

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

ANTI-MONEY LAUNDERING (AML) POLICY

KING ENTERPRISES N.V.

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

POLICY OWNER: KING ENTERPRISES N.V.

APPROVER: VASIL TONCHEV TONCHEV

DATE APPROVED: MAY 10, 2026

REVIEW FREQUENCY: ANNUALLY

NEXT REVIEW DATE: MAY 10, 2027

SECURITY CLASSIFICATION: CONFIDENTIAL

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

TABLE OF CONTENTS	
SCOPE AND PURPOSE.....	4
SIGNATURE OF COMPLIANCE OFFICER AND MANAGING DIRECTOR.....	4
LEGAL FRAMEWORK.....	5
CUSTOMER DUE DILIGENCE (CDD) – TRANSACTION THRESHOLDS AND ENHANCED VERIFICATION	5
AML – BUSINESS RISK ASSESSMENT AND RISK-BASED APPROACH	7
AML – CUSTOMER RISK ASSESSMENT (CRA)	8
AML – CUSTOMER ACCEPTANCE POLICY (CAP)	9
ONGOING DUE DILIGENCE AND REVERIFICATION	10
SOURCE OF FUNDS AND SOURCE OF WEALTH	11
SANCTIONS SCREENING AND RESTRICTED PERSONS	11
APPOINTMENT OF AML COMPLIANCE OFFICER	12
AML COMPLIANCE OVERSIGHT	12
INDEPENDENT AML REVIEW	12
CRYPTOCURRENCY AND VIRTUAL ASSET CONTROLS	13
TRANSACTION MONITORING AND SUSPICIOUS ACTIVITY REPORTING	14
TRANSACTION THRESHOLDS AND ENHANCED VERIFICATION.....	15
UNUSUAL TRANSACTION REPORTING TO CURAÇAO FIU (XCG 5,000 THRESHOLD).....	16
RECORD RETENTION	17
AML TRAINING.....	18

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

King Enterprises N.V. is dedicated to upholding rigorous standards in Anti-Money Laundering (“AML”), Counter-Terrorist Financing (“CTF”), and compliance with all applicable laws, regulations, and regulatory guidance in Curaçao, including requirements issued by the Curaçao Gaming Authority (“CGA”). As outlined in this Anti-Money Laundering and Counter-Terrorist Financing Policy (referred to as “the Policy”), we maintain a risk-based framework designed to prevent, detect, and respond to money laundering and terrorist financing risks, supported by effective governance, customer due diligence, transaction monitoring, and reporting obligations to the competent authorities where required.

SCOPE AND PURPOSE

This Policy applies to all individuals associated with King Enterprises N.V., including employees, agency personnel, temporary and permanent staff, interns, and any third parties acting for or on behalf of the Company.

The purpose of this Policy is to define King Enterprises N.V.’s:

- Approach to anti-money laundering (“AML”) and counter-terrorist financing (“CTF”) risk management; and
- Framework for compliance with applicable AML/CTF obligations, including the prevention, detection, and reporting of suspected money laundering, terrorist financing, or other criminal activity to the relevant competent authorities.

The principles and standards set out in this Policy are intended to ensure that identified money laundering and terrorist financing risks are appropriately assessed, managed, and mitigated.

This Policy should be read in conjunction with the procedures and controls relevant to your role and responsibilities. If you are uncertain about the appropriate course of action, unable to comply with any aspect of this Policy, or require clarification, you must promptly consult the Compliance Officer. A lack of understanding of the Policy or related procedures will not constitute an acceptable excuse for non-compliance.

Failure to comply with this Policy may expose the Company to significant financial, legal, regulatory, and reputational risk, including regulatory sanctions, fines, or enforcement action, and may also result in disciplinary measures.

SIGNATURE OF COMPLIANCE OFFICER AND MANAGING DIRECTOR

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

This Policy shall be approved and signed by our designated Compliance Officer and Managing Director.

The signed version of this Policy shall be maintained as part of our official compliance and governance records and may be provided to the Curaçao Gaming Authority (“CGA”) or other competent authorities upon request.

