluding restricted markets** where online gambling is prohibited or high-risk (e.g. the United States, sanctioned countries, etc.). All customer transactions are in fiat currency (e.g. EUR, USD, etc.), processed via approved payment providers – no cryptocurrency is accepted, per company policy and regulatory guidance. The customer base ranges from casual recreational bettors to higher-stakes VIP players, all of whom are subject to the same core compliance standards.

Licensing and 2025 CGA Regime: Trendy Games operates under an on-line casino license, issued by **Curaçao Gaming Authority (CGA)**. The CGA requires licensees to have a comprehensive AML/CFT compliance program, including: a documented Business Risk Assessment, Customer (client) Risk Assessment procedures, internal policies for Know Your Customer (KYC) and record-keeping, and active monitoring and reporting of suspicious activities. The 2025 regime introduces more direct regulator supervision (replacing the former sub-licensing system) and mandates stricter **fit-and-proper tests** for operators, enhanced due diligence on owners, and more robust compliance audits. Trendy Games B.V. is fully committed to meeting these enhanced obligations and has updated its BRA and policies accordingly.

AML/CFT Legal Obligations: As a Curaçao-licensed entity, Trendy Games is subject to the jurisdiction's AML/CFT laws and regulations, which are heavily influenced by the recommendations Financial Action Task Force (FATF)** and the Kingdom of the Netherlands' AML framework. Key legal instruments include:

- **National Ordinance on the Reporting of Unusual Transactions (NORUT):** This law requires financial institutions and designated non-financial businesses (including gambling operators) to **identify and report unusual transactions** to the national Financial Intelligence Unit (FIU). Unusual transactions are defined by certain indicators (see *Regeling Indicatoren* below) or any transaction raising suspicions of ML/TF. Trendy Games must file Unusual Transaction Reports (UTRs) with the FIU (also referred to as the Meldpunt Ongebruikelijke Transacties) **without undue delay** for any transaction meeting these criteria. Reporting under NORUT is a legal obligation, even if a reported transaction

may later be deemed innocent – it ensures potential illicit activity is evaluated by authorities.

- **“Regeling Indicatoren” (Indicator Regulations):** This is a regulation that provides **specific indicators for unusual transactions** in various sectors. For the gaming sector, it lists objective criteria that automatically make a transaction reportable (for example, a single or cumulative transaction above a certain monetary threshold, or transactions linked to certain high-risk countries or persons), as well as subjective criteria (any transaction a casino **knows or suspects** may be related to criminal activity. Trendy Games’ internal transaction monitoring rules are calibrated to capture these indicators – e.g., large deposits or payouts over regulatory thresholds trigger automatic review and potential reporting, as do patterns like rapid in-and-out movements of funds or use of multiple accounts.
- **Customer Due Diligence (CDD) and Identification:** Curaçao’s laws (historically influenced by the Netherlands’ **Wwft** and **Sanctieregelingen**) require casinos and gaming operators to **verify customer identity** and, when applicable, the source of funds. Under the CGA’s expected guidelines, all customers must be **identified and age-verified** before gambling, and **enhanced due diligence (EDD)** must be applied for higher-risk customers (such as Politically Exposed Persons or those from high-risk countries). Trendy Games implements rigorous KYC checks based on a risk-based approach: collecting government-issued photo ID, proof of address, and verifying the information through reliable sources. No anonymous play or payouts are allowed. Additionally, the company screens customers against international sanctions and PEP lists at signup and on an ongoing basis, complying with applicable sanctions laws (UN, EU, OFAC lists as applicable). Accounts belonging to individuals on sanctions lists are prohibited, and any match to a sanctions list results in account freezing and reporting as required.
- **Record-Keeping:** Per AML regulations, Trendy Games keeps comprehensive records of all customer identification documents, transactions, and due diligence measures for the legally required retention period (typically 10 years, per international standard). This ensures that audit trails are available for any investigation, and it’s also a CGA requirement to maintain such records for regulatory inspections.
- **FATF Recommendations Alignment:** The AML/CFT program is designed in alignment with the FATF’s 40 Recommendations. Notably, **FATF Recommendation 22** classifies casinos (including internet casinos) as designated businesses that must implement CDD and record-keeping measures akin to financial institutions. Additionally, **FATF Recommendation 1** emphasizes a risk-based approach where countries and businesses should identify and mitigate their ML/TF risks. In line with this, Trendy Games has embraced a risk-based approach in this BRA, devoting greater resources and stricter controls to higher-risk areas. **FATF Recommendation 23** also requires such businesses to report suspicious transactions – which is operationalized via compliance with NORUT for unusual transaction reporting.

Risk-Based Approach Methodology

Trendy Games employs a **Risk-Based Approach (RBA)** to identify and manage risks, meaning resources and controls are allocated in proportion to the level of risk identified. The methodology for this Business Risk Assessment is as follows:

- **Risk Identification:** We identified potential inherent risks across all aspects of the business that could facilitate money laundering, terrorist financing, fraud, or cybercrime. We categorized these risks into seven key **Risk Categories**:
 (1) **Products & Services**,
 (2) **Customers**,
 (3) **Delivery Channels**,
 (4) **Geography**,
 (5) **Transactions**,
 (6) **Technology**,
 (7) **Human Factors**.

These categories encompass both external risk factors (e.g. the nature of our products, or the jurisdictions we serve) and internal risk factors (e.g. our technology and staff practices).

- **Inherent Risk Assessment:** For each risk category, we evaluated the **inherent risk level**, i.e. the level of risk present if no specific controls or mitigations were in place. Inherent risk is assessed by considering both the **likelihood** of an adverse event (e.g. the probability that money laundering could occur through a given product or channel) and the **impact** or severity if it did occur (e.g. regulatory, financial, and reputational damage). We use a quantitative **scoring scale from 1 (Very Low) to 5 (Very High)** for each category's inherent risk. For example, a category scored 5 would be one with very likely occurrences of ML/TF or fraud and with potentially severe consequences, whereas 1 would indicate minimal risk.
- **Control Evaluation:** We then identified and documented all existing **mitigation measures/controls** that address the risks in each category. These include preventive controls (like KYC verification to prevent anonymous accounts), detective controls (like automated alerts to detect suspicious activity), and corrective controls (like incident response procedures). We gauged the **strength and effectiveness** of each control (considering factors such as coverage, consistency of implementation, and any historical incidents indicating control gaps). Some controls are enterprise-wide (e.g. an AML transaction monitoring system affects multiple categories), while others are specific (e.g. IT firewall pertains to Technology risk).
- **Residual Risk Assessment:** Taking into account the mitigating controls, we re-assessed the risk level for each category to determine the **residual risk** – the risk that remains after controls are applied. Residual risk also is scored on the 1 to 5 scale. We define residual risk as acceptable if it falls within Trendy Games' risk appetite (generally "**Moderate**" or **lower** on our scale). If any residual risk were assessed as "High" or above appetite, it would trigger a need for additional controls or a reconsideration of the business strategy in that area.
- **Weighted Scoring & Heat Map:** Each category's risk score (inherent and residual) is documented, and we assign **weightings** to reflect the relative contribution of each category to the overall business risk. For instance, **Customer risk and Transaction risk** might be weighted higher (given their criticality in ML/TF) than, say, Human Factors, when computing an overall risk score. The weighted scores feed into an overall risk evaluation. We also utilize a **risk heat map** visualization, plotting likelihood vs. impact for each risk category, to easily identify areas of highest concern (e.g. high likelihood & high impact

items appear in the red zone of the heat map). This visual tool helps management and regulators quickly grasp the risk landscape.

PROBABILITY	Very High	4	4	5	5	5
	High	3	3	4	4	5
	Medium	2	2	3	4	5
	Low	1	2	2	3	4
	Very Low	1	1	2	3	4
		Insignificant	Minor	Moderate	Major	Severe
	IMPACT					

- **Risk Rating Definitions:** For clarity, our risk ratings correspond roughly to the following qualitative definitions: **1 (Low)** – minimal risk, well within appetite; **2 (Low-Moderate)** – minor issues possible, requires routine controls; **3 (Moderate)** – notable risk that needs active management; **4 (High)** – significant risk, controls must be robust and maybe enhanced; **5 (Very High)** – critical risk, close monitoring and possibly outside risk appetite without major change. Each category in the next section is discussed in terms of inherent vs residual rating on this scale.
- **Documentation and Approval:** The findings of this BRA are documented in this report, including tables and scoring evidence. The BRA has been reviewed and approved by senior management and the designated Compliance Officer. It will be provided to the CGA and to banking partners on request to demonstrate our risk management approach.

This structured and quantitative RBA methodology ensures that Trendy Games not only identifies where its greatest risks lie but also can **demonstrate the rationale** for its risk ratings and the sufficiency of its controls to regulators and banks. The next sections break down the risk analysis by category, detailing inherent risks, existing mitigations, and residual risk outcomes.

Inherent Risk Assessment and Mitigation by Category

In this section, we examine each risk category in detail, describing the inherent risks present, the mitigation measures in place, and the resulting residual risk after those measures. Each category is analyzed with respect to ML/TF risk as well as fraud and cyber-security considerations where applicable.

1. Products & Services Risk

This category assesses the nature of Trendy Games gambling products and services and how they might be exploited for illicit purposes. Trendy Games offers **sports betting, RNG casino games, and live dealer casino games**, all of which have associated risk profiles.

