



KKPOKER AML & CFT Policy

Company Policy

TABLE OF CONTENTS



1. Definition for Money Laundering and Terrorist Financing
2. Regular Reviews
3. MLRO and AML/CFT Compliance Officer Duties
4. SAR / Reporting to the Financial Intelligence Unit (FIU)
5. ML enquiries from Curacao Authorities
6. Sanctions
7. Reporting Unusual Transactions
8. Monitoring
9. Training
10. Risk Assessments
11. Record Retention
12. Fictitious, Anonymous and Numbered Accounts
13. Payment of Online Gambling Winnings
14. AML Programme Testing
15. Crypto Payments
16. Payment and Withdrawal Methods
17. Corporate Affiliates and Club Owners
18. Staff Recruitment
19. GCB External Audit

It is the policy of KKPoker to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Curacao AML and CFT Regulations 2024 and its implementing regulations.

1. Definition for Money Laundering and Terrorist Financing

Money laundering (ML) is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the criminal property can lose its criminal identity and appear legitimate, meaning that criminals can benefit from their crimes without the fear of being caught by tracing their money or assets back to a crime. Illegal arms sales, smuggling, and the activities of organised crime, including for example, drug trafficking and prostitution, can generate huge profits.

Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through ML. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds or assets to a place where they are less likely to attract attention.

Placement: Where the proceeds of crime are placed into the financial system.

Layering: Where funds are converted from one form to another, e.g., moved between various accounts and/or jurisdictions to disguise the audit trail and the illegitimate source of the funds.

Integration: Where funds that now appear legitimate re-enter the economy for what would appear to be normal business or personal transactions.

In general terms, financing of terrorism (FT) is the financial support, in any form, of terrorism or those who encourage, plan, or engage in terrorism. FT differs from ML in that the source of funds can either be legitimate, such as an individual's salary, or illegitimate, often the proceeds of crimes such as selling pirate DVDs, fraud, or drug trafficking.

Usually, the focus of scrutiny for potential terrorist financing activity will be the end beneficiary and intended use of the money or assets. A terrorist financier may only need to disguise the origin of the property if it was generated from criminal activity, but in the vast majority of cases, they will seek to disguise the intended use, i.e., the act of terrorism.

Terrorist financing often involves a complex series of transactions, generally considered as representing three separate phases.

Collection: Funds are often acquired through seeking donations, carrying out criminal acts or diverting funds from genuine charities.

Transmission: Where funds are pooled and transferred to a terrorist or terrorist group.

Use: Where the funds are used to finance terrorist acts, training, propaganda etc.

ML/FT can have serious negative consequences for the economy, national security, and society in general. Some of these consequences may include:

- Reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;
- Attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;
- Damaging the legitimate private sector who may be unable to compete against front companies;

- Weakening of financial institutions who may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc.;
- Economic distortion and instability;
- Increasing tax rates due to the loss of tax revenues following tax evasion; or
- Increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

The Company's approach is based upon the following:

- The National Ordinance on Identification of Clients When Rendering Services 2017
- The National Ordinance on the Reporting of Unusual Transactions 2017
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions 2015
- Sanctions National Ordinance 2014
- Kingdom Sanction Act 2016
- National Decree entering into force of Kingdom Sanction Law 2017

Together, these are referred to as the 'Codes' in relation to the detection and prevention of money laundering and terrorist financing.

2. Regular Reviews

A regular review will be carried out to ensure policies and procedures are up to date with the Curacao Gambling codes as and when it is updated.

At any such time as we receive notice that an authorized agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will at the time determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any authorized agency and designated as such.

We will continue to review the codes and all directives issued to comply with Curacao rules prohibiting transactions with certain foreign countries or their nationals.

3. MLRO and AML/CFT Compliance Officer Duties

KKPoker has appointed Ms Lee Ho Yin as the MLRO and AML/CFT Compliance Officer. The

MLRO is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the Company to all external agencies and any other third-party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the Company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.