LEGAL FRAMEWORK

This Policy is established in accordance with the applicable laws, regulations, ordinances, and regulatory guidance of Curaçao, including but not limited to:

- The National Ordinance for Games of Chance (“LOK”);
- The National Ordinance on the Reporting of Unusual Transactions (“NORUT”);
- The National Ordinance on Identification when Rendering Services (“NOIS”);
- Curaçao Gaming Authority (“CGA”) Guidelines and applicable regulatory instructions;
- Applicable Sanctions Ordinances and sanctions-related regulations;
- The Criminal Code of Curaçao;
- Applicable Anti-Money Laundering and Counter-Terrorist Financing (“AML/CTF”) obligations.

We may periodically review and update this Policy to reflect changes in applicable laws, regulatory expectations, operational risks, or industry best practices.

CUSTOMER DUE DILIGENCE (CDD) – TRANSACTION THRESHOLDS AND ENHANCED VERIFICATION

We apply risk-based Customer Due Diligence (“CDD”) measures in accordance with applicable AML/CTF obligations, including customer identification, identity verification, sanctions screening, Politically Exposed Person (“PEP”) screening, transaction monitoring, and ongoing customer review procedures.

CDD measures may include:

- Identity verification through government-issued documentation;
- Verification of residential address;
- Age verification;
- Source of Funds (“SOF”) and Source of Wealth (“SOW”) reviews where appropriate;
- PEP screening;
- Sanctions and watchlist screening;
- Ongoing monitoring of account activity;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Transactional and behavioral analysis;
- Enhanced Due Diligence (“EDD”) procedures for higher-risk customers.

We may apply enhanced due diligence procedures when cumulative transactional activity reaches or exceeds the equivalent of XCG 4,000 or other applicable regulatory thresholds.

For AML/CTF monitoring purposes, the XCG 4,000 threshold is calculated based on the cumulative total of deposits and withdrawals conducted by a customer within a rolling thirty (30) day period, converted to XCG using the applicable exchange rate at the time of each transaction.

Where you reach the applicable threshold and the required verification documents or information have not yet been fully submitted, we may apply temporary account restrictions, withdrawal limitations, transaction delays, or enhanced monitoring measures until satisfactory verification is completed.

If the requested information or documentation is not satisfactorily received within thirty (30) days from the date the applicable threshold is reached, we reserve the right to suspend, restrict, or terminate the business relationship in accordance with our AML/CTF obligations and internal compliance procedures.

Where we determine that the business relationship cannot continue due to AML/CTF, sanctions, fraud, regulatory, verification, or financial crime concerns, we may:

- Restrict or suspend account access;
- Freeze or withhold funds where required by applicable law or regulatory obligations;
- Block or reject transactions;
- Escalate the matter for compliance review;
- File suspicious or unusual transaction reports with competent authorities in Curaçao where required;
- Terminate the business relationship.

We maintain ongoing sanctions screening procedures designed to monitor customers, transactions, wallets, jurisdictions, and related activity against applicable sanctions and watchlists, including United Nations (“UN”) sanctions lists and European Union (“EU”) sanctions lists.

Sanctions screening may occur:

- During onboarding;
- During ongoing monitoring;
- Upon material account changes;
- Upon reaching transactional thresholds;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Upon triggering elevated risk indicators;
- Periodically throughout the business relationship.

Where sanctions exposure, prohibited activity, or potential sanctions matches are identified, we may immediately restrict accounts, freeze relevant funds or transactions where required, conduct enhanced review procedures, and report relevant activity to competent authorities in Curaçao where applicable.

In such cases, we may:

- Temporarily restrict or freeze the relevant account or transaction;
- Escalate the matter to our Compliance Department for review;
- Conduct enhanced verification or investigation procedures where necessary;
- File reports with competent authorities in Curaçao where required by applicable law or regulatory obligations.

We and our personnel may be prohibited by law from disclosing the existence of sanctions investigations, suspicious activity reviews, or regulatory filings to affected customers or third parties.