Inherent Risk Factors:

- **High-Value Turnover & Payouts:** Gambling products inherently involve flows of funds (bets and winnings) that could be used to “clean” illicit money. Criminals may deposit dirty money, place bets, and then withdraw “winnings” as ostensibly legitimate funds. Sports betting and casino games can facilitate this, especially if bets can be structured to minimize losses. For example, a launderer might bet on low-odds outcomes or two opposite outcomes (with multiple accounts) to guarantee some return of funds. The potential for converting ill-gotten cash into gambling credits and then into seemingly clean payouts makes the sector attractive for money laundering.
- **Product Specific Risks:** Different products have unique angles of exploitation:
 - *Sports Betting:* Could be used for match-fixing or collusion, where criminals manipulate events to ensure certain bets win (though as a bookmaker, FridayBet is exposed as a victim in match-fixing scenarios). Also, sports betting with very low margins might allow laundering with minimal loss.
 - *Casino RNG Games:* These have a built-in house edge, meaning a launderer would likely lose a small percentage when cycling money through slots or roulette. However, they might consider it an acceptable “fee” for cleaning funds. Large, frequent bets or playing specifically low-house-edge games (like certain blackjack strategies) could signal laundering intent to cycle money.
 - *Live Casino:* Similar to RNG table games, but involves human dealers. No additional anonymity, but higher betting limits typical at live tables may attract high-rolling players including potential launderers aiming to churn larger sums quickly.
- **Jackpots and Big Wins:** If the platform offers jackpots or high payouts, a criminal might attempt to mask illicit funds as a “lucky win”. For instance, depositing money, deliberately taking high-risk bets, and claiming any remaining funds as jackpot winnings. While outcomes are random, this *jackpot narrative* can be used by launderers to explain wealth if they win even a portion back.
- **No Crypto Services:** (Positive note for risk) The company does **not offer crypto-gambling or crypto payments**, which actually *reduces* inherent risk compared to some competitors. Crypto can add layers of anonymity and regulatory complexity. By sticking to fiat-only, Trendy Games avoids crypto-specific ML risks.

Considering these factors, the **Inherent Risk Level for Products & Services is rated High (4/5)**. Online gambling is recognized internationally as a higher-risk sector for ML, and by offering popular betting and gaming services globally, FridayBet faces an inherently elevated risk that its products could be misused by criminals or corrupt actors to launder funds or engage in fraudulent schemes.

Mitigation Measures for Products & Services:

Trendy Games has implemented robust controls embedded into its products and platform to counter these risks:

- **Account-Based Play with KYC:** All gambling activities on FridayBet require a registered user account that has passed KYC verification. There are **no guest accounts or anonymous betting**. This ensures every bet is tied to an identified individual, greatly mitigating the risk of unknown actors using the products. KYC details (identity, age,

address) are verified before any significant play or any withdrawal, preventing access by alias identities.

- **Transaction Monitoring & Betting Pattern Analysis:** The platform's **automated monitoring system** tracks betting patterns and game play in real time. It is configured with rules to flag unusual gambling behaviors that could indicate ML or fraud, such as:
 - *Abnormal Betting Patterns:* e.g. very large bets relative to a customer's profile, or minimal gameplay (betting a large sum once and immediately withdrawing), or simultaneous opposite bets on the same event (which might indicate two colluding accounts).
 - *Rapid Cycles of Deposit-Bet-Withdraw:* e.g. a user depositing €10,000, placing a few even-chance bets (like red/black in roulette) and then withdrawing most of the balance – this cycle is flagged as suspicious as it resembles layering of funds.
 - *Multiple Accounts or Linked Identities:* The system uses device fingerprinting and other data to detect if one person might be operating multiple accounts to bypass betting limits or to bet both sides of an event. Detected multi-accounting leads to investigation.
- **Bet Limits and Wager Requirements:** As a policy, FridayBet imposes certain limits that incidentally help mitigate ML risk – for instance, **maximum bet limits on certain high-risk games** and **limits on quick successive large bets**. Additionally, for bonus offers, wagering requirements prevent immediate withdrawal of bonus funds without play (closing a potential fraud loophole). While these are mainly for operational and promotional integrity, they also discourage the quick-in/quick-out abuse by launderers.
- **Product Design & Provider Due Diligence:** All RNG and live dealer games come from vetted, licensed software providers. This ensures game integrity (no rogue software that could be manipulated by criminals to guarantee wins). The company performs due diligence on game providers to confirm they themselves comply with AML/CFT and fairness standards. This mitigates the risk of outsiders introducing tampered games or backdoors.
- **Ongoing AML Training with Product Focus:** The compliance team and customer support are trained to understand how each product can be misused. For example, support staff monitor chat in live casino for any collusion hints. The betting risk team gets alerts on suspicious sports bets (e.g. unusually large bets on obscure leagues which could hint at match-fixing or ML). This human oversight complements automated controls.
- **No Cash or Physical Chip Interface:** By operating purely online with fiat through financial institutions, many classical casino ML methods (like buying chips with cash and redeeming) are not applicable. This inherently removes some avenues of risk that physical casinos face.

Residual Risk (Products & Services): After applying the above mitigation measures, the risk associated with Products & Services is significantly reduced. The platform's requirement for identified accounts and its vigilant monitoring of gameplay patterns greatly lowers the likelihood of undetected laundering or fraud through the games. However, some residual risk remains **Moderate (2/5)** because no system is foolproof – a very determined launderer might still attempt to test the controls, and the inherently high throughput of funds in gambling means some suspicious activity might only be detected after the fact. Continuous fine-tuning of monitoring

rules and periodic independent audits of gaming transactions are used to keep this risk at an acceptable level.

2. Customer Risk

This category examines the risks stemming from the **types of customers** who use FridayBet.com and their attributes. Certain customer profiles or behaviors can elevate the risk of ML/TF or fraud (for example, a politically exposed person gambling large amounts, or an account with unclear source of funds).

Inherent Risk Factors:

- **Global Customer Base:** By serving customers globally (outside restricted markets), Trendy Games inevitably attracts a wide range of individuals. This includes customers from various economic backgrounds, occupations, and risk profiles. Some customers may originate from high-risk industries (e.g. cash-intensive business owners) or have links to higher-risk jurisdictions. The sheer diversity increases the inherent risk that a certain percentage of users could be involved in illicit activity.
- **Politically Exposed Persons (PEPs) and High-Profile Individuals:** PEPs (such as government officials or their family members) pose higher corruption and money laundering risk. An online casino could be seen as a way to funnel bribe money or embezzled public funds. Without controls, such individuals might seek to gamble large sums to obscure the money's origin. Similarly, other high-profile or high-net-worth individuals might pose higher ML risk if their source of wealth is unclear. The platform inherently could attract such users given its global reach.
- **Criminal Actors or Frontmen:** There is an inherent risk that **criminal organizations or terrorist financiers** might attempt to register accounts, either under their own identity or using straw men/proxies, to launder money. For example, a drug trafficking ring might recruit individuals to open accounts and process dirty money through gambling. The anonymity of online registration (if unchecked) could make it easier for such frontmen to operate compared to entering a physical casino with cameras.
- **Underage or Vulnerable Persons:** While not directly an ML risk, minors or problem gamblers attempting to access the site is a social responsibility risk and could indirectly relate to fraud (identity misuse). The inherent risk exists that without strong verification, underage individuals could register using false details. This is illegal and could also be a vector for fraud (e.g. a minor using a parent's credit card unbeknownst).
- **Customer Fraud Behavior:** Some customers might inherently pose fraud risk – e.g. using stolen payment cards, engaging in bonus abuse, or colluding with others to defraud the operator (like chip-dumping in poker, although FridayBet doesn't list poker, collusion could still occur in multiplayer bets or through coordinated betting). Accounts created solely to abuse promotions or launder money might show certain tell-tale behaviors if not controlled for.

Given these factors, the **Inherent Risk Level for Customer Risk is High (4/5)**. The platform could be targeted by a range of high-risk individuals and the impact of onboarding a criminal (who

then launders money or causes legal issues) is significant. Without robust customer due diligence, the customer base could become a major vulnerability.

Mitigation Measures for Customer Risk:

Trendy Games has put extensive measures in place to know its customers and manage their risk:

