

Risk Assessment Policy

Jazz Business Solution B.V.
2025

Table of Contents

Contenido

1 – INTRODUCTION	3
2 – MONEY LAUNDERING	3
2.1 What is Money Laundering?	3
3 – AML RISK ASSESSMENT AND MITIGATION	4
3.1 – General	4
3.2 – Risk Management Strategy	5
Detailed Descriptions	6
4 – IDENTITY VERIFICATION (Tier 1)	6
4.1 KYC POLICY	6
4.2 Preliminary Screening	7
4.3 EDD (Enhanced Due Diligence Procedures)	9
4.4 Politically Exposed Persons Policy	10
5 – SOURCE OF FUNDS (Tier 2)	11
5.1 – General	11
5.2 – Mitigation through Deposit Limits	12
6 – CONTINUOUS MONITORING (Tier 3)	12
6.1 – Suspicious Conduct	13
6.2 – Reports and Reporting	13
7 – DESTINATION CONFIRMATION (Tier 4)	15
Governing Payout Transaction Policy	15
8 - EMPLOYEE DILIGENCE	16
8.1 – Employee Screening	16
8.2 – AML Training	16
8.3 – Third Party Supplier Diligence	16
9 – WIDER ENVIRONMENT	17
9.1 General	17
9.2 – Market Changes	17
10 - CONCLUSION	17

1 – INTRODUCTION

Jazz Business Solutions B.V. operates an online gaming enterprise and is committed to the implementation of robust KYC (Know Your Customer) protocols and operational monitoring/reporting mechanisms to mitigate risks that could negatively impact the organization. **Jazz Business Solutions B.V.** (hereinafter referred to as the “**Company**”) has established the following general principles to reasonably mitigate Anti-Money Laundering (AML) exposure, considering the source and nature of its various business channels and targeted markets:

This Risk Assessment (hereinafter referred to as the “**Policy**”) is designed to identify and address any real or perceived risk of money laundering and terrorism financing posed by the Company's activities as it conducts operations in the online gaming sector.

2 – MONEY LAUNDERING

2.1 What is Money Laundering?

*The Regulations of the GCB for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, have defined **Money Laundering** as:*

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean.

Money Laundering consists of **three phases**:

- **Placement:** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering:** This stage involves converting the proceeds of crime into another form

to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;

- **Integration:** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

3 – AML RISK ASSESSMENT AND MITIGATION

3.1 – General

The Company has implemented necessary and effective measures to reasonably mitigate any money laundering risk associated with its services and various transactional processes:

- The identity of players is verified through appropriate KYC protocols before permitting any payout transactions and whenever possible, considering the nature of the payment method.
- All deposits are received from verified sources associated with the player's identity.
- All payout transactions are verifiably issued only to the account holder.
- Where possible, payout transactions are restricted to the transaction method used for the initial deposit (i.e., funds are paid out only to the card, wallet, or other deposit method from which the deposit was received).
- Cash transactions are prohibited, both as deposit and payout methods.
- Credit is not extended to players under any circumstances other than through bonus programs.
- Inter-account transfers of funds or tokens, poker chips, or any redeemable coupon or credit of any kind are not permitted.
- Player activity is actively monitored daily for suspicious activity that could result in an effective transfer of funds from one player to another, such as "chip dumping."
- All bet or wager transactions are in electronic format, recorded, maintained, and auditable.

3.2 – Risk Management Strategy

Purpose

The Anti-Money Laundering (AML) protocols of the Company are structured around four critical tiers. These tiers, collectively implemented, are designed to reasonably mitigate any potential AML risks associated with the Company's operations.

Tiers of AML Protocols

Tier 1: Identity Verification

- **Objective:** Verify the identity of the account holder.
- **Procedure:** Ensure that the identity verification process is completed as soon as practicable, but strictly before any withdrawal or payout is made. This is to mitigate AML risks by confirming that the account holder's identity is valid.

Tier 2: Source of Funds

- **Objective:** Confirm the legitimacy of the funds deposited.
- **Procedure:** Verify that the funds deposited into the account are from a source that can be confirmed as belonging to the account holder, whenever possible. This process considers the nature of the deposit method to ensure the source of funds is legitimate.