AML – BUSINESS RISK ASSESSMENT AND RISK-BASED APPROACH

We apply a comprehensive risk-based approach to Anti-Money Laundering (“AML”), Counter-Terrorist Financing (“CTF”), sanctions compliance, fraud prevention, identity abuse prevention, payment abuse prevention, gameplay integrity protection, and related financial crime controls.

We maintain, document, implement, and periodically review a formal Business Risk Assessment (“BRA”) designed to identify, assess, evaluate, monitor, and mitigate risks associated with money laundering, terrorist financing, sanctions exposure, fraud, identity abuse, payment abuse, collusion, cryptocurrency-related risks, gameplay abuse, and other unlawful activities.

Our BRA considers, among others, the following risk factors:

- Customer risk profiles;
- Geographic and jurisdictional exposure;
- Products and services offered;
- Payment methods and transaction channels;
- Cryptocurrency-related risks;
- Peer-to-peer transactional exposure;
- Delivery channels and onboarding methods;
- Transactional behavior and wagering activity;
- Fraud indicators and suspicious behavioral patterns;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Gameplay integrity risks;
- Emerging technologies and operational changes;
- Third-party service provider exposure;
- Cross-border transactional exposure.

We apply risk-based mitigation measures, controls, monitoring procedures, restrictions, enhanced verification measures, transaction reviews, and compliance escalations proportionate to the identified level of risk.

We reserve the right to refuse, restrict, suspend, delay, review, or terminate customer relationships, transactions, products, services, or activities where the identified AML/CTF, fraud, sanctions, security, gameplay integrity, or operational risk exceeds the level deemed acceptable by Us.

We monitor the effectiveness of our risk mitigation controls and procedures through internal reviews, transaction monitoring, complaint reviews, fraud investigations, account reviews, audit activities, operational assessments, escalation procedures, security reviews, and periodic policy reassessments.

We review and update our BRA at least annually and additionally whenever material changes occur to our products, services, operating environment, technologies, customer base, transactional activity, delivery channels, payment methods, jurisdictions, or compliance obligations.

We may conduct dedicated risk assessments prior to the launch or implementation of new products, services, technologies, payment solutions, delivery mechanisms, operational practices, or other material business changes.

Our BRA shall be reviewed and approved by our Managing Director and Compliance Officer, and documentation relating to such reviews, approvals, assessments, and updates shall be maintained as part of our compliance and governance records.

We do not accept relationships, transactions, or activities involving sanctioned persons or jurisdictions, prohibited payment activity, fraudulent conduct, identity abuse, or cryptocurrency mixing or tumbling services designed to conceal transactional origin or ownership.

We periodically assess the effectiveness of our AML/CTF controls and risk mitigation measures through internal compliance reviews, operational monitoring activities, independent audits, and periodic reassessments of our risk management framework.

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

We apply a risk-based Customer Risk Assessment (“CRA”) framework designed to classify, assess, monitor, and periodically reassess customers based on money laundering, terrorist financing, sanctions, fraud, identity abuse, payment abuse, collusion, gameplay integrity risks, cryptocurrency exposure, and other financial crime risks.

Customers may be categorized into varying risk levels based on factors including, but not limited to:

- Geographic exposure;
- Transactional behavior;
- Deposit and withdrawal activity;
- Payment methods utilized;
- Cryptocurrency usage;
- Peer-to-peer transactional activity;
- Account activity and wagering patterns;
- Adverse media or suspicious indicators;
- Fraud or abuse indicators;
- Gameplay integrity concerns;
- Source of Funds (“SOF”) and Source of Wealth (“SOW”) considerations;
- Device, behavioral, or transactional inconsistencies.

We reserve the right to apply Enhanced Due Diligence (“EDD”), enhanced monitoring, additional verification procedures, periodic reassessments, account restrictions, transaction delays, temporary freezes, or termination of the customer relationship where elevated risk indicators are identified.

AML – CUSTOMER ACCEPTANCE POLICY (CAP)

We apply a risk-based Customer Acceptance Policy designed to prevent misuse of our products and services for money laundering, terrorist financing, fraud, sanctions evasion, identity abuse, collusion, gameplay abuse, payment abuse, or any other unlawful activity.