- **Customer Due Diligence (CDD) at Onboarding:** Every new customer must undergo CDD at account creation. **Identity Verification** is mandatory. Accounts remain restricted (no withdrawals, limited deposits) until verification is completed. This process filters out most fake or stolen identities and deters would-be anonymous bad actors.
- **Age and Identity Verification:** The system automatically verifies that the customer is **18+ (legal gambling age)**. Any underage applicant is rejected immediately. Additionally, identity information is checked for any known fraud indicators (like an ID that has been used by multiple people, or an address that is a known mail drop). This mitigation addresses underage risk and basic identity fraud risk among customers.
- **PEP and Sanctions Screening:** Upon registration and periodically thereafter, all customers are screened against up-to-date **PEP lists, sanctions lists, and adverse media databases**. Trendy Games utilizes a compliance screening tool that flags if a new registrant's name matches a politically exposed person or someone on international sanctions/watchlists. If a match occurs (or even a potential match that needs review), the compliance team reviews it. Confirmed PEPs are allowed to proceed only under enhanced due diligence; sanctioned individuals or those with unacceptable adverse media (e.g. known criminals) are denied service and reported as required. This ensures high-risk individuals are either not onboarded or are identified and monitored closely from the start.
- **Risk Profiling and Scoring:** As part of the **Customer Risk Assessment (CRA)** process (detailed in a later section), each customer is assigned a preliminary risk rating (low, medium, high) based on their profile at onboarding. Factors include their nationality, country of residence, occupation (if collected or inferred), PEP status, and initial deposit amount. For example, a customer from a low-risk country depositing a small amount might be rated low risk, whereas a customer from a higher-risk jurisdiction or who immediately deposits a very large sum would be rated higher risk. High-risk customers are required to undergo **EDD** – providing additional information such as source of funds or wealth, and obtaining senior management approval to continue the relationship.
- **Source of Funds (SoF) Checks:** For customers who reach certain deposit thresholds or exhibit high spending, Trendy Games conducts Source of Funds checks. Customers may be asked to provide evidence of how they obtained the money they are gambling (e.g. salary slips, bank statements, business income, or inheritance documents). This is crucial for detecting if funds might be coming from illicit sources. If a customer cannot reasonably account for their funds relative to their profile, it raises a red flag. The company has set triggers (like cumulative deposits exceeding €50,000 or a single large deposit that's unusual) to request SoF documentation. Refusal or inability to comply can result in account suspension.
- **Ongoing Monitoring of Customer Activity:** Beyond initial checks, the customer's behavior is continuously monitored. The transaction monitoring system and fraud detection tools look at how each customer transacts: their deposit frequency, bet sizes, game choices, win/loss patterns, withdrawal behavior, etc. Significant deviations from the expected

profile (e.g., a normally low-stakes player suddenly starts depositing large amounts, or a customer from one country consistently logs in from another region) will trigger alerts for review. This ongoing monitoring can catch customers who were low risk at onboarding but later exhibit high-risk indicators.

- **Customer Interaction & Review:** The VIP/high-value customer team and the compliance team collaborate to keep an eye on big spenders. High-risk customers (by CRA rating) have periodic account reviews – e.g. quarterly or monthly – where their activity is scrutinized more deeply and their risk rating is updated. The company also employs measures like direct interaction: if needed, contacting the customer to get clarity on unusual behavior (in line with tipping-off rules – such interactions are carefully handled to avoid tipping off a suspicious customer that they are under scrutiny).
- **Limits and Controls:** Customers can be subject to tailored limits based on risk. For example, new customers or those with higher risk may have lower deposit or withdrawal limits until they build transaction history and trust. The system can impose dynamic limits (automatically or manually by compliance) to manage risk exposure per customer.
- **Account Closure and Reporting:** If a customer is deemed too risky (e.g., appears to be using the account for laundering or is found to be a sanctioned entity), Trendy Games will promptly close the account and freeze funds as necessary. An unusual activity report (UTR) will be filed with the FIU under NORUT, and in certain cases law enforcement may be notified. The BRA process ensures criteria for exiting relationships with unacceptable risk are clear.

Residual Risk (Customers): With these strong KYC, screening, and monitoring measures, the **residual customer risk is reduced to Moderate (2/5)**. Most legitimate customers pose low risk and are served normally, while those few that fall into higher risk categories are identified and managed with enhanced measures. The possibility remains that a well-concealed bad actor could slip through initial checks (for example, someone with no record on watchlists who is laundering moderate sums), or that a customer's risk elevates over time. However, the layered defenses greatly mitigate the chance that such activity goes unnoticed or unaddressed for long. Residual risk is thus at an acceptable level, with vigilance maintained via continuous monitoring and periodic re-screening.

3. Delivery Channels Risk

Delivery channels refer to **how products and services are delivered to customers** – in this case, the channels are entirely remote/online via digital platforms (web and mobile). The risk here involves the vulnerabilities of non face-to-face interactions and any intermediaries in reaching customers.

Inherent Risk Factors:

- **Non Face-to-Face Onboarding:** FridayBet's customer acquisition is 100% online. The inherent risk of remote customer onboarding is higher than face-to-face because the business **cannot physically verify identity documents or the presence of the customer**. Digital onboarding can be exploited with stolen or forged identification, and there is a risk of **identity fraud** (someone using another person's identity to open an account). This

makes robust digital verification critical, but inherently, the lack of in-person contact elevates risk.

- **Global Accessibility:** The platform is accessible via the internet globally (except geo-blocked locations). This means anyone with an internet connection could attempt to access the service, including from countries that are supposed to be restricted. Sophisticated users might use VPNs or other means to mask their location. The delivery channel being the open internet inherently introduces risk that bad actors will attempt to **bypass geo-restrictions** or anonymity controls.
- **Use of Third-Party Introducers/Affiliates:** Like many online gaming companies, Trendy Games likely uses affiliate marketing and third-party advertising to attract customers. Affiliates are essentially a delivery channel for new players. If not properly vetted, affiliates could introduce risks by bringing in customers through deceptive means or from banned locations. Inherent risk exists if an affiliate were complicit with criminals (e.g. knowingly referring high-risk gamblers for a share of profits) or if the company relied on an affiliate's due diligence (Trendy Games does **not outsource KYC to affiliates**, but the volume of affiliate traffic could challenge the onboarding process).
- **24/7 Digital Service:** The online channel is available 24/7 and is highly automated. This means large volumes of transactions and interactions occur without direct staff oversight at each moment. The inherent risk is that suspicious activity might occur in real-time when compliance staff are not immediately watching (though automated systems are). Also, the immediate and rapid nature of online transactions (deposits and bets can happen within seconds) means a lot could happen in a short time before any manual intervention is possible.
- **Mobile App/Platform Security:** If the service has a mobile app or just a web interface, there is a risk that if the app or site has vulnerabilities, criminals could exploit those channels (for example, creating scripts/bots to automate fraudulent transactions or probe for weaknesses). While more of a technology risk, it's related to the delivery channel being digital.

Given these factors, the **Inherent Risk Level for Delivery Channels is High (4/5)**. The purely online, non-face-to-face nature of FridayBet's service means higher exposure to identity fraud, global anonymity issues, and reliance on technology for control. The wide funnel of customer entry via the internet is inherently risky without strong controls.

Mitigation Measures for Delivery Channels:

Recognizing these risks, Trendy Games has instituted controls and practices to secure its delivery channels:

- **Robust Digital Verification Tools:** As noted in the Customer risk controls, the company employs advanced verification solutions. By leveraging technology, Trendy Games compensates for the lack of face-to-face contact with a high degree of assurance in digital identity proofing.
- **IP and Device Intelligence:** The platform records the **IP address, device type, and other browser fingerprints** of each login and registration. GeoIP checks automatically flag if someone is signing up from a restricted jurisdiction. If a user tries to use a VPN or proxy, the system often can detect mismatches (e.g., IP says one country, but their declared

address is another; or known VPN IP ranges). High-risk or Tor network access is blocked outright. This reduces the risk of customers masking their true location. In cases where a legitimate customer is traveling, additional verification is done to ensure it's still them (for instance, requiring a 2FA or security check on login from a new country).

- **Affiliate Management and Due Diligence:** Trendy Games runs an affiliate program for marketing, but with strict oversight. Affiliates are **subject to due diligence** – they must be approved partners who are vetted for reputation and legal compliance. The affiliate contracts include clauses that they must not target prohibited countries or use misleading tactics. The company monitors traffic sources; if an affiliate were found sending traffic from blacklisted regions or engaging in questionable referrals, that partnership would be terminated. By controlling who can promote the site, the company mitigates the risk of bad actors entering via affiliates.
- **Automated Controls and Flags:** Given the 24/7 automated nature of the service, the company relies on real-time automated controls within the delivery channel. For example, the system may automatically restrict an account if certain risk thresholds are hit (such as too many failed login attempts – mitigating account takeovers, or multiple accounts detected on one device). It also has velocity limits – limiting how fast one can deposit or how many bets per minute, to prevent automated bot abuse or rapid movement of money atypical for a human user.
- **User Activity Monitoring:** Not only transactions, but also general user activity on the platform is logged and can be analyzed. Unusual patterns like a single device being used to access many different accounts (potential **device sharing or fraud rings**) are detected and investigated. This helps catch situations where one person might be controlling multiple accounts (possibly mule accounts).
- **Customer Communication & Verification:** If there is suspicion about a user's identity or location, the compliance team will reach out to the user for clarification or additional documents. For example, if a user claims to be in Country A but system indicates they often log in from Country B, the user may be asked to explain and provide proof of presence or residency. This direct intervention serves as both a deterrent and a way to resolve discrepancies.
- **Secure Platform Access:** From a tech perspective, the website and app enforce **secure logins** (strong password requirements, two-factor authentication availability for users, etc.). Sessions are encrypted and protected to prevent hijacking. These measures ensure that the delivery channel (web/mobile) itself is not easily compromised to allow unauthorized access or tampering with account information.

Residual Risk (Delivery Channels): With the above controls, the **residual risk for Delivery Channels is lowered to Moderate (3/5)**. We have largely mitigated the risk of anonymous or fraudulent access through stringent verification and monitoring. Nonetheless, some risk remains that sophisticated fraudsters may attempt new methods (for instance, high-quality fake IDs that fool systems, or inventive ways to mask location). The company stays abreast of new fraud trends in the industry (through membership in AML forums and compliance networks) and updates its digital security measures accordingly. The current residual risk is deemed acceptable and is continuously managed.

4. Geographic Risk

Geographic risk assesses the **jurisdictions in which Trendy Games does business or from which it draws customers**, as different countries carry different ML/TF risk levels due to their regulatory environments, corruption levels, and prevalence of financial crime.