- Undertaking the internal review of all suspicions and determining whether such suspicions have substance and require disclosure to the FIU.
- All contact between the Company and the Authorities in respect of routine reports to law enforcement in respect of any specific investigations.
- Establishing the suspicious reporting process and ensuring that this process is understood by all staff.
- Maintenance of the register of internal and external disclosures and register of money laundering and financing of terrorism enquiries.

The AML/CFT Compliance Officer is responsible for:

- Establishing, recording, maintaining and operating appropriate procedures and controls for monitoring and testing compliance with the AML/CFT legislation.
- Adopt policies which manage the risks identified by the Company's business risk assessment, monitor the performance of these policies and address any deficiencies identified.
- Submission of a report, on at least an annual basis, to the Company's senior management that describes:
 - Any new developments within the industry in relation to AML/CFT including updates to any legislation or regulatory guidance.
 - Any updates to the Company's internal AML/CFT procedures and policies.
 - Any activities relating to compliance with the Curacao AML and CFT Regulations 2024 that have been undertaken by the Company during the period covered by the report.

As Lee Ho Yin has taken on both these roles, he will be responsible for all of the above.

The firm has also appointed Lee Ho Yin as the AML Officer with full responsibility for the firm's AML program. The MLRO and the AML officer have working knowledge of the Curacao AML and CFT Regulations 2024, its regulations and are qualified by previous experience, knowledge, and training.

The duties of the AML officer will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees as well as client profiling and transactional monitoring.

4. SAR/Reporting to the Financial Intelligence Unit (FIU)

An external Suspicious Activity Report (SAR) is a report made to the Financial Intelligence Unit (FIU) informing it that certain activity (usually, but not always, that of a customer or client) causes knowledge or suspicion of money laundering, or belief or suspicion of terrorist financing. This report is made via Themis, the reporting tool for the FIU. Themis requires the MLRO to complete several fields. Completing all the relevant fields in detail will result in a quality SAR, which will streamline the process for both the FIU and the MLRO.

Prior to this being submitted, an internal SAR must be raised by the staff member holding the suspicion to the MLRO. Suspicions must be reported to the MLRO or DMLRO as soon as reasonably practical using the form at the end of this document (Appendix A). The form must be sent to the MLRO via email (crystal.lee@icmtech.com). Include as much detail as possible in the form in addition to

any supporting documents (see below) as this will help the MLRO determine as to whether an external SAR should be made or not.

The form is also available on request from the MLRO or DMLRO. The case may be discussed initially with the MLRO or DMLRO, but a telephone discussion is not a substitute for formal notification using the appropriate form.

It is important that the form is used as this properly documents the report itself and ensures that all relevant information is included. For this reason, it is important that all parts of the form are completed.

Receipt of the report will be acknowledged by the MLRO or DMLRO. It is necessary for the person making the report to include their name on it. Once an initial report has been submitted the person should continue to submit reports where further suspicious activity takes place, or if there are developments in respect of the matter originally reported.

Supporting information must also accompany the form, such as KYC documents, bank statements, transaction records, client correspondence and copies of relevant media articles.

Sufficient suspicion to raise a SAR is when a person suspects, or has reasonable grounds for suspecting, that another person is engaged in money laundering when he or she recognises that this is a possibility which is not over imaginative or unrealistic.

There may be an aspect of a transaction or activity that is at odds with normal expectations and therefore raises suspicion, whether through inference, sight of documents, clients' comments, or professional insight and experience. Typically, suspicion will arise when something unusual is identified and subsequent research or checking confirms that there are abnormal or contradictory factors. Definite knowledge or evidence of facts is not required for suspicion (or reasonable grounds for suspicion) to arise.

Where a suspicion is reported in respect of a transaction that has not taken place or an activity that has not commenced this fact should be made clear to the MLRO or DMLRO. If the person submitting the report is involved with the transaction or activity, they should not do anything further until advised that they can do so by the MLRO or DMLRO.

The MLRO and DMLRO in conjunction with the Directors will manage the process of ensuring that the transaction may proceed, including obtaining FIU clearance if appropriate.