We reserve the right, at our sole discretion, to refuse, suspend, restrict, delay, review, or terminate accounts where:

- Sufficient identification or verification cannot be completed;
- False, misleading, altered, incomplete, or suspicious information is provided;
- The customer is located in a prohibited or high-risk jurisdiction;
- Suspicious transactional or gameplay behavior is detected;
- Geographic restrictions or compliance controls are circumvented or attempted to be circumvented;
- Payment methods not registered in the customer’s own name are used;
- AML, security, verification, or gameplay integrity requirements are not satisfied;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Fraud, collusion, chip dumping, gameplay abuse, prohibited software use, or suspicious activity is identified.

We reserve the right to reject deposits, delay withdrawals, freeze transactions, restrict gameplay activity, or terminate customer relationships where financial crime, fraud, sanctions, security, gameplay integrity, or compliance concerns arise.

ONGOING DUE DILIGENCE AND REVERIFICATION

We conduct ongoing due diligence throughout the customer relationship in order to monitor account activity, transactional behavior, identity consistency, source of funds, gameplay integrity, payment activity, and overall risk exposure.

We reserve the right to request updated documentation, enhanced identity verification, Source of Funds (“SOF”) information, Source of Wealth (“SOW”) information, cryptocurrency wallet verification, or supplementary information at any time, including where:

- Transactional thresholds are reached;
- Aggregate deposits, withdrawals, transfers, or cryptocurrency transactions exceed designated thresholds;
- Suspicious or unusual activity is detected;
- Material changes in customer behavior occur;
- Fraud, sanctions, AML, security, or gameplay integrity concerns arise;
- Customer information becomes outdated, inconsistent, or unverifiable;
- Additional review is required for operational, compliance, fraud prevention, or security purposes.

We reserve the right to apply temporary restrictions, withdrawal delays, enhanced review procedures, account freezes, transaction withholding, or termination of the customer relationship where requested information or documentation cannot be satisfactorily obtained or verified.

Where cumulative transactional activity reaches or exceeds applicable verification thresholds, including thresholds equivalent to XCG 4,000 or other internally established risk-based thresholds, we may suspend or restrict deposits, withdrawals, transfers, gameplay activity, or account access until required due diligence and verification measures have been completed.

Failure to provide requested documentation within thirty (30) days following the request may result in account suspension, account closure, withholding of transactions, escalation to compliance review, or reporting to competent authorities where required or permitted.

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.**SOURCE OF FUNDS AND SOURCE OF WEALTH**

We reserve the right to request information or documentation relating to a customer's Source of Funds ("SOF") and/or Source of Wealth ("SOW") in accordance with our AML/CTF obligations, ongoing monitoring procedures, risk-based controls, or enhanced due diligence requirements.

Such documentation may include, without limitation:

- Banking information;
- Employment or income information;
- Business ownership documentation;
- Cryptocurrency wallet verification;
- Blockchain transactional records;
- Tax-related documentation;
- Asset ownership documentation;
- Payment method ownership verification;
- Any other information reasonably required by Us.

We reserve the right to restrict, suspend, delay, freeze, or terminate account activity where satisfactory SOF/SOW information cannot be obtained or verified.

SANCTIONS SCREENING AND RESTRICTED PERSONS

We maintain sanctions compliance procedures designed to identify customers, transactions, wallets, jurisdictions, payment methods, cryptocurrency addresses, or activities that may be subject to sanctions restrictions, watchlists, prohibited jurisdiction restrictions, or other legal prohibitions.

We conduct ongoing sanctions screening and monitoring against applicable sanctions lists, watchlists, blockchain intelligence tools, regulatory databases, fraud databases, or other risk intelligence sources.

Where potential matches, sanctions exposure, prohibited activity, or high-risk transactional behavior is identified, we reserve the right to:

- Restrict or suspend account activity;
- Delay, reject, reverse, or block transactions;
- Freeze withdrawals or transfers;
- Request additional verification;
- Escalate the matter for compliance or security review;
- Terminate the customer relationship where appropriate;
- Report relevant activity to competent authorities where required or permitted.