Inherent Risk Factors:

- **Global Market Exposure:** FridayBet.com is available globally except for certain blocked jurisdictions. This means inherently exposure to a **mix of countries**, some of which may be well-regulated and low risk, and others which may be considered high-risk or non-cooperative in AML efforts. For example, customers might come from countries with high corruption indices, known drug transit regions, or countries under partial sanctions. Without restrictions, this global exposure is a major risk driver for ML/TF because criminals often route money through jurisdictions where oversight is weaker.
- **High-Risk Jurisdictions:** The FATF regularly identifies **High-Risk Jurisdictions** subject to a call for action (like Iran, North Korea, etc.) and **Jurisdictions under Increased Monitoring** (the “grey list”). If the platform were accessible from such places, the risk of ML/TF would be extremely high. Additionally, countries subject to international sanctions (e.g. certain regimes) pose legal risks – doing business with those residents could violate sanctions and facilitate terrorist financing or proliferation financing.
- **Offshore Financial Centers:** Some customers might be based in or channel funds through offshore financial centers or bank secrecy havens. For example, if a customer’s bank is in a known secrecy jurisdiction, it complicates the transparency of their funds’ origin. Curaçao itself, while improving, has historically been seen as a lenient jurisdiction for gambling – thus other similar jurisdictions might treat Curaçao licensed operators cautiously. Engaging customers from other offshore jurisdictions (like certain Caribbean or South Pacific islands) can raise risk eyebrows among correspondent banks and regulators.
- **Differing Legal Status of Online Gambling:** In some countries online gambling is illegal or unregulated; in others it’s legal but with strict local licensing. If customers from a country where online gambling is illegal access FridayBet (even if against our terms), it creates a legal risk and possibly an AML risk (since those players are by default not monitored by their government, possibly operating in cash economies). Additionally, some regulated markets (like many European countries) expect that citizens only play on locally licensed sites; if they play offshore, from a bank’s perspective, it might appear as a cross-border transaction to a gambling entity, attracting scrutiny.
- **Transaction Routing via Various Countries:** Even if a customer is in a low-risk country, the funds might pass through other countries (e.g., an EU customer using a payment processor based in another country). International fund flows can introduce intermediate geographic risks. For example, a wire transfer might go through a correspondent bank in a high-risk jurisdiction. These indirect geographic exposures are also considered.

Given these factors, the **Inherent Risk Level for Geography is Very High (5/5)** prior to mitigations. Operating globally is core to the business model, but it means without controls, the business could unwittingly serve sanctioned or high-risk areas. Geographic risk is often cited by regulators and banks as a key concern for offshore online casinos, thus it’s treated with high importance.

Mitigation Measures for Geographic Risk:

Trendy Games proactively manages geographic risk through a combination of **country-level policies and transaction controls**:

- **Restricted & Prohibited Jurisdictions Policy:** The company maintains a clear list of **prohibited countries** from which it will not accept customers or transactions. This list includes:
 - Countries under comprehensive international sanctions or embargoes (e.g. North Korea, Iran, Syria, etc.).
 - Countries identified by the FATF as high-risk or with serious strategic AML/CFT deficiencies.
 - Any country where online gambling is explicitly illegal and where offering services could pose legal jeopardy.
 - Other jurisdictions as directed by the CGA or company's risk appetite (for example, perhaps countries with extreme corruption or conflict zones where the risk of terrorist financing is acute).

The registration system automatically blocks attempts to sign up from IP addresses in these countries, and the KYC process will flag addresses or identification from these locations. If somehow a customer from a banned country gets through, once identified, their account is terminated immediately. This policy eliminates the highest-risk geographies from the active customer base.

- **Geographic Risk Scoring:** For allowed countries, the company employs a **country risk-rating system** as part of the CRA. Each country in which customers are allowed is rated High, Medium, or Low risk based on a variety of indices: FATF listing, Transparency International Corruption Perception Index, Basel AML Index, presence of active terrorist groups, etc. For instance, a stable EU country would be Low risk, whereas a country with high corruption and weak AML enforcement might be High risk even if not outright banned. The customer's country risk rating influences their overall risk score (as detailed in CRA section). This means customers from higher-risk countries receive more scrutiny (EDD, transaction limits, etc.) even if the country is not banned.
- **Payment Blocking by Geography:** The payment systems are configured to block transactions (deposits or withdrawals) that involve banks or cards from prohibited jurisdictions. For example, if someone somehow tries to use a credit card issued in a banned country, the payment will be declined. Additionally, certain high-risk payment routes are disallowed. For instance, we might disallow accepting funds from a bank in Country X known for money laundering issues, even if the user claims to be elsewhere. The payment gateway and banking partners provide some level of geo-data that is used in rules.
- **Enhanced Due Diligence for Certain Regions:** If we decide to serve a medium-risk region, we implement **enhanced measures**. For example, if operating in parts of Latin America or Eastern Europe where AML controls vary, we may require additional verification steps for customers (like secondary ID checks, proof of income, etc.) before they can transact large amounts. We also might enforce lower thresholds for unusual

transaction reporting in those cases (reporting even smaller transactions that originate from those regions, as an extra precaution).

- **Regular Review of Country List:** The compliance team regularly updates the prohibited and high-risk country list based on the latest information from the UN, EU, FATF, and CGA directives. For instance, if a country gets added to the FATF high-risk list (grey or black list) or experiences a significant negative event (say a coup or sanctions imposition), we swiftly adjust controls to either block or heighten scrutiny of transactions related to that country. This ensures our geographic risk measures remain current.
- **Segmentation by Geography in Monitoring:** Our transaction monitoring system filters alerts by geography as well. Transactions involving cross-border movement from our main customer countries to unusual locations (e.g., a withdrawal to a bank in a third country that's not the customer's residence) are flagged. This helps identify possibly undisclosed geographic exposure (such as a customer claiming to be in Country A but actually sending money to Country B).
- **CGA and International Cooperation:** Under the new CGA regime, there will be more information sharing about risky jurisdictions and possibly a unified approach among licensees in Curaçao to avoid certain markets. Trendy Games participates in industry forums and follows CGA guidance to ensure its geographic risk controls meet or exceed regulatory expectations. For example, if CGA issues guidance to cease operations in a newly risky region, we will comply immediately.

Residual Risk (Geography): Despite these strong measures, **Geographic risk remains one of the higher residual risks at Moderate-High (around 4/5)**. This is because even with blocking and caution, the business inherently still serves a broad international customer base. There is always a possibility that a determined user from a risky area finds a loophole (e.g., using a foreign identity or a proxy location). Also, the fact that Curaçao itself is not an EU jurisdiction means some counterparties (like EU banks) might perceive any cross-border transaction with our platform as higher risk – an external perception risk we manage through transparency and compliance. Our controls reduce the likelihood of direct sanctions or high-risk country exposure to very low, but they cannot entirely eliminate **country risk factors** for customers who reside in, say, medium-risk jurisdictions. We accept this residual risk as manageable and continuously monitor geopolitical developments. Overall, no business is without geographic risk unless it's extremely geofenced; for our model, the residual geographic risk is kept at a **manageable moderate level**, with CGA oversight adding an extra layer of comfort that we are in line with global norms.

5. Transactions & Payment Channels Risk

This category focuses on the **movement of funds** into, within, and out of the FridayBet platform – essentially deposit and withdrawal channels, transaction patterns, and related fraud risks. Since the BRA scope explicitly excludes crypto, we consider only **fiat payment channels** such as credit/debit cards, bank transfers, and e-wallets.

Inherent Risk Factors:

- **Volume and Velocity of Transactions:** Online gambling involves a high number of financial transactions. Inherent risk lies in the potential for **structured transactions** or

“smurfing” – where a launderer breaks down a large amount of money into many smaller transactions to avoid detection. For instance, without controls, someone could deposit just under a reporting threshold repeatedly. The large volume also makes manual oversight challenging, increasing reliance on automated systems.

- **Multiple Payment Methods:** FridayBet likely supports a variety of payment methods for customer convenience: e.g., Visa/MasterCard, bank wire transfers, and possibly e-wallets like Skrill or Neteller. Each channel has unique risks:
 - *Credit/Debit Cards:* Risk of stolen cards being used (fraud), chargebacks if the card owner disputes the gambling charges (could be used as a form of fraud or even ML layering by pushing money through a credit line), and anonymous prepaid cards if allowed.
 - *Bank Transfers:* These are traceable but can be complex if coming from foreign banks; risk if third-party deposits occur (someone other than the account holder sends money, indicating potential money mule activity). Also, if banks from secrecy jurisdictions are involved, transparency is reduced.
 - *E-Wallets:* Wallets like Skrill/Neteller involve the customer funding an intermediary first. If those e-wallet accounts were themselves funded illicitly, the gambling operator might not see the origin. E-wallets can also be in different names if not careful. However, reputable e-wallets do their own KYC – the risk is somewhat shared.
- **Rapid In/Out Transactions:** A major ML red flag inherently is a customer who deposits a large sum and shortly thereafter withdraws most of it with little gameplay (essentially using the casino account as a passthrough). Without active monitoring, such transactions could occur frequently due to the automated nature of the platform.
- **Transaction Size and Frequency:** Very large transactions carry obvious risk (potential proceeds of crime). Very frequent small transactions can indicate structuring or even automated bot usage. Spikes in transaction activity, especially around known risky periods (like year-end or events) can indicate something like criminals trying to clear accounts.
- **Fraud Risks:** Inherent to transactions are various fraud risks that also tie to ML:
 - *Chargeback Fraud:* A user might deposit with a card, gamble, then issue a chargeback claiming the card was stolen – essentially reversing the legitimate flow and causing losses. Or criminals might use gambling to test stolen card validity.
 - *Bonus Abuse and Arbitrage:* Not directly ML, but multiple accounts could abuse bonuses or arbitrage betting, generating illicit gains (fraud against the house) which then become “clean” money if withdrawn – effectively similar to laundering fraudulently obtained funds.
 - *Insider Payment Manipulation:* Though more of a human risk, if internal staff had access, they could illicitly approve transactions that should be stopped. (We address internal fraud under Human Factors).