Tier 3: Continuous Monitoring

- **Objective:** Monitor account activity for suspicious behavior.
- **Procedure:** Continuously observe account activities for any potentially suspicious patterns, behaviors, or transactions. Examples include attempted chip dumping or player collusion. This ongoing monitoring helps in identifying and mitigating risks promptly.

Tier 4: Destination Confirmation

- **Objective:** Ensure payouts are made to legitimate destinations.
- **Procedure:** Whenever possible, verify that any payout transactions are directed to a destination that can be confirmed as belonging to the account holder. This step

ensures that the funds are transferred securely to the rightful owner.

Detailed Descriptions

Each tier mentioned above is elaborated in detail in the subsequent sections of this policy document. This ensures a comprehensive understanding and implementation of each step to maintain the integrity of the Company's AML measures.

4 – IDENTITY VERIFICATION (Tier 1)

4.1 KYC POLICY

Know Your Client (KYC) Protocols Policy

Purpose

Effective and closely monitored Know Your Client (KYC) protocols are fundamental to mitigating Anti-Money Laundering (AML) risks. Customer due diligence is an essential process that enables the Company to identify its clients and service providers, and to verify their identities.

Objectives

The objectives of this policy are:

1. **Identity Validation:** To ensure that the identity of each client is verifiable and valid.
2. **Risk Assessment:** To determine whether the validated identity poses a heightened risk of fraud, terrorist financing, or AML activities.

Procedures

1. **Customer Due Diligence (CDD):**
 - **Verification Process:** The Company will conduct thorough due diligence to verify the identity of each client. This involves collecting and examining identity documents and other relevant information to confirm the client's identity.
 - **Risk Assessment:** Upon verifying the identity, the Company will assess the

potential risks associated with the client. This includes evaluating the risk of fraud, terrorist financing, and AML activities.

2. Account Restrictions:

- **Inability to Complete Due Diligence:** If the Company is unable to complete the due diligence process for any reason, the affected account will be disabled. This means the account will be restricted from depositing funds or engaging in any gaming or wagering activities.
- **Implementation of Safeguards:** The Company may implement additional safeguards or procedures as necessary to mitigate risks until due diligence can be completed.

3. Re-enabling Accounts:

- **Verification Confirmation:** Once the client's identity has been verified and deemed valid, the account may be re-enabled.
- **Company Discretion:** The decision to re-enable the account will be at the sole discretion of the Company, ensuring that all AML and KYC requirements are satisfactorily met.

4.2 Preliminary Screening

Customer Account Policy

Account Ownership

1. **Individual Accounts Only:** Customer accounts may only be held in the name of an individual. Corporations, partnerships, trusts, associations, or any other form of legal entity are prohibited from holding accounts.
2. **No Anonymous or Fictitious Accounts:** The Company shall not establish anonymous customer accounts or accounts under names it knows or reasonably suspects to be fictitious.

Account Registration

3. **Mandatory Details:** All individuals are required to provide their details upon sign-up with the Company system. Each individual is permitted to operate only a single account.

Screening Process

4. **Preliminary Screening:** Upon creation of a new account, a preliminary screening, both automated and manual, is conducted to identify potentially linked or other suspect account activities. Third-party service providers such as Iovation significantly aid in the initial screening process. Information captured through these services includes:
 - Device IP (silently gathered) – also known as "device fingerprinting"
 - ISP
 - Geo-location
 - VPN/Proxy usage (silently gathered)
 - Customer information (name, address, date of birth)
 - Email address
 - Password
 - Security questions/answers
 - Acceptance of the Company's Terms and Conditions

Risk Detection

- **Information Utilization:** Capturing this information allows the Company to detect and screen for account holders who may:
 - Create and/or access more than one account
 - Have similar/identical information to other accounts
 - Share the same device used to access accounts
 - Share the same deposit/withdrawal instrument to fund the account
 - Exhibit other suspicious activity such as appearing on a PEPs list
- **Investigation and Risk Mitigation**
- **Automated Alerts and Investigation:** If any screening identifies potential issues, the investigation team is automatically notified to investigate and apply applicable business rules. These business rules may result in various potential risk mitigation steps, including:
 - Closure of the account
 - Escalation to the Fraud team for enhanced diligence

- Limitation of deposit or withdrawal methods
- Imposition of deposit limits
- This policy ensures that all customer accounts are managed with high standards of security and due diligence to mitigate potential risks associated with account activities.