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

We also reserve the right to prohibit or restrict transactions involving anonymizing services, mixers, tumblers, privacy-enhancing technologies, sanctioned wallet addresses, or high-risk cryptocurrency activities.

APPOINTMENT OF AML COMPLIANCE OFFICER

We have appointed a designated Anti-Money Laundering Compliance Officer (“AMLCO”) responsible for overseeing the implementation, effectiveness, and ongoing administration of our AML/CTF compliance framework.

Our AMLCO reports to senior management, including our Managing Director, and operates with sufficient independence, authority, and access to information to perform AML/CTF oversight responsibilities effectively and without undue commercial influence.

Our AMLCO is authorized to review and escalate suspicious activity, request enhanced due diligence measures, recommend account restrictions or suspensions, support regulatory reporting obligations, and coordinate AML/CTF compliance activities across relevant operational areas.

AML COMPLIANCE OVERSIGHT

We maintain AML/CTF compliance oversight procedures designed to support the effective implementation, administration, monitoring, and ongoing review of our AML/CTF framework.

Compliance oversight responsibilities may include:

- Monitoring AML compliance obligations;
- Supervising customer due diligence procedures;
- Reviewing suspicious activity escalations;
- Supporting internal reviews and audits;
- Coordinating AML awareness and operational training;
- Reviewing transaction monitoring procedures;
- Supporting regulatory and operational compliance processes.

INDEPENDENT AML REVIEW

We maintain independent review and assessment procedures designed to evaluate the effectiveness, adequacy, implementation, and operational performance of our AML/CTF compliance framework.

Independent reviews may include assessment of:

- AML policies and procedures;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Customer due diligence processes;
- Transaction monitoring systems;
- Security controls;
- Gameplay integrity controls;
- Recordkeeping procedures;
- Escalation and reporting procedures;
- Fraud prevention systems;
- Operational compliance measures.

We may implement remediation measures, operational improvements, control enhancements, or policy updates where deficiencies, emerging risks, or operational vulnerabilities are identified.

We maintain an annual independent AML review plan designed to assess the effectiveness of our AML/CTF controls, monitoring procedures, governance measures, and compliance framework.

Such reviews may be conducted by qualified independent internal personnel or external independent parties with appropriate AML/CTF knowledge and experience.

The scope of the annual review may include assessment of AML/CTF policies, customer due diligence procedures, sanctions screening measures, transaction monitoring controls, suspicious activity escalation procedures, recordkeeping practices, and overall control effectiveness.

Findings, recommendations, and identified deficiencies may be documented and reported to senior management, including our Managing Director and AML Compliance Officer (“AMLCO”), for review and oversight purposes.

Where deficiencies, weaknesses, or operational vulnerabilities are identified, we may implement remediation plans, corrective measures, enhanced controls, policy updates, or operational improvements within reasonable timeframes based on the nature and severity of the identified risk.

CRYPTOCURRENCY AND VIRTUAL ASSET CONTROLS

We may permit the use of certain cryptocurrencies, virtual assets, blockchain networks, or related payment technologies that we determine to be acceptable based on our operational, compliance, AML/CTF, fraud prevention, security, and risk management requirements.

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

We maintain risk-based monitoring and review procedures designed to assess cryptocurrency transactions, wallet activity, blockchain exposure, transactional behavior, and related financial crime risks.

Cryptocurrency-related controls may include:

- Wallet screening and blockchain monitoring procedures;
- Review of wallet activity and transactional patterns;
- Sanctions and watchlist screening;
- Enhanced monitoring of higher-risk cryptocurrency activity;
- Review of unusual, suspicious, or inconsistent transactional behavior;
- Enhanced Due Diligence (“EDD”) measures where appropriate;
- Source of Funds (“SOF”) and Source of Wealth (“SOW”) reviews for higher-risk or elevated cryptocurrency activity.