Considering all, the **Inherent Risk Level for Transactions is High (4/5)**. The constant movement of funds through various channels is the primary vector for money laundering and fraud to actually happen in practice. If not monitored, the platform could be used like a bank account by criminals.

Mitigation Measures for Transactions & Payments:

Trendy Games employs strict financial controls and monitoring to mitigate transaction-related risks:

- **Approved Payment Processors and Banks:** The company only works with **established, regulated payment processors and banking partners**. Each payment method on FridayBet goes through companies that are themselves regulated for AML (e.g., acquiring banks for card payments, licensed e-money institutions for e-wallets). This means there's an extra layer of KYC/AML at the funding source. For example, credit card issuers have fraud detection, and e-wallets require user verification. We also perform due diligence on our payment partners to ensure they have robust AML controls and are not known to facilitate shady transactions.
- **Name Matching and Third-Party Payment Prevention:** A firm policy is in place: **the name on the payment account must match the customer's name on file**. For withdrawals, the beneficiary account must belong to the verified customer. This prevents third-party payments (e.g., a criminal using someone else's account to launder money through the player's account). If a mismatch is detected (say a deposit comes from a card not in the account holder's name), the transaction is blocked or refunded and the account is reviewed. Typically, customers are informed they can only use their own financial instruments.
- **Deposit and Withdrawal Limits:** Trendy Games sets limits on deposit and withdrawal amounts based on risk and business policy. New or unverified users have low limits until they complete full KYC. Even verified users have daily and monthly maximums for deposits and withdrawals, which can be increased upon request only after further review. These limits help prevent extremely large transfers from happening unchecked. They also give the team a chance to scrutinize high-amount requests (e.g., if someone asks to raise their deposit limit significantly, it triggers a source of funds check).
- **Automated Transaction Monitoring System:** A specialized AML transaction monitoring software is integrated with the platform. It aggregates all customer transactions (deposits, bets, withdrawals) and runs them against predefined **scenarios/rules** and anomaly detection algorithms. Examples of scenarios:
 - Large single deposits over a certain threshold (e.g., €10,000) – triggers an alert if not already justified by the customer profile.
 - Rapid funds turnaround: deposit followed by withdrawal of $\geq X\%$ of funds within a short period – high priority alert.
 - Multiple deposits in a short time frame that cumulatively exceed a threshold (catching structuring).
 - Dormant account that suddenly becomes very active financially.
 - Use of multiple payment methods by one account (especially if they add many different cards or accounts) – could indicate trying to obscure source of money.
 - Withdrawal to a new bank account different from the deposit source – flagged for review of reason.

Each alert is reviewed by the compliance or risk team. The system also uses machine learning to some extent, improving detection of unusual patterns that don't fit normal player behavior.

- **Tiered Due Diligence on Transactions:** The company employs tiered CDD measures depending on transaction sizes. For example: any cumulative transactions (deposit or withdrawal) that exceed €15,000 in a short period will prompt an intermediate review (even if KYC is done) to ensure everything is consistent (this €15k often mirrors an international standard threshold for large transactions). At higher tiers (e.g., €50k+), senior management is notified and explicit sign-off is required to continue the relationship, as per our internal policy. These tiers ensure escalating scrutiny as transaction volumes grow.
- **Real-Time Fraud Controls:** On the fraud side, our payment gateway has fraud scrubbing tools: CVV verification, 3-D Secure for cards (Verified by Visa/MasterCard SecureCode), velocity checks (limiting repeated card attempts), device fingerprinting to catch the same device using multiple cards, etc. These reduce the chance of stolen card use and subsequent chargebacks. If a transaction triggers a fraud rule (e.g., AVS mismatch, or blacklisted card BIN), it's declined automatically. This not only prevents fraud losses but also denies criminals an easy path to test cards via our site.
- **Segregation of Funds and Source Tracking:** The platform maintains clear records linking each deposit to the subsequent withdrawal (if any). Internally, we can trace which deposit(s) any withdrawal is coming from, to ensure, for example, that if a user deposits from a bank account and wants to withdraw to another, we have verified the reasons and consistency (maybe the first account was closed or something; we'd need proof). Normally, we aim to send withdrawals back to the *same source* they came from when possible (cards can be refunded, bank wires back to sender account) to maintain a closed loop, which is a known best practice in AML for gambling.
- **Unusual Transaction Reporting (UTR):** In line with NORUT and indicator regulations, the compliance team files a report to the FIU for any transaction or series of transactions that meet reporting criteria. For instance, if a user's cumulative transactions surpass a set objective threshold (as mandated by the "Regeling Indicatoren" – often a specific large amount) or if transactions are suspicious (subjective indicator), a report is sent. This legal obligation acts as a backstop – even if we cannot fully determine the intent of a transaction, we ensure the authorities are informed when thresholds or suspicions arise.
- **Withdrawal Scrutiny and Freezing:** The company reserves the right to **delay or freeze withdrawals** if suspicious activity is suspected, pending further investigation. This is stated in the terms and is an important control to ensure potentially illicit funds are not paid out until cleared. In practice, if an alert comes on an account that is requesting a payout, the payout is paused until compliance completes a review (and if needed, obtains more info from the customer). This can prevent money from leaving the ecosystem and allow time for possibly filing a report.
- **Audit Trail & Reconciliation:** All transactions are logged with unique IDs and timestamps. Regular reconciliation is done to ensure no anomalies in the system (like no phantom transactions, everything balances). Anomalies could indicate technical issues or fraud. An external auditor also annually reviews our financial transactions and controls, which provides additional oversight.

Residual Risk (Transactions): Through these measures, the **residual risk in Transactions is brought down to Moderate (2/5)**. The automated nature of transaction flow is now buffered by automated detection and manual oversight of flagged cases. The risk of large-scale money laundering going unnoticed is greatly reduced – any large or suspicious transactions are very likely

to be detected and stopped or reported. Fraud risk like stolen cards is mitigated by upfront checks. Some residual risk persists: clever criminals might attempt new patterns that evade known rules, or an internal collusion could bypass a control (though we have those mitigations in Human Factors). Also, not all unusual activity is illicit – so we must balance not stopping legitimate high rollers, which is why the risk can't be driven to zero without impeding business. The current residual risk is acceptable and in line with industry standards for a regulated online gambling firm.

6. Technology & Cybersecurity Risk

This category addresses the risks in the **technical infrastructure and cybersecurity** of FridayBet.com. As an online operation, the integrity and security of the technology environment is paramount to prevent cyber attacks, data breaches, or technical failures that could be exploited for crime.

Inherent Risk Factors:

- **Attraction to Hackers:** Online gambling platforms are often targets for hackers due to the combination of financial transactions and personal data stored, as well as the potential to disrupt service for ransom (Denial of Service attacks). Inherent risk is that a successful cyber attack could lead to theft of funds (e.g., attackers manipulating accounts or payment processes), theft of customer data (leading to identity theft or compromise of customer accounts), or general disruption which could be exploited (e.g., downtime during which fraud goes undetected).
- **Data Breach Risk:** The platform stores sensitive information (personal info, identification docs, financial transaction details). A breach could leak this data, harming customers and the company's reputation, and possibly enabling further financial crime (like identity fraud using stolen data). Inherent risk is significant given the value of such data on black markets.
- **System Integrity and Game Fairness:** The fairness and integrity of the RNG and betting systems must be maintained. Inherent risk exists that a malicious actor (either external or internal) might try to manipulate game software or outcomes – for example, rigging a game to produce certain results or altering odds – either to facilitate fraud (cheating players or the house) or to launder money (e.g., ensuring certain accounts win). While robust game software design mitigates this, it's a risk if systems are compromised.
- **Technology Failures:** A less direct risk to ML/TF but still relevant: if key systems (like the transaction monitoring system or KYC verification service) fail or glitch, there could be a window during which suspicious activities aren't caught. For instance, if the connection to the sanctions screening service goes down, someone on a sanctions list might slip through. Inherent risk of tech downtime or bugs is always present.
- **Insider Threats (IT):** A rogue administrator or developer with high system access could theoretically abuse that access – e.g., to whitelist a suspicious account, alter logs, or exfiltrate data. This overlaps with Human Factors but is specifically a tech risk when insiders have system privileges.
- **Third-Party Dependencies:** The platform relies on third-party software and services (payment gateways, game providers, cloud hosting perhaps, KYC providers). Inherent risk lies in those third parties – if any one of them has a security breach or failure, it could cascade to affect our platform. For example, if our live chat support provider is

compromised, it might expose some user data; or if the data center is attacked, servers could be compromised.

Overall, considering modern cyber threats, the **Inherent Risk Level for Technology & Cyber is High (4/5)**. The online gaming industry is known to be targeted by cybercriminals and nation-state actors (for either monetary gain or data theft), so we assume a high likelihood of attempts and high impact if successful.

