

ANTI-MONEY LAUNDERING, COUNTER-
TERRORISM FINANCING AND COUNTER-
PROLIFERATION FINANCING POLICY

WUNGroup B.V.

Information:

- **This Policy was approved by** the Board of Directors
- **Responsible Office for the compliance** - Compliance Officer
- The review of this Policy will be conducted **annually**
- This Policy should be read and understood by **all employees, contractors and third parties**
- This Policy is effective from the **May 28, 2025**
- Next review date - **May 28, 2026**

Policy History:

- May 28, 2025 - 1.0 - Policy Implementation

For any questions regarding this policy, please contact

Name: Diana Poksane

Email: di.poksane@gmail.com

TABLE OF CONTENTS

1. INTRODUCTION	5
GENERAL STATEMENT	5
PURPOSES.....	5
DEFINITIONS	6
CONSEQUENCES OF NON-COMPLIANCE	8
2. THE RISK-BASED APPROACH.....	9
WHAT IS THE RISK-BASED APPROACH.....	9
BUSINESS RISK ASSESSMENT	9
CUSTOMER RISK ASSESSMENT.....	9
3. CUSTOMER ACCEPTANCE POLICY.....	13
4. CUSTOMER DUE DILIGENCE (CDD).....	15
ENHANCED DUE DILIGENCE (EDD).....	17
TARGETED FINANCIAL SANCTIONS	18
POLITICALLY EXPOSED PERSONS	19
5. ONGOING MONITORING	22
6. RELIANCE ON THIRD PARTIES TO PERFORM CDD	24
CONDITIONS FOR RELIANCE.....	24
DISTINCTION FROM OUTSOURCING	25
RESPONSIBILITIES FOR CUSTOMER ONBOARDING	26
7. REPORTING OF UNUSUAL TRANSACTIONS	27
UNUSUAL TRANSACTIONS RECOGNITION.....	27

OBLIGATION FOR REPORTING	27
PROHIBITION OF DISCLOSURE	28
KEEPING RECORDS.....	29
8. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	31
COMPLIANCE OFFICER APPOINTMENT	31
AML MEASURES REGARDING EMPLOYEES	31
INDEPENDENT AUDIT.....	33
EXAMINATION BY THE CURACAO GAMING CONTROL BOARD	33

1. INTRODUCTION

GENERAL

STATEMENT

WUNGroup B.V. (hereinafter referred to as “Lucky Star” or the “Company”) is a licensed and regulated operator authorized by the Curaçao Gaming Authority (CGA) to provide remote (online) gaming services (OGL/2024/1382/0969). The Company’s number is 160576 and registered address is Chuchubiweg 17, Curaçao.

In line with the obligations set forth by its license and applicable regulatory frameworks, Lucky Star has established a robust Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing policy (hereinafter referred to as the “AML, CTF, and CPF Policy” or simply the “Policy”).

Operating as a responsible online gaming provider in Curaçao, Lucky Star is fully committed to preserving the integrity of the financial system and ensuring its platforms are not misused for illicit purposes. Compliance with AML, CTF, and CPF obligations is not only a regulatory necessity but also a key element of our broader commitment to ethical conduct and corporate accountability.

PURPOSES

This Policy is intended to secure the Company’s adherence to all applicable legal and regulatory obligations imposed by the designated supervisory authorities overseeing Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) within the gaming industry, namely the Curaçao Gaming Authority (CGA) and the Curaçao Financial Intelligence Unit (FIU). Simultaneously, the Policy aims to uphold the operational integrity and long-term viability of the Company’s business.

The Company is subject to the following legislative instruments and regulatory frameworks, including any further provisions enacted under the NOIS, NORUT, the Sanctions National Ordinance, and the Kingdom Sanction Law:

- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- 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 (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);

- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

DEFINITIONS

A. Money Laundering

Money Laundering (ML) refers to the practice of disguising the illicit origin of funds generated through criminal activities, thereby making such proceeds appear lawful. This activity broadly includes concealing or transforming assets derived from offences such as fraud, theft, or organized crime, as well as assisting in the movement or conversion of property linked to terrorism or criminal conduct.

ML is commonly executed through a three-phase methodology:

- **Placement:** This initial stage entails introducing unlawfully acquired funds into the financial ecosystem. Techniques may involve converting physical cash into monetary instruments or digital value through financial entities, casinos, or high-cash-volume businesses. Within the gambling sector, placement may be carried out by acquiring gaming chips with cash and subsequently exchanging them for payment after little or no gameplay. Alternatively, it may involve loading funds into casino accounts using instruments such as credit cards, prepaid options, cryptocurrencies, or checks, and then seeking withdrawals or issuing refund claims. Some also exploit gaming machines by depositing cash and quickly reclaiming it as credits.
- **Integration:** At this final phase, the illicit funds, having been sufficiently distanced from their origins, are re-entered into the legitimate economy. This is typically done through investment in lawful businesses, acquisition of high-value goods or services, or engagement in various forms of commercial activity that obscure the funds' criminal provenance.
- **Layering:** This stage consists of complex financial maneuvers intended to mask the criminal source of the funds. It frequently involves moving funds between multiple bank accounts or financial intermediaries, sometimes across borders or into different casinos, executing currency

exchanges, structuring or refining transactions to avoid detection thresholds, or simply retaining funds in gambling accounts to evade regulatory scrutiny.

B. Terrorism Financing

The concept of Terrorism Financing (TF) pertains to the allocation or transfer of financial resources intended to support terrorist entities, activities, or individuals. Its defining characteristic lies in the purpose behind the funding: to coerce, influence, or instill fear in governments, populations, or international organizations by facilitating acts of violence or disruption.

Unlike Money Laundering (ML), which is intrinsically linked to proceeds from unlawful conduct, the origin of funds involved in terrorism financing is not always illicit. In many cases, TF is sustained through legitimate income streams, such as revenues from lawful businesses, personal earnings, foreign governmental contributions, or charitable donations that are diverted from their stated purposes.

A key distinction between TF and ML lies in what is being concealed. While ML primarily seeks to obscure the origin of illicit funds, TF is