We do not permit the use of cryptocurrency transactions, wallets, services, or activities involving mixers, tumblers, privacy-enhancing mechanisms, sanctions exposure, prohibited jurisdictions, fraudulent conduct, or other activities designed to conceal transactional origin, ownership, or destination.

We reserve the right to request additional verification, restrict transactions, delay withdrawals, suspend account activity, freeze relevant funds where required, reject cryptocurrency transactions, or terminate the business relationship where cryptocurrency-related activity presents elevated AML/CTF, sanctions, fraud, security, or operational risk.

Where required by applicable law or regulatory obligations, we may escalate cryptocurrency-related activity for compliance review and report relevant activity to competent authorities in Curaçao.

TRANSACTION MONITORING AND SUSPICIOUS ACTIVITY REPORTING

We maintain ongoing monitoring systems and procedures designed to identify, review, assess, investigate, and escalate suspicious, unusual, fraudulent, abusive, manipulative, or potentially unlawful activity.

Monitoring may include:

- Transactional analysis;
- Deposit and withdrawal monitoring;
- Behavioral monitoring;
- Cryptocurrency wallet monitoring;
- Blockchain transactional analysis;
- Peer-to-peer transfer analysis;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Gameplay integrity analysis;
- Bonus abuse detection;
- Structuring and layering indicators;
- Device and identity correlation analysis;
- Collusion and chip-dumping indicators;
- Real-Time Assistance (“RTA”) indicators;
- Fraud and account abuse detection.

Our monitoring procedures may include automated triggers and alert mechanisms relating to:

- Structuring or fragmented deposit activity;
- High-velocity deposits or withdrawals;
- Repeated withdrawal reversals or cancellation patterns;
- Multiple accounts linked through shared devices, wallets, IP addresses, or behavioral indicators;
- Cryptocurrency wallets with exposure to mixers, tumblers, sanctions exposure, or other high-risk activity;
- Significant transactional activity inconsistent with known customer behavior;
- Rapid movement of funds with limited gameplay activity;
- Unusual peer-to-peer transfer patterns;
- Repeated failed verification attempts or inconsistent identity indicators;
- Frequent changes in device, location, IP address, or access behavior;
- Suspicious gameplay patterns, collusion indicators, or gameplay manipulation activity;
- Unusual, inconsistent, or elevated risk transactional behavior identified through internal monitoring procedures.

Where monitoring alerts, elevated risk indicators, suspicious activity triggers, or potential compliance concerns are identified, we may conduct internal reviews, apply enhanced monitoring measures, escalate the matter to our Compliance Officer or relevant internal teams, restrict account activity where appropriate, and report relevant activity to competent authorities where required by applicable law or regulatory obligations.

We reserve the right to report suspicious, unusual, fraudulent, abusive, or prohibited activity to competent regulatory, governmental, law enforcement, supervisory, financial intelligence, or compliance authorities where required or permitted.

We and our personnel may be prohibited from disclosing the existence of suspicious activity reviews, investigations, escalations, reports, account restrictions, monitoring procedures, or regulatory filings to affected customers or third parties.

TRANSACTION THRESHOLDS AND ENHANCED VERIFICATION

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

We apply enhanced verification, enhanced due diligence, monitoring, account review procedures, or transactional restrictions where certain transactional, cumulative, behavioral, security, or risk-based thresholds are reached.

Such measures may include:

- Additional identity verification;
- Source of Funds and Source of Wealth reviews;
- Enhanced monitoring;
- Temporary account restrictions;
- Transaction delays;
- Deposit or withdrawal freezes;
- Gameplay restrictions;
- Additional documentation requests;
- Escalation to compliance or security review.

Threshold calculations may include cumulative deposits, withdrawals, transfers, peer-to-peer transactions, cryptocurrency transactions, wagering activity, gameplay activity, or other relevant transactional activity over designated periods of time.

UNUSUAL TRANSACTION REPORTING TO CURAÇAO FIU (XCG 5,000 THRESHOLD)

We maintain monitoring and review procedures designed to identify, assess, investigate, and escalate unusual or potentially suspicious transactional activity in accordance with applicable AML/CTF obligations and reporting requirements in Curaçao.