Mitigation Measures for Technology & Cybersecurity:

Trendy Games invests heavily in IT security and resilience to mitigate these risks:

- **Network & Application Security:** The platform infrastructure is secured with **firewalls, intrusion detection/prevention systems (IDS/IPS)**, and continuous network monitoring. All web traffic goes through a web application firewall that filters out malicious requests (SQL injection, XSS, etc.). We regularly conduct **penetration tests** and vulnerability assessments (at least annually, using external cyber security firms) to find and patch any weaknesses in our web application, mobile app, and backend systems. Any critical vulnerabilities are fixed immediately, and patches/updates to software and servers are applied promptly (we maintain updated OS, frameworks, etc., to avoid known exploits).
- **Data Encryption & Protection:** All sensitive data in our databases (customer personal data, passwords, payment card details if stored, etc.) is encrypted at rest using strong encryption algorithms. Data in transit is protected by TLS encryption (HTTPS for all user connections, secure VPN or SSH for internal admin connections). Even if an attacker intercepts traffic or gets a database dump, the data would be of limited use due to encryption and hashing (passwords are salted & hashed). We also tokenize payment card data so we do not store raw card numbers – they are held by our payment processor, reducing our breach impact.
- **Access Controls and Monitoring:** We enforce the principle of **least privilege** for all system accounts. Only authorized IT personnel have access to production environments, and even then, their actions are logged and monitored. Multi-factor authentication (MFA) is required for any administrative access. We segment the environment so that compromise of one subsystem doesn't automatically grant access to others (e.g., game servers separate from database servers, separate from corporate network). All administrative activities (deployments, database queries, etc.) create audit logs. The IT security team reviews logs for any unusual activity.
- **DDoS Protection and Redundancy:** We employ **Distributed Denial of Service (DDoS) protection** services to absorb and mitigate flooding attacks that could otherwise take down the site. This includes working with our hosting providers or specialized security services that can detect and block malicious traffic patterns. Additionally, we have redundancy in place – backup servers and failover processes – to maintain service continuity. Service disruptions are not just a business continuity issue but also a security risk (sometimes used as smokescreen for other intrusions), so quick recovery is important.
- **Cybersecurity Monitoring and Response:** A Security Operations Center (SOC) function is in place (either in-house or outsourced) to continuously monitor for security alerts. If a potential breach or intrusion attempt is detected, an **Incident Response Plan** is triggered. This plan outlines steps to contain the incident, eradicate the threat, recover systems, and

communicate as needed (including to regulators if required by data breach laws). We also have a disaster recovery plan to rebuild systems from backups in a secure state if needed. Regular drills are conducted to ensure the team is prepared for cyber incidents.

- **Integrity of Gaming Software:** All game software (RNGs, live dealer systems) is obtained from licensed vendors and is subject to integrity checks. We maintain checksums or digital signatures of critical software to detect any unauthorized modifications. Additionally, game outcomes and payout percentages are monitored over time to detect any anomalies that could indicate something is off. This helps ensure no tampering has occurred that would, for example, allow certain users to win unusually consistently or otherwise manipulate outcomes.
- **Third-Party Risk Management:** We assess our critical third-party service providers for their security posture. Contracts with providers include clauses on data protection and breach notification. If a provider has an issue (say an outage or breach), we have contingency plans such as alternate providers or manual procedures. For example, if our automated ID verification service went down, we can manually verify documents as a backup. Diversification (using more than one provider where feasible) also mitigates risk of single points of failure.
- **Employee Cyber Hygiene:** All employees, especially those in IT and customer support, receive training on cybersecurity best practices (phishing awareness, safe handling of data, etc.). Since human error (like a staff member clicking a malicious email) can lead to breaches, we cultivate a security-aware culture. Developers follow secure coding practices to minimize introduction of vulnerabilities in our own code.
- **Compliance with Standards:** We align with international standards such as **ISO/IEC 27001** for information security management and follow guidance from relevant frameworks (OWASP for web security, NIST for cyber security). Additionally, if we process payment data directly, we maintain **PCI-DSS compliance** for the handling of card information. These frameworks ensure a systematic approach to tech risk management and are often expected by banks and regulators.

Residual Risk (Technology & Cyber): After applying these comprehensive cybersecurity measures, the **residual technology risk is assessed as Moderate (2/5)**. While we can never completely eliminate cyber risk (the threat landscape evolves constantly and even top companies face incidents), we have reduced the likelihood of a successful breach significantly and limited the potential impact. Importantly, any single cyber incident is unlikely to directly enable money laundering without triggering alarms (for instance, even if one account were hacked, withdrawal attempts would still go through our monitored processes). The remaining risk is mainly the possibility of a novel attack or an unexpected zero-day vulnerability. This residual risk is acceptable and continuously monitored; we also carry cyber insurance as a financial mitigation for this risk. We remain vigilant and regularly update our cyber defenses to keep this risk controlled.

7. Human Factors Risk

Human factors risk covers the **people aspect** – employees, management, and culture – and how that could lead to compliance failures, internal fraud, or facilitation of ML/TF. In any AML program, the effectiveness ultimately hinges on the humans implementing and overseeing it.

Inherent Risk Factors:

- **Human Error:** People can make mistakes. An inherent risk exists that a staff member might inadvertently **fail to follow procedures**, e.g., approving an account without complete documents, missing a red flag in a transaction alert, or mis-configuring a monitoring rule. Given the volume of work (many customers, many alerts), the risk of oversight or fatigue leading to error is present.
- **Insider Malfeasance:** There's a risk that an employee could **collude with criminals** or be corrupted (bribed or extorted) to bypass controls. For example, a staff member in payments could be bribed to approve a large withdrawal without proper KYC, or a compliance analyst could be convinced to clear a suspicious alert falsely. Similarly, a disgruntled employee with IT access could sabotage systems or steal data.
- **Inadequate Training or Resources:** If employees, especially in compliance and fraud teams, are not sufficiently trained or if they are understaffed, they might not effectively identify and manage risks. Inherent risk if the company did not invest in training is that policies exist on paper but aren't executed well. Also, if the compliance culture was not strong ("tone at the top"), staff might de-prioritize AML measures in favor of profits or speed.
- **High Turnover or New Teams:** The online gambling industry can have high staff turnover. New or temporary employees might be less aware of risks or easier to exploit. Continuity risk exists if key personnel leave – e.g., losing an experienced Compliance Officer could temporarily weaken oversight until a replacement is up to speed.
- **Management Decisions:** Inherent risk also stems from management's risk appetite. If management were overly aggressive in player acquisition or revenue growth at the expense of compliance, they might encourage practices that increase risk (e.g., being lenient on VIP due diligence to not scare off big depositors). While at Trendy Games the management is committed to compliance, this category considers the theoretical risk of misaligned incentives.

Considering these points, the **Inherent Risk Level for Human Factors is Moderate (3/5)**. People are a potential vulnerability, but also the strongest control when properly managed. Unlike external factors, we have more direct influence here. The inherent risk is not as high as some external categories because we can implement training and checks; however, human-related failures have occurred in many cases of AML breaches globally (e.g., staff complicity in casinos allowing known high-risk customers to gamble freely). Thus it's a significant area to manage.

Mitigation Measures for Human Factors:

Trendy Games fosters a strong compliance culture and uses internal controls to mitigate human risks:

- **Hiring and Vetting:** We perform **background checks on all new hires**, especially those in sensitive departments (finance, payments, compliance, IT). This includes verifying employment history, criminal record checks where possible, reference checks, and in some cases credit checks (for roles handling money). This helps screen out candidates with red flags, such as a history of fraud or financial trouble (which could make them susceptible to bribery).

- **Training and Awareness:** Comprehensive AML/CFT training is provided to all relevant staff at onboarding and refreshed annually. This training covers regulatory obligations, how to detect and report suspicious behavior, internal policies, and real-world case studies of money laundering in gaming. Specialized training is given to the compliance and fraud teams on using our systems and recognizing patterns. We also train customer support and VIP managers on responsible gambling and AML red flags (since they interact with customers and can observe unusual behavior). Cybersecurity training is given to all staff to reduce risk of phishing or social engineering attacks that could compromise systems. A culture of “if you see something, say something” is promoted, encouraging staff to speak up if they notice anything off.
- **Clear Policies and Procedures:** The company has a detailed AML/CFT policy manual, as well as operational procedures for each department. There are SOPs (Standard Operating Procedures) for KYC processing, for handling escalations, for approving large transactions, etc. These documents guide employees on exactly what to do in various scenarios, reducing reliance on ad-hoc judgment and ensuring consistency. Staff are required to certify they’ve read and understood these policies annually.
- **Segregation of Duties:** We implement **segregation of duties** to ensure no single individual has end-to-end control over critical processes. For example, the person who approves KYC documents is not the same who reviews and approves large withdrawals; financial transactions require dual approval for any manual payouts; system changes in production require at least two people (a developer and a reviewer) to sign off. This reduces the chance of an insider acting alone to misuse the system. It also helps catch errors (one person’s mistake might be caught by the second approver).
- **Dual-Control and Approvals:** Certain high-risk decisions require managerial approval. For instance, raising a VIP customer’s deposit limits beyond policy, or deciding not to file an unusual transaction report that was recommended by an analyst, would need sign-off by the Compliance Officer or senior management. This ensures oversight on decisions that could carry risk, preventing a single employee from ignoring red flags.
- **Whistleblower Mechanism:** We have established a whistleblower policy and mechanism (a confidential reporting channel) for employees to report any unethical or suspicious behavior internally. If, for example, a staff member suspects a colleague is tampering with KYC processes or notices someone behaving unethically, they can report it without fear of retaliation. Reports are investigated by the compliance officer or an independent auditor if needed. This helps surface any internal collusion or misconduct early.
- **Monitoring Employee Actions:** Just as we monitor customer transactions, we also monitor certain employee actions on internal systems. For example, any manual changes to customer data or transaction records are logged and reviewed. If an employee accesses a high number of customer accounts without clear reason, that triggers a review. Also, emails and communications may be subject to IT security monitoring (within legal limits) to ensure no sensitive data is being exfiltrated. These measures can catch or deter insider wrongdoing.
- **Culture and Tone at the Top:** The leadership of Trendy Games has made it clear that **compliance is a priority** even if it sometimes conflicts with short-term revenue. This message is conveyed regularly in company meetings. The company has allocated sufficient budget and headcount for compliance functions relative to its size. We celebrate compliance successes (like successfully passing audits or regulatory inspections) to

reinforce positive behavior. By making compliance part of performance evaluations (for instance, operations staff are partly evaluated on adherence to procedures, not just volume of customers handled), we align incentives so that doing the right thing is rewarded.