4.3 EDD (Enhanced Due Diligence Procedures)

In situations where customer relationships present heightened AML or fraud risks, the Company will implement enhanced due diligence (EDD) procedures in addition to its regular customer due diligence protocols. The following outlines the steps involved:

1. **Purpose of Enhanced Due Diligence:** Enhanced due diligence is conducted to gather more comprehensive information about a potential customer, their personal and financial background, and the source of their funds. This process includes obtaining additional evidence to verify the customer's identity and ensuring thorough monitoring.
2. **Enhanced Due Diligence Steps:**
 - **Additional Verification Evidence:** Obtaining further evidence to verify the customer's identity.
 - **Particular Aspects Verification:** Verifying specific aspects of the customer's identity.
 - **Source of Funds Verification:** Establishing the source of any funds of the customer.
 - **Frequent Monitoring:** Conducting more frequent and extensive monitoring of the customer's activities.
3. **Tools and Resources:** The Company's fraud department agents utilize a variety of tools and databases provided by suppliers to verify submitted documentation, such as:
 - Driver's Licenses
 - Passports
4. **Accepted Forms of Verification:** The following documents are accepted as forms of verification:

- Marriage Certificate
- Name Change Certificate
- Driver's License
- Passport or other valid government-issued identification

5. Circumstances Requiring Enhanced Due Diligence: Enhanced due diligence is required in the following circumstances:

- **Geographic Risk:** The customer or potential customer is situated in a country or territory that does not apply or insufficiently applies the FATF Recommendations.
- **Politically Exposed Persons (PEPs):** The customer or potential customer is or appears to be a Politically Exposed Person.
- **Heightened Risk Perception:** Any other circumstances the Company reasonably perceives to pose a heightened risk of money laundering.

By adhering to these procedures, the Company aims to mitigate risks associated with AML and fraud, ensuring a secure and compliant operational environment.

4.4 Politically Exposed Persons Policy

A “Politically Exposed Person” (PEP) is an individual who currently holds or previously held a prominent public function in any country. This category encompasses a broad range of individuals, including heads of state, senior members of the judiciary, senior military officers, and immediate family members of such individuals.

Identification and Screening Process

During the initial screening process using third-party providers, the identity risk assessment reliably identifies Politically Exposed Persons. If an account is flagged as a potential match to a PEP list, it will be immediately blocked from making successful deposits pending further escalation and review.

Verification and Documentation

The Compliance Officer/MLRO will generate a report highlighting all new PEP notifications. This officer will then oversee client contact to verify, through documentation or other means, whether the account holder is indeed the “matched” PEP. All documentation and

feedback obtained during this verification process shall be promptly reported to the CEO and Managing Director.

Account Activation and Monitoring

No PEP account may be activated without the explicit authorization of the CEO, Managing Director, and Compliance Officer/MLRO. If reactivation is authorized, it will be subject to additional constraints or enhanced monitoring as mandated by the CEO, Managing Director, and Compliance Officer.

By adhering to these procedures, the Company ensures thorough scrutiny and due diligence in handling accounts associated with Politically Exposed Persons, thereby mitigating potential risks related to money laundering and other illicit activities.

5 – SOURCE OF FUNDS (Tier 2)

5.1 – General

Upon validating the identity of the account holder through either standard or enhanced due diligence, the next step involves ensuring that the source of the funds can be attributed to the validated identity, considering the method of deposit used.

To participate in gaming activities on the Company's platform, customers must first deposit funds into their accounts. The Company offers various deposit options to ensure a seamless customer experience while fulfilling its customer due diligence (CDD) obligations:

a. Credit Cards

Credit cards can only be used if the name on the card matches the name on the account; otherwise, the transaction will be denied. If necessary, the Company may request the player to provide evidence of possession and ownership of the credit card. Transactions require 'Verified By Visa' or 'MasterCard SecureCode' processes and this applies to refillable credit cards as well.

b. Wire Transfers and Direct Deposit Transfers

These methods require the source of funds to be an account or credit facility in the

customer's name, which has been subjected to the KYC processes of the bank or applicable card issuer. These institutions and issuers are under stringent regulatory oversight and AML compliance requirements. Therefore, the Company assumes their KYC processes to be reliable for its operations.

c. Cryptocurrencies

With advancements in monitoring tools such as OXT.me and KYCP.org, cryptocurrency transactions can now be thoroughly analyzed. The Company employs blockchain experts to keep staff updated on the latest developments in the crypto world. These methods and reports assist in detecting shared wallets and other suspicious activities.