The company will file a SAR with the FIU for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving movement of funds (either individually or in the aggregate) where we know, suspect, or have reason to suspect:

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade the Curacao law or regulation or to avoid any transaction reporting requirement under Curacao law or regulation;
- the transaction is designed, whether through structuring or otherwise, to evade any requirements of the Curacao Gambling regulations;
- the transaction involves the use of the firm to facilitate criminal activity.

The company will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that FIU in cases where a SAR we have filed may require immediate attention by the FIU. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

If the MLRO is of the view that there are not reasonable grounds for knowing or suspecting that the activity is related to money laundering or terrorist financing, but the MLRO believes that it would assist the FIU in the exercise of any of its functions, the MLRO may make a disclosure to the FIU for information only purposes.

When the company reports suspicious transactions by completing a SAR, we will collect and maintain supporting documentation as required by the FIU regulations. We will file a SAR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

The company will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR, unless otherwise directed from an appropriate authority. We will identify and maintain supporting documentation and make such information available to FIU, any other appropriate law enforcement agencies.

The company will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the FIU and thereafter shall be undertaken in conjunction with the relevant Curacao authorities and in accordance with Curacao custom and practice to avoid any risk of the Company committing a tipping-off offence.

Tipping off is an offence under the Curacao AML and CFT Regulations 2024 . It occurs when a representative of the Company makes a customer aware that they are under investigation due to a suspicion of money laundering or terrorist financing, and in doing so prejudices the investigation.

It is therefore extremely important for all customer facing staff to avoid communicating this information to a customer under investigation. Please note however, that requests for due diligence items from staff to the customer will not necessarily constitute tipping-off. However, if you have reasonable grounds to believe that requesting due diligence, particularly EDD, will tip off the customer, do not proceed with this action and inform your senior manager or the MLRO who will advise on the next steps.

5. ML Enquiries from Curacao Authorities

The MLRO will respond to any Financial Investigation Unit (FIU) request concerning accounts and transactions by advising the AML officer to immediately search our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organisation named in the request.

All requests will be recorded in the ML request from authorities register. We will not disclose the fact that the FIU has requested or obtained information from us, except to the extent necessary to comply with the information request.

We will employ strict procedures both to ensure that only relevant information is shared and to protect

the security and confidentiality of this information, by segregating it from the firm's other records.

The company will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

6. Sanctions

A review of the Sanctions/SDN list provided by the Curacao government will be regularly checked and reviewed.

International sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries, or interests. They may be aimed at certain people and targets in a particular country or territory, or some organisation or element within them. There are also sanctions that target those persons and organisations involved in terrorism, including Al Qaida.

The Curacao Government's policy with regard to financial sanctions is to maintain the lists of those affected.

To help the government fight the funding of terrorism and money laundering activities, Curacao law requires all institutions to obtain, verify, and record information that identifies each person who opens an account.

Before opening an account, and on an ongoing basis, the AML Department will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes.

7. Reporting Unusual Transactions

An unusual transaction is a transaction inconsistent with the player's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the player. The purpose of collecting player information is to provide us with documentation to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship.

Based on the NORUT legislation, objective and subjective indicators have been established by means of which we must assess whether a customer's transaction qualifies as an unusual transaction. Management will provide staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All these unusual transactions will be reported to the compliance officer in the format approved by management. All additional documents available, such as copies of identification documents and other records will also be submitted as supplements. The compliance officer will keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by us, the reasons shall be adequately documented and signed off by the compliance officer and/or management. In order to implement FATF

recommendation 11, we will pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

The following transactions or intended transactions are deemed unusual:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. Transactions in the amount of NAF. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means.

This includes but is not limited to:

- 1. A cashless transaction in the amount of NAF. 5,000 or more.

A cashless transaction is a transfer from our bank account to a local or international bank account, at the request of the client.

- 2. Accepting or releasing a deposit in the amount of NAF. 5,000 or more at the request of the client;

- 3. A cash out in the amount of NAF. 5,000 or more;

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAF. 5,000 or more and is considered per gaming day.