- **Periodic Independent Audits:** We bring in external auditors or consultants periodically to review our AML/CFT program and its implementation. They check not just policies, but whether staff are actually following them and whether any gaps exist. Findings are used to improve processes and sometimes to retrain or discipline staff if needed. Knowing that their work might be reviewed externally also keeps employees diligent.

Residual Risk (Human Factors): With these controls, the **residual human factor risk is Low (1/5)**. The combination of good hiring, thorough training, oversight, and a positive compliance culture significantly reduces the likelihood of insider-enabled laundering or major procedural mistakes. Of course, no organization can eliminate human fallibility entirely – the risk that an employee might miss a subtle sign or that a cleverly corrupt actor might attempt to groom an employee is never zero. But we believe our multi-layered approach (including oversight and whistleblowing) makes this risk low and manageable. We continue to invest in our people’s capabilities and ethical standards to maintain this low residual risk.

Customer Risk Assessment (CRA) Methodology

In addition to the broad business-wide risk assessment, Trendy Games B.V. has a **structured Customer Risk Assessment (CRA)** process that evaluates the risk of each individual customer and guides the level of due diligence and monitoring applied to them. This section outlines how customers are risk-scored, the criteria used, and how the company monitors customer risk on an ongoing basis.

CRA Approach Overview: Every customer is assigned a **risk rating** (e.g., Low, Medium, High) upon onboarding and this rating is updated throughout the customer’s lifecycle based on their activity and any new information. The risk rating is derived from a **scoring system** where various risk factors are evaluated and given numeric points or weights. The sum (or a weighted composite) of these points determines the customer’s overall risk score. The higher the score, the higher the risk category of the customer, which in turn dictates the intensity of monitoring and due diligence for that customer.

Key Risk Factors and Scoring Criteria: The following are the primary factors considered in the customer risk scoring model, along with examples of how they are assessed:

- **Geography of Customer (Country Risk):**
 - Customers are assigned a country risk score based on their country of residence (and nationality, if known and different).
 - **Low-Risk Country:** e.g., EU, UK, Canada, Japan – Strong AML regulations and low corruption. *(Score: 1 point)*
 - **Medium-Risk Country:** e.g., some Eastern European, Latin American or Asian countries with moderate AML regimes. *(Score: 3 points)*

- **High-Risk Country:** e.g., countries on FATF increased monitoring list or known for high corruption/drug trade (Russia, Nigeria, Pakistan as examples, if not outright banned). *(Score: 5 points)*
 - Note: If a country is on the prohibited list (very high risk or sanctioned), the customer is simply not accepted at all.
- **Customer Profile and Occupation:**
 - During KYC, if occupation or source of income is gathered (or inferred from documents), certain profiles are riskier.
 - **Politically Exposed Person (PEP):** (current or former senior official, or their family/close associate). *(Automatically High Risk – 5 points)* and triggers EDD.
 - **High Net Worth Individual / VIP with unclear income source:** e.g., someone who deposits very large amounts but has an unclear or cash-based profession. *(High Risk – 4 points)* unless clarified.
 - **Regular Profession (with steady income) or Retiree:** e.g., teacher, engineer, salaried employee of a company. *(Low Risk – 1 point)* provided their gambling spend is in line with income.
 - **Unemployed/Student with significant gambling spend:** Potential mismatch between wealth and gambling. *(High Risk – 4 points)* requiring checks.
 - If occupation is not provided, risk is evaluated via other proxies (like income evidence or by requesting info for big spenders).
- **PEP/Sanctions/Adverse Media Screening Results:**
 - As discussed, if a customer is found to be a **PEP**, they are high risk by default.
 - If a customer is on a **sanctions list**, they are not onboarded at all (account rejected/frozen immediately). *(This is an exclusionary criterion rather than scoring.)*
 - If screening reveals **adverse media** (e.g., news linking the person to financial crime, fraud, etc.), the compliance team will assign a higher risk score or even decide not to onboard depending on severity. For example, a customer named in a money laundering investigation (even if not convicted) would be treated as High risk or refused.
- **Transaction and Betting Activity Levels:** (initially predicted, later actual)
 - **Initial Deposit/Balance Amount:** At onboarding, the customer's intended deposit levels or first deposit amount can signal risk. A very high first deposit (relative to typical players) raises risk.
 - e.g., Initial deposit under €1,000 *(Low risk contribution)*, €1,000-€5,000 *(Medium)*, €5,000+ *(High)* – though this is adjusted if the customer provides justification.
 - **Ongoing Volume of Transactions:** Over time, the total amounts deposited/withdrawn monthly contribute to risk rating.
 - e.g., Monthly turnover < €5k *(Low)*, €5k-€20k *(Med)*, >€20k *(High)*, with increasing scores as volume grows.
 - **Abrupt Changes in Activity:** If a typically small-stakes player suddenly starts moving large amounts, the risk rating is bumped up and a review is done.
- **Product Usage / Behavior:**
 - Some products or betting behaviors can increase risk:

- A customer who primarily uses the site as a “money mule” might deposit and withdraw without much betting – this behavior pattern would flag them as High risk in our system.
 - A customer who engages in **high-risk gambling patterns** (like always betting max amounts, or frequently betting both sides via multiple accounts – if detected) is marked high risk for fraud/abuse.
 - Conversely, a recreational pattern (small bets, consistent play, moderate net spend) might indicate lower risk.
- We incorporate these patterns into a behavior score. For example, an alert from the monitoring system about minimal play would automatically increase that customer’s risk score until resolved.
- **Payment Methods Used:**
 - The type of payment methods a customer uses also factors in:
 - **Using personal bank account or major credit card in their own name:** (*Low risk*) because it’s traceable and tied to KYC’d financial institutions.
 - **Using multiple different credit cards or various e-wallets:** (*Elevated risk*) since it could indicate possible fraud or that the person is trying to obscure money origins.
 - ****Use of any high-risk**
- **Payment Methods Used:**
 - Generally, if a customer sticks to **one verified payment method** (like a bank account or credit card in their own name), it’s viewed as lower risk (*score ~1*), since the funding source is traceable and tied to the customer’s identity.
 - Using **multiple or frequently changing payment methods** increases risk (e.g., someone who alternates between several cards and e-wallets) (*score ~3*), as it could indicate attempts to obscure the money trail or use of third-party funds.
 - Reliance on **high-anonymity methods** (for example, prepaid vouchers bought with cash) would be considered high risk (*score ~5*). In practice, Trendy Games has strict rules against anonymous funding; the mere attempt to use a non-traceable payment method or a payment account not in the player’s name will flag the account for investigation.

Scoring and Classification: Each customer’s risk factors are input into our scoring model. Some factors are weighted more heavily (for instance, being a PEP or in a high-risk country will almost automatically result in a high-risk classification regardless of other factors). The scores correspond to risk levels as follows (illustrative thresholds): **a total score up to 5 = Low Risk, 6-10 = Medium Risk, 11+ = High Risk.** For example, a customer from a low-risk country, with a verified job, modest deposits, and standard play behavior would score low. Conversely, a customer from a high-risk country, who is a PEP and quickly transacts large sums would score high and be treated accordingly.

For clarity, the table below provides examples of criteria at low vs. high risk levels:

Risk Factor	Low Risk Example	High Risk Example
Geography	Resident of a low-risk country (e.g. Canada)	Resident of a high-risk country (listed by FATF)

Risk Factor	Low Risk Example	High Risk Example
Customer Profile	Non-PEP, salaried occupation	Politically Exposed Person (PEP)
Initial Deposit	Small first deposit (e.g. €200)	Very large first deposit (e.g. €20,000)
Monthly Turnover	< €5,000 in bets/deposits	> €20,000 in bets/deposits
Account Behavior	Regular play, consistent patterns	Minimal play, mainly deposits & quick withdrawals
Payment Methods	Single credit card in own name	Multiple cards/e-wallets or prepaid vouchers

Risk-Based Actions and Monitoring: The customer's risk rating dictates the level of due diligence and ongoing monitoring:

- **Low-Risk Customers:** These undergo the standard identity verification and are then mostly monitored through automated systems. No special action is needed beyond baseline controls, though they are still subject to random compliance checks and continuous automated screening.
- **Medium-Risk Customers:** These may face some additional measures – for instance, moderate source of funds queries if their activity grows, and a **periodic review** (e.g., review of their account and documents at least every 1-2 years). Their transaction patterns are watched with slightly lower thresholds for alerts than low-risk customers.
- **High-Risk Customers:** These undergo **Enhanced Due Diligence (EDD)**. This can include requesting detailed source of wealth documentation, verifying the source of funds for each large deposit, and senior management approval to either continue the relationship or allow higher transaction limits. High-risk accounts are reviewed more frequently (at least annually, often every 6 months or even more often if activity is high). They are also subject to more stringent transaction monitoring rules – our systems flag smaller anomalies for high-risk players to ensure early detection of potential issues. All PEPs, for example, are categorized as high-risk and have dedicated oversight.