For AML/CTF monitoring purposes, we monitor cumulative transactional activity, including deposits, withdrawals, transfers, and other relevant account activity. Where cumulative transactional activity reaches or exceeds the equivalent of XCG 5,000 within a rolling thirty (30) day monitoring period, an internal review process will be initiated to determine whether the activity should be reported as an unusual transaction to the Financial Intelligence Unit of Curaçao (“FIU Curaçao”).

Where the applicable threshold or other elevated risk indicators are identified, we may:

- Generate an internal compliance review case;
- Compile relevant Customer Due Diligence (“CDD”) information and transactional records;
- Escalate the matter to our AML Compliance Officer (“AMLCO”) for review;
- Conduct enhanced investigation or verification procedures where appropriate;
- Determine whether the activity should be reported to FIU Curaçao as an unusual transaction;

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

- Submit reports to FIU Curaçao through the goAML reporting system (or other FIU-designated reporting system, as applicable) where required;
- Maintain internal documentation relating to the review, escalation, and reporting process.

We and our personnel may be prohibited by law from disclosing the existence of unusual transaction reviews, FIU reports, suspicious activity investigations, or related reporting obligations to affected customers or unauthorized third parties. Access to FIU-related reporting information shall be limited to authorized personnel with a legitimate compliance, legal, regulatory, or operational need to know.

We maintain records relating to unusual transaction reviews, FIU reporting activities, AML/CTF investigations, and related compliance processes in accordance with applicable legal and regulatory obligations.

Such records may include:

- Customer identification and verification records;
- Customer Due Diligence (“CDD”) documentation;
- Source of Funds (“SOF”) and Source of Wealth (“SOW”) information where applicable;
- Sanctions and screening results;
- Transactional records and account activity related to the review or report;
- Internal case notes, escalations, and investigation records;
- AMLCO review outcomes and reporting decisions;
- FIU reporting references, confirmations, or related documentation where applicable.

We retain such records for a minimum period of five (5) years, or for such longer period as may be required by applicable law, regulatory obligations, ongoing investigations, or competent authorities in Curaçao.

RECORD RETENTION

We maintain records relating to customer identification, verification, transactions, complaints, investigations, escalations, compliance reviews, suspicious activity assessments, gameplay reviews, communications, security reviews, and related operational materials for AML/CTF, fraud prevention, audit, operational, security, regulatory, and business purposes.

Such records shall be retained for a minimum period of five (5) years following closure of the customer relationship, completion of the relevant investigation, or completion of the relevant transaction, unless a longer retention period is required.

ANTI-MONEY LAUNDERING POLICY - KING ENTERPRISES N.V.

We maintain records and registers relating to unresolved, pending, escalated, or externally reviewed complaints and investigations for compliance, operational, audit, supervisory, and regulatory purposes.

We reserve the right to securely store, archive, restrict access to, disclose, or provide access to such records where required for regulatory, legal, audit, fraud prevention, compliance, operational, or security purposes.

AML TRAINING

We maintain AML/CTF awareness and operational training measures designed to support compliance with financial crime prevention, fraud prevention, sanctions compliance, responsible gaming, security, and operational integrity obligations.

Relevant personnel may receive periodic training covering areas including:

- Customer due diligence;
- Suspicious activity identification;
- Fraud prevention;
- Transaction monitoring;
- Gameplay integrity risks;
- Sanctions compliance;
- Escalation procedures;
- Responsible gaming awareness;
- Data protection and confidentiality obligations;
- Cryptocurrency-related risk indicators;
- Security and account compromise indicators.

Training measures may be periodically reviewed and updated to reflect operational changes, emerging risks, technological developments, industry standards, and evolving compliance obligations.

Signed by:

Vasil Tonchev
C52C22CBD3684E0...

VASIL TONCHEV TONCHEV

Compliance Officer

Signed by:

Charles N. Porter
1E3D8C95E7764C4...

CHARLES N. PORTER

On behalf of Local Partners B.V

Managing Director