- d. Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Reporting of unusual transactions

By virtue of article 11 of the NORUT, we will report unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, we have procedures for internal and external reporting of unusual transactions in place.

All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, will be reported internally, without any delay. Also supporting documents will be submitted as part of the reporting.

The documentation of unusual transactions

The compliance officer will prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. We shall report to the FIU the details of these transactions by means of the goAML reporting portal.

8. Monitoring

KKpoker maintains an ongoing monitoring system of transaction monitoring, relating to deposits, withdrawals and gameplay. KKPoker staff monitor these transactions on a daily basis, looking for any potential suspicious or unusual activity.

It is recognised that a significant change to the normal operation of an account could be a sign of suspicious or unusual activity. A change may be:

- Unusually large deposits based on past deposit history
- Unusual patterns in betting activity
- Large deposits followed by large withdrawals combined with minimal betting transactions
- Multiple changes to deposit and withdrawal methods
- Unusual gameplay on the poker tables

A player that reaches a risk level of KYC3 or above will have all of their transactions reviewed to determine whether any of their activities appear unusual. Additionally, any existing KYC already held by the company will also be reviewed to ensure that it is still in date and relevant to the player's personal details. Players of a risk level of KYC3 and above are also added to ongoing monitoring list on KYC6 where they are continuously screened against new updated information.

If during the course of daily monitoring it is noted that a player's profile has altered in a way that would alter their risk level an immediate review would be undertaken to ensure that all due diligence criteria for the new risk level is met. Should any further documents or information be required the participant will be contacted with a request to provide such within a timely manner.

Transaction reports will be reviewed on a monthly basis, overseen by the MLRO. Particular scrutiny will be applied to medium and high-risk customers. Where the activity is deemed to be unusual, an investigation into the customer may begin which may include asking the customer for their rationale for carrying out the activity or further information or evidence of the source of funds or source of wealth. Transaction monitoring for transfer affiliates will be conducted as per KKPoker's Transfer Affiliate Policy.

As part of these transaction reviews, other factors rising from outcomes of business, technology and customer risk assessments will also be considered.

Changes made to a customer's identity and personal information will be reported on to the Company's management. The evidence of identity previously provided by the participant will be reviewed and steps taken to renew and update that information considering the reported changes to the participant's identity. In certain cases, this may mean that the account is suspended pending receipt of new identity and address verification.

Of course, there are many acceptable reasons as to why a person's identity may change, for example getting married and changing their surname to that of their spouse. However, differing identity details may be due to having previously provided false details due to an attempt at some form of criminality.

In such circumstances, the verification procedures established in this document shall be followed in addition as to the customer providing reasoning for the change in details.

Should a customer's risk level increase (e.g. from low risk to medium risk) and due diligence documents are already held on the customer, consideration must be made whether further documents must be submitted. The previously supplied documents must be reviewed to ensure that they are not expired, in such circumstances up to date documents must be requested.

CDD/EDD held will be reviewed each time a player triggers a risk related flag, such as reaching a transaction threshold as per the company's KYC rules, or when they change address or name. EDD held on high risk players, transfer affiliates and business participants will be reviewed on an annual basis.

In the event that satisfactory confirmation of the information as to the identity of the participant or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further betting or transactional activity allowed, and consideration be given to the lodging of a suspicious transaction report.

The MLRO will conduct periodic sample checking of all of the above monitoring procedures to ensure full compliance is being met and to identify any potential weaknesses and risks within the procedures.

9. Training

We will develop ongoing employee training under the leadership of the AML Officer and senior management. All new staff will receive AML/CFT training and ongoing training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum:

- how to identify red flags and signs of money laundering that arise during the course of the employees' duties;
- what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs);
- what employees' roles are in the firm's compliance efforts and how to perform them;
- the firm's record retention policy; and
- the disciplinary consequences (including civil and criminal penalties) for non-compliance with the FIU.
- Awareness of the provisions of the AML/CFT code and any personal obligations thereof including offences and any revocations.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We are currently reviewing available training resources in the Curacao and online.