5.2 – Mitigation through Deposit Limits

The Company targets casual, recreational bettors or players, operating a "retail" gaming enterprise. As an additional measure to mitigate AML and fraud risks (and to help prevent problem gambling), the Company imposes deposit limits on each available deposit method.

These limits are practical given the nature of the Company's target clientele and serve as a further barrier against money laundering schemes. Even without other safeguards, these limits make significant money laundering efforts logistically impractical.

If a customer reaches their deposit limit, they may contact Customer Service to request a limit increase or a one-time bypass. These requests are reviewed by a supervisor, and the client must submit additional documentation or information to confirm their identity and source of funds.

6 – CONTINUOUS MONITORING (Tier 3)

This section addresses the continuous account monitoring and overview process designed to mitigate the risk of fraudulent conduct or the covert transfer of funds between account holders (e.g., "chip dumping"). The Company is committed to ongoing monitoring of existing customer relationships and accounts, including:

- Reviewing identification data to ensure they remain current and relevant, especially for high-risk registered customers.

- Ensuring the proper recording and storage of identification data to facilitate continuous monitoring of each customer relationship.
- Scrutinizing transactions to ensure they align with the Company's knowledge of the registered customer and their risk profile.

Several daily and weekly reports are generated to assist in detecting and analyzing suspicious activities from individual accounts or groups of accounts.

6.1 – Suspicious Conduct

Suspicious activity cannot be exhaustively defined, but the following instances shall be investigated by the Fraud personnel, potentially constituting suspicious activity under this Policy (many reports will assist in detecting these cases):

- Suspicious play or financial activity by the customer.
- Deposits made by the customer without subsequent wagering over a significant period.
- Apparent “chip dumping,” collusion with other account holders, or other suspect behavior.
- Unusual transaction patterns or activities lacking apparent economic or lawful purposes.
- Attempts to deposit unusually large amounts of money.
- Use of deposit options not in the customer's name.

All suspicious conduct shall be immediately escalated to the Fraud Department and, if necessary, brought to the attention of the Compliance Officer without delay. Failure to report any such case in accordance with the designated escalation process will result in disciplinary action, potentially leading to termination of employment or engagement. The Compliance Officer/MLRO will promptly investigate all reported cases and determine if a reporting requirement is triggered. The findings and recommended remedial actions will be documented and reported to the CEO.

6.2 – Reports and Reporting

The following reports are generated daily or weekly for review and analysis by the appropriate department. Other reports require the Compliance Officer/MLRO or an authorized individual to compile and submit to the Regulator:

a. Significant Payment Reports (STRs)

The Company maintains an automated system to identify all account withdrawals exceeding a specific amount within a rolling 30-day period. Reports are generated within 48 hours of payment and submitted to the relevant Regulator.

b. Suspicious Activity Report (SARs)

The Company implements an automated system to identify accounts that may exhibit suspicious activity, including unusual gaming or transactional behavior. SARs are filed by the Compliance Officer/MLRO or an authorized individual and submitted to the Regulator.

c. Sports Betting Reports

Effective controls monitor and track customer activity in sports betting. Automated controls prevent customers from betting on both sides of an event, using multiple accounts, and participating in betting syndicates. Daily reports help identify potential violations of the Company's Terms and Conditions, leading to appropriate account actions.

d. Casino Gaming Reports

The Company's security and fraud prevention tools track all financial and gaming transactions. Daily reports assist in identifying players exploiting system vulnerabilities, leading to appropriate account actions.

e. Poker Security Reporting and Tools

The Company monitors online poker play to prevent money laundering and ensure fair play using tools such as:

- **Collusion Analyzer:** Flags accounts for potential collusive activity in ring games, based on various gameplay metrics.
- **Bot Detection:** Identifies accounts using third-party software, flagging them for review.
- **Bonus Abuse Reports:** Ensures compliance with bonus terms and detects abuse through referral incentives.

In cases where accounts are flagged for fraud, illicit activity, or other concerns, accounts are disabled and reviewed by the Poker Security, Fraud, and Compliance teams for

appropriate action. If collusion is confirmed, funds are redistributed to affected accounts, and cheaters' accounts are disabled to prevent new account creation.