Ongoing Screening and Monitoring Tools: Trendy Games uses several tools to continually monitor customer risk:

- A real-time sanctions/PEP screening service automatically re-checks the customer database whenever sanctions lists are updated (and at minimum, we run batch re-screening of all customers nightly). This ensures that if a customer becomes a PEP or gets added to a sanctions list after onboarding, we catch it promptly and escalate their risk rating.
- The **transaction monitoring system** described earlier works across all customers, with risk-tiered rules. High-risk customers might have custom rules or lower thresholds (for instance, a €5,000 transaction might trigger for a high-risk customer whereas the threshold is €10,000 for a low-risk one). The system generates risk scores for each customer based on their rolling activity, which feeds into their overall risk profile (dynamic scoring).

- A **case management software** is used by the compliance team to track investigations on customer accounts. All alerts and their resolutions are logged. If a customer has multiple alerts, the system will highlight this trend, potentially prompting an in-depth review or SAR (Suspicious Activity Report) filing.
- **Management Reporting:** We produce internal reports on the risk segmentation of our customer base (e.g., what percentage of customers are high-risk, how many high-risk customers have provided SoW documentation, etc.). This helps ensure our risk profile remains aligned with our expectations and resources – for example, if the number of high-risk customers were to increase rapidly, we would allocate more compliance staff to handle the workload.

In summary, the CRA ensures that each customer is subject to a level of scrutiny proportional to their risk. This dynamic system, combined with robust monitoring tools, allows Trendy Games to detect and respond to potentially illicit behavior on an individual customer level, complementing the broader business-wide controls.

Residual Risk Matrix and Overall Findings

For a concise overview, the following table summarizes the **inherent vs. residual risk** by category, along with key mitigating controls that drive the risk reduction:

Risk Category	Inherent Risk	Residual Risk	Key Mitigations Implemented
Products & Services	High (4/5) – Online gambling inherently high ML risk due to fund turnover and potential misuse.	Moderate (2/5) – Risk reduced by account-based play, KYC on all players, bet monitoring, and game integrity checks.	KYC on registration; monitor betting patterns; bet limits; vetted game software.
Customers	High (4/5) – Global user base may include PEPs, criminals, or high spenders with illicit funds.	Moderate (2/5) – Thorough KYC, PEP/sanctions screening, and risk-based customer due diligence mitigate most risk.	ID verification; PEP/sanctions screening; EDD for high-risk (PEPs, high rollers); ongoing SoF checks.
Delivery Channels	High (4/5) – Non face-to-face digital onboarding and global internet access pose identity fraud and anonymity risks.	Moderate (3/5) – Digital verification tools and strict controls on access (geo-blocking, device monitoring) reduce risk, though remote nature still adds some residual risk.	Advanced eKYC technology; IP/Geo blocking for banned regions; affiliate vetting; device fingerprinting.
Geography	Very High (5/5) – Global reach includes areas of high	Moderate-High (4/5) – Most high-risk	Prohibited countries list (sanctions, FATF high-

Risk Category	Inherent Risk	Residual Risk	Key Mitigations Implemented
	AML risk (if not restricted); risk of sanctioned or high-risk jurisdiction involvement.	jurisdictions are blocked, and country risk scoring is applied, but serving a wide range of countries inherently leaves some elevated exposure.	risk); risk-based country controls; enhanced checks for medium-risk regions.
Transactions	High (4/5) – High volume of deposits/withdrawals via multiple channels; potential for structuring, rapid in-out laundering and payment fraud.	Moderate (2/5) – Comprehensive transaction monitoring, enforced payment matching, and limits significantly lower the likelihood of undetected suspicious transactions.	Automated AML transaction monitoring; deposit/withdrawal limits; same-name withdrawal policy; suspicious transaction reporting (NORUT).
Technology & Cyber	High (4/5) – Attractive target for cyber attacks; a breach or manipulation could facilitate theft or undetected ML.	Moderate (2/5) – Strong cybersecurity framework and continuous monitoring greatly reduce risk of successful attacks or system abuse, though cyber risk persists.	Firewalls/IDS, encryption, regular pen-tests; DDoS protection; secure software development; incident response plan.
Human Factors	Moderate (3/5) – Potential for human error or rogue insider undermining controls.	Low (1/5) – Compliance-oriented culture, training, and oversight minimize the chance of insider failure or collusion.	Staff AML training; background checks; segregation of duties; compliance audits; whistleblower policy.

Overall Residual Risk: Taking into account all categories and their weightings, Trendy Games B.V.’s overall residual risk rating is **Moderate**. This means that while inherent risks in this industry are high, our mitigation measures have successfully lowered the risk to a level considered acceptable by the company and in line with regulatory expectations. No category is left with unmitigated “High” risk; the highest residual rating (Geography at 4/5) is being carefully managed with specific controls and is expected to further decrease as we refine country-level measures under the new CGA regime. The **money laundering and terrorist financing risk** is broadly under control (moderate residual risk), **fraud risk** is contained through strong payment controls and monitoring, and **cybersecurity risk** is actively managed to prevent incidents. All residual risks are within our risk appetite, which has been reviewed and approved by senior management.

Conclusion and Commitments

Trendy Games B.V.'s Business Risk Assessment for FridayBet.com demonstrates a rigorous evaluation of risks and a strong framework of controls aligned with the latest regulatory standards and best practices. Key findings indicate that after mitigation, the company's risk exposure is **moderate and manageable**. Each risk domain – from the nature of our gambling products to the profile of our customers and the technologies we use – has been addressed with targeted risk controls, resulting in substantial risk reduction. This BRA provides assurance to regulators and banking partners that:

- **Robust AML/CFT Measures are in Place:** We have implemented a comprehensive risk-based approach, meeting the obligations of the 2025 Curaçao Gaming Authority regime and relevant AML laws (NORUT and indicator regulations). We are aligned with FATF Recommendations in our policies for customer due diligence, record-keeping, ongoing monitoring, and suspicious activity reporting. Our Customer Risk Assessment model ensures enhanced vigilance over higher-risk clients, and our internal reporting and escalation processes ensure timely action on any red flags.
- **Fraud and Cybersecurity Risks are Managed:** Beyond AML/CFT, we recognize the importance of guarding against fraud and cyber threats. Controls such as payment verification, anti-fraud checks, data encryption, and cybersecurity monitoring are actively protecting the platform and its financial transactions. This dual focus on financial crime and information security preserves the integrity of our operations and protects both the business and its customers from harm.
- **Residual Risk is Acceptable:** The residual risk matrix shows that no uncontrolled high risks remain. The few areas with relatively higher residual risk (e.g., geographic exposure) are under enhanced monitoring and are deemed acceptable given the controls and the nature of our business. In practice, this means the likelihood of Trendy Games being used as a vehicle for significant money laundering or terrorist financing without detection is low. Minor to moderate risks that remain are continuously watched and kept within tolerance.
- **Continuous Improvement:** We are not complacent. This BRA is a **living document** and part of an ongoing risk management cycle. We commit to reviewing and updating the Business Risk Assessment at least **annually**, and sooner if there are major changes in our risk profile – for instance, entering a new market, offering a new product type, or if emerging threats (like a new fraud trend or cyber vulnerability) are identified in the industry. Each review will incorporate any new regulatory guidance from the CGA, findings from internal audits, and evolving best practices in AML/CFT. The effectiveness of our controls will be tested periodically (through internal audits and independent third-party audits as required by regulators or banks) and enhancements will be made as needed.
- **Governance and Oversight:** The Board of Directors and senior management of Trendy Games are engaged in the oversight of risk management. They have reviewed this assessment and endorse the adequacy of the controls in place. Going forward, they will receive regular compliance reports summarizing risk indicators (such as number of suspicious reports filed, training completed, any compliance breaches, etc.) to ensure ongoing governance of the risk landscape. This high-level oversight underscores our commitment to a tone at the top that prioritizes compliance and ethical operation.

In conclusion, Trendy Games B.V. has a strong risk management framework befitting a modern online gaming company under heightened regulatory scrutiny. We acknowledge the inherent risks

of our industry and global footprint, but through a diligent risk-based approach we have implemented robust measures to prevent misuse of our platform for illicit purposes. The residual risk is at a level deemed acceptable by both the company and, we believe, by regulatory and banking standards. We will maintain vigilant operations, continue to invest in compliance and technology, and work closely with the Curaçao Gaming Authority and financial institutions to ensure ongoing trust and compliance. **This Business Risk Assessment will serve as a cornerstone document for internal risk awareness, regulatory compliance, and partnership transparency, reaffirming Trendy Games' commitment to integrity and responsible operation.**

Approved and signed by statutory director Kurason Trust Curacao,
represented by Jonathan Marshal Ruwel Heymans
Date: 7 of April 2025
Signature:

DocuSigned by:

BFFB053659204B9...