To demonstrate compliance, we will keep thorough records documenting the individuals who have undergone training, the training dates, and the topics covered. Specifically, records will include:

- Comprehensive details of the training program content;
- The names of employees who completed the training;
- The dates on which training sessions were conducted;
- Outcomes of any assessments used to evaluate employees' understanding of anti-money laundering and counter-terrorist financing obligations; and
- An established plan for ongoing training to ensure continued staff competence.

We will review our operations to see if certain employees require specialised additional training. Our written procedures will be updated to reflect any such changes.

10. Risk Assessments

Customer Risk Assessment and Customer Acceptance Policy

The company adopts a risk-based approach to manage risks related to money laundering, terrorist financing, and proliferation financing associated with its customers. To effectively mitigate these risks, the following Customer Risk Assessment (CRA) and Customer Acceptance Policy (CAP) are in place.

Customer Risk Assessment (CRA)

Customers are risk assessed immediately upon registering an account on the platform and continually on an ongoing basis as they interact with the platform through activities such as depositing, withdrawing, and playing games. Risk ratings at levels KYC2 and above are recorded in the customer's back-office profile. Customers with no noted risk level are deemed to be at risk level KYC1. Any changes in a customer's circumstances—either increasing or decreasing their risk level—as well as any profile reviews, will be documented in the customer's back-office.

The CRA process is conducted either before an occasional transaction or at the establishment of the business relationship and is continuously updated to reflect changes in customer behavior or new information. It assesses the specific risks the company faces when providing services to customers, including economic activity and source of wealth.

Relevant risk factors considered in the assessment include, but are not limited to:

- Customer residential jurisdiction
- Politically Exposed Person (PEP) or sanctions status
- Whether the interaction occurred during ongoing customer relationships, formation, or occasional transactions
- Risk indicators based on high-risk jurisdiction lists, including those published by the government of Curacao
- Any warnings or adverse media related to AML/CFT matters involving the customer

Other risk indicators such as multiple or irregular income sources, high or disproportionate spending, use of third parties, multiple accounts to obscure gambling activity, unknown customers redeeming large chip amounts, and engagement with junket operators are also taken into account.

Customer Acceptance Policy (CAP)

The CAP sets forth criteria for customer acceptance or rejection based on assessed risks of money laundering, terrorist financing, and proliferation financing. It includes:

- Profiles and characteristics of customers likely to pose higher than average risk
- Risk indicators classifying customers as low, medium, or high risk
- The corresponding level of Customer Due Diligence (CDD), including enhanced due diligence for higher-risk customers such as PEPs and sanctioned persons
- Requirements for ongoing monitoring commensurate with the customer's risk level
- Circumstances under which service provision may be declined, such as when risks cannot be sufficiently mitigated

This integrated approach ensures the company maintains robust defenses against illicit financial activities while meeting regulatory obligations.

Please see the "Client Due Diligence" section of this document for full details of client risk assessments.

Reviews of all assessments will be carried out according to the risk factors as determined by the company taking into account the assessment sections and ratings.

Business Risk Assessment

Risk assessments on the company's business will be conducted on an annual basis and will include the following factors:

- the nature, scale, and complexity of the operator's activities
- any relevant findings of the most recent National Risk Assessment relating to the Island
- the products and services provided by the operator
- the manner in which the products and services are provided including whether the operator meets its customers
- the involvement of any third parties for elements of the customer due diligence process;
- Information for the Technology Risk Assessment and Client Risk Assessment

Technology Risk Assessment

The Company recognises the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The Directors retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the company has engaged with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

Any developments to the Company's software or new products introduced by a business partner that poses a potential increased risk of ML/FT will require a technology risk assessment. This must be conducted prior to the launch of the update/product, regularly reviewed and if necessary, amended to be kept up to date.