7 – DESTINATION CONFIRMATION (Tier 4)

The Company's AML/CTF risk mitigation strategy ensures that payout transactions are directed to a destination associated with the verified account holder identity.

Governing Payout Transaction Policy:

- Payouts are processed back to the original transaction vehicle from which the initial deposit was made whenever feasible (e.g., payouts are credited back to the same credit card used for the initial deposit). This practice ensures that both deposits and payouts are linked to the verified individual, significantly reducing AML risk for the organization.

Exceptions and Enhanced Diligence:

- Deviations from this policy are permitted only on an exceptional basis. If the transaction vehicle cannot receive the credit transaction (e.g., MasterCard credit cards, which do not allow crediting), enhanced diligence is required before processing such a payout.
- In such cases, account holders must submit verifying documentation to validate their identity, the initial deposit vehicle, and the payout destination vehicle.

Withdrawal Request Review:

- Prior to processing any withdrawal request by the account holder, the generated funds are reviewed by the appropriate department. This review, applicable across all channels (Sports Betting, Casino, Poker), ensures that funds were legitimately won or generated and that all applicable bonus terms have been respected.

This structured approach to AML/CTF risk management ensures a robust framework for verifying the legitimacy of transactions and protecting the organization from potential risks.

8 - EMPLOYEE DILIGENCE

8.1 – Employee Screening

All employees and staff members of business affiliates or service providers involved in Company tasks undergo comprehensive screening before being hired or appointed. This includes an extensive background check and may involve credit and criminal record checks prior to any offer of employment.

8.2 – AML Training

Specific training protocols will be provided to the following functional groups:

- Frontline Staff (customer service)
- Fraud/Investigation employees
- Financial Services
- Management/Senior Management

The Compliance Officer/MLRO is responsible for ensuring that training modules effectively communicate the requirements of this Policy. Training will cover the identification and reporting of transactions that must be reported to the Compliance Officer/MLRO, and examples of different forms of money laundering schemes that could exploit the Company's business.

Training participants will be assessed to ensure understanding, and AML training sessions will be conducted at least once every twelve months. The Compliance Officer will maintain records of employee attendance and assessment results, which will be retained for a minimum of six years.

8.3 – Third Party Supplier Diligence

The Company acknowledges the potential AML risk posed by contracting or outsourcing certain functions to third parties. Therefore, due diligence is conducted to establish the corporate credentials of potential partners before entering into any service agreements relevant to this Policy.

This diligence includes securing the following documentation:

- Certificate of Incorporation and Memorandum & Articles of Association
- Identification of Directors and, for private companies, shareholders
- Declaration of Beneficial Ownership
- KYC information for signatories

Additionally, third-party suppliers providing payment or processing services must submit a copy of their AML/CFT policies and procedures. These documents will be reviewed by the Compliance Officer/MLRO and the Legal team to ensure the supplier's KYC processes and AML risk management are satisfactory, considering the nature and extent of potential AML risk.

9 – WIDER ENVIRONMENT

9.1 General

The Company operates an online gaming enterprise, offering its services worldwide, with the exception of the United States and Canada. The successful laundering of funds requires obfuscating the origin of illicit funds. In the Company's case, there is no opportunity for anonymous transactions. The origin and ultimate destination of funds (in the case of winnings) are traceable to a financial instrument in the customer's name, presenting a significant obstacle for money launderers or terrorist financiers.

9.2 – Market Changes

The Company provides customers with the means to bet on sports, play poker, and engage in casino gaming. The Company will comply with any changes and updates mandated by various jurisdictions. It will consult with the Legal department to implement any necessary measures required to uphold these regulations.

10 - CONCLUSION

This Policy ensures that funds are transferred only to the original financial instrument in the name of the account holder used to fund the account. When this option is unavailable, funds are disbursed via a method that can only be cashed by the named account holder.

Positive verification of the customer is conducted prior to accepting a deposit and always

prior to initiating a withdrawal. Consequently, the process of deposits and withdrawals presents minimal opportunities for customers to launder funds.

Jazz Business Solution B.V.'s operations are intended for recreational gamblers, not for professional gamblers. While the potential for money laundering exists, it is adequately monitored and considered low risk. All transactions are logged, suspicious activities are investigated, and all customers, regardless of deposit amounts, are verified.