The technology risk assessment must take consideration of the following:

- technology currently used by the Company to comply with AML/CFT legislation.
- any risks identified in previous business risk assessments
- the products and services provided by the Company
- the way the products and services are provided by the Company or Business Partner with consideration given to delivery methods
- communication channels and payment mechanisms
- digital information and document storage
- electronic verification of documents
- data and transaction screening systems

11. Record Retention

As required by the Curacao AML and CFT Regulations 2024, records will be kept by the company including but not limited to - identification information, account files, business correspondence records and the results of any analysis undertaken for:

The policies and procedures for the company

- Client due diligence and Enhanced due diligence analysis and results
- transactions carried out in the course of gambling business
- Internal and External disclosures
- ML/TF Enquiries from the FIU/ Curacao authorities
- Employee training
- SARs
- Risk Assessments
- Reporting procedures
- all such other records as are sufficient to permit reconstruction of individual transactions and compliance

Format and retrieval of records

In the case of any records that are required to be established and maintained by this Code, we will ensure we are able to retrieve the records without undue delay and if kept outside of the Curacao, ensure they are available within 7 days.

Records associated with a customer (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the partner's account or the date of the last transaction.

Records associated with the register of internal and external disclosures and the register of money laundering and financing of terrorism enquiries will be maintained for a period of 5 years following the finalisation of the relationship with the related parties or for the period as advised by the FIU or any other relevant authority.

In the event of the Company becoming de-licensed from the GCB, KKPoker will maintain the above record retention policies, ensuring that any data is still accessible to the relevant authorities within the stated time frames upon their request.

In the course of or in preparation for an examination, and upon request by the GCB, the company will ensure the following documents and records are promptly available:

- The approved written AML Compliance Program addressing money laundering, terrorist financing, and proliferation financing;
- Customer Risk Assessment documentation;
- The Customer Acceptance Policy;
- Documentation of the company's Business Risk assessment;
- Identification of each Compliance Officer responsible for overseeing the company's AML and CTF policies, along with their assigned job descriptions;
- Records of reported unusual transactions;
- Documentation of unusual transactions that require further investigation;
- Records pertaining to frozen accounts;

- Training schedules provided to personnel on money laundering, terrorist financing, and proliferation financing;
- Internal audit or external auditor assessment reports on the effectiveness of the AML, CTF, and proliferation financing policies and procedures;

Complete customer files, including customer risk assessments, Customer Due Diligence (CDD), customer acceptance, and transaction details.

12. Fictitious, Anonymous and Numbered Accounts

The company will not set up or maintain an anonymous account, a numbered account, or an account that we have grounds to believe is fictitious for any new or existing customer.

While it is possible for users to setup duplicate or fictitious accounts, there are stringent KYC procedures that are followed by the various teams to detect and process such accounts.

The Customer Services Team, Fraud and Payments Team and the AML Team perform their relevant checks at registration, deposit, withdrawal, transfers and user monitoring. Any payments over USD 5000.00 are also automatically flagged for Fraud & Payments to review.

At each stage of the checks, notes are added to the user account to record any findings or decisions. The user accounts are checked for fictitious, duplicate, related and syndicate accounts using the details and documentation provided by the user such as name, date of birth, identity document and proof of address as well as the user login details.

- Name – duplicate, previous closed account, or mismatch with a confirmed valid identity document
- Date of Birth – duplicate or mismatch with identity document, confirmation the user is of a legal age (18+)
- Home address – duplicate, match to other user or mismatch with proof of address provided
- Email address - duplicate
- Device – duplicate
- Matching of the IP to the address provided as confirmation and not from a restricted country

Depending on various factors such as club membership, account balance, activity, or age of the user/user account, either the original or new account will be restricted as per the handling process. Multiple duplicate accounts will result in a permanent ban of the extra account(s).

Users will be contacted regarding incorrect information for an explanation and if established to be a legitimate mistake, will be advised to re-register or correct the user information manually, if the user activity or user account is assessed as low risk.

If the user is found to be high risk or there is suspicious or unusual activity, the account will be frozen and a SAR will be raised.

Any documentation or information found to be invalid or falsified will have the account deactivated, no further activity will be allowed, and the Management team will be informed. Any user account that has been reported will have a note added with the description of the findings and the decision thereof.

13. Payment of Online Gambling Winnings

Any winnings due to a customer will be paid only to:

- A card account or other financial facility from which a deposit has previously been made by the customer and which the operator is satisfied stills belongs exclusively to the customer;
- A card account or other financial facility that the operator is satisfied will result in the customer exclusively receiving the withdrawal

As in accordance with the relevant Curacao laws and regulations.

14. AML Programme Testing

The testing of our AML programme will be monitored and tested at least annually (on a calendar year basis) by an adequately resourced internal audit department or outside party that is independent. The audit will be performed by people not involved with the company's AML compliance staff. To ensure that the audit findings and conclusions are reliable, those performing the audit will have at least two years of experience in AML/CFT compliance along with a bachelor's degree and a relevant AML certification.

The tests shall include:

- An evaluation of the institution's anti-money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

After we have completed the testing, The Operations Manager will report findings to senior management [or to an internal audit committee]. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

Employees will promptly report any potential violations of the firm's AML compliance program to the AML officer, unless the violations implicate the AML officer, in which case the employee shall report to (Head of Compliance). Such reports will be confidential, and the employee will suffer no retaliation for making them.

15. Crypto Payments

An alert system is in place for the Payments team for the processing of crypto payments alerts for new and repeat deposits over USD 2,000.00 within 30 days, and ad hoc checks can occur on deposit, withdrawal, and transfer. Once the alert is received, manual checks are completed on a transaction monitoring level by the Payments team.

The customer account will be assessed which will include checks for:

- Registration date
- The user KYC and status thereof
- duplicate accounts
- multiple deposits
- withdrawal methods
- Player patterns

Once the assessment is completed this will then be sent for management review and either approved or declined and if required a SAR will be raised.

Crypto currency providers such as Cryptopay provide an additional layer of scrutiny via their own AML/KYC policies when users create an account with these providers.

Crypto currency providers also use scoring techniques such as the Bitscore platform which is available to provide information on a cryptocurrency source. The platform's algorithm returns a risk score after evaluating the source of the funds. The information can include if at any time in the past the monitored address has ever sent funds to high-risk parties. These include dark markets, hacking sites or money-laundering services. Bitscore can also examine several generations of transactions in both directions (receiving and sending) and applies a weighting function that determines the amount of questionable cryptocurrency flowing through the studied transactions.

The AML team monitors crypto payments on a player level during user activity and profile monitoring. This includes variances in crypto payment method, amounts and forward on activity.

The management team is to be notified of any rejected payments and suspicious activity will be provided in a SAR to the MLRO as per section 4. SAR/Reporting to the Financial Intelligence Unit (FIU).

16. Payment and Withdrawal Methods

User accounts are allowed one unique payment method in the system with 3 credit/debit cards and 1 of each e-wallet option available. Once a successful deposit has been made then the system prevents this unique deposit/withdrawal method from being used on any other account, and 3rd party payments are not accepted. Withdrawal requests will be processed only to the account that was used for deposits where possible by the user. If no deposits have been made, evidence of ownership of the account will be required.

At any time there is a variance recorded in the deposit or withdrawal method, or if usage of 3rd party payments is detected, the user account will undergo full due diligence and evidence of account ownership will be required.

To combat the risk of parent/child or wallet/card abuse, additional monitoring and reporting is in place by the Fraud and Payments Team to detect and assist in preventing these transactions.

The user payment method and amounts are monitored by the Fraud and Payments team on a

transactional level and by the AML team on an individual user level. This monitoring includes the user KYC status, any previous recorded activity, an increase in volume and player patterns.

The management team is to be notified of any rejected deposits or withdrawals and suspicious activity will be provided in a SAR to the MLRO as per section 4. SAR/Reporting to the Financial Intelligence Unit (FIU).

17. Corporate Affiliates and Club Owners

Prior to onboarding a corporate affiliate, its company information is collected and verified via local company registration. Management sign-off by the Director is required, and then an affiliate marketing agreement is to be signed by both parties.

A UID is created by us and delegated to the corporate affiliate. The KYC information of such UID is manually set by the Customer Services Team with a description added to the back-office notes section.

Specific settings are allocated to the corporate affiliate UIDs to ensure no table play is allowed and they do not use the withdrawal function. Any balance that is to be paid out to the corporate affiliates will be settled by the Director as set out in each affiliate marketing agreement.

Club owners' UIDs are assigned as per normal users with the same KYC requirements to be completed.

Comprehensive client due diligence and monitoring processes are completed for all users, whether individual users, corporate affiliates, or club owners. This is covered via registration, user activity, transactional and profile monitoring by the Customer Services Team, Fraud and Payments Team and the AML Team.

18. Staff Recruitment

It is important that we take appropriate steps to ensure the integrity of new staff. Such steps should be risk based, with the extent of the effort proportional to the role of the employee and the money laundering threat inherent in the role they are being recruited for.

The following staff screening procedures are operated by the Company:

- For all new staff at least one reference will be taken up. References will be obtained by obtaining the permission of the prospective employee to write direct to the referee. References supplied by the prospective employee and references addressed 'to whom it may concern' will not be accepted unless they can be confirmed directly with the referee.
- Copies of relevant qualifications will be confirmed by requesting sight of certificates, copies of which will be retained on the employees file.
- Curriculum Vitae (CV) will be obtained from all prospective employees. The employment history included on the CV will be tested by taking a reference from a previous employer. This should usually be the most recent employer.
- Request details of any regulatory action or criminal convictions taken against the individual (or the absence of such action) and verify where possible.

All staff will be required to conduct AML/CFT training in addition to "KKPoker Training" which will

familiarise staff members with the product that KKPoker offers.

19. GCB External Audit

We shall comply with all GCB requests in relation to external independent audits of our company and procedures accordingly as necessary.

20. Senior Management Oversight and Board Approval

The Board of Directors is committed to ensuring effective governance of the company's AML program. To this end, the following oversight and approval processes are established:

1. **Board Approval**
This AML Policy shall at all times be formally reviewed and approved by the Board of Directors. Approval shall be documented in the minutes of the Board meeting where the policy is considered.
2. **Periodic Review and Oversight**
The Board of Directors shall conduct periodic reviews of the AML policy, at least annually, to assess its adequacy, effectiveness, and compliance with applicable laws and regulations. Any amendments or updates to the policy shall require further Board approval.
3. **Senior Management Responsibility**
Senior management is responsible for the implementation, monitoring, and enforcement of the AML policy. Senior management shall regularly report to the Board on AML matters, including compliance status, risks identified, and any issues or incidents related to money laundering and terrorist financing.
4. **Documentation and Reporting**
All Board approvals, reviews, and senior management reports concerning AML policies and controls shall be documented and retained as part of the company's governance records. This governance framework ensures that the AML program at this company is subject to appropriate senior-level scrutiny, accountability, and continuous improvement.

Referenced documentation

- The National Ordinance on Identification of Clients When Rendering Services 2017
- The National Ordinance on the Reporting of Unusual Transactions 2017
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions 2015
- Sanctions National Ordinance 2014
- Kingdom Sanction Act 2016
- National Decree entering into force of Kingdom Sanction Law 2017



(SMES) Solutions for Managment and Employment Support N.V.

Managing Director

12.11.2025

Version Control

Name	Description
Document Name	AML/CFT Manual
Author	Lee Ho Yin
Updated By	Lee Ho Yin
Authorised By	Board of Directors
Distribution Date	1 st September 2025

Typ hier uw tekst

Appendix A: SAR Form

Report prepared by:	
Business partner (if relevant)	
Customer Name	
Account ID	
Customer Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	
Reason for suspicion	
<i>To include:</i> <i>Identification verification</i> <i>Criminal conduct known or suspected</i>	
Date of report	
Receipt of report acknowledged	
Signed	
MLRO	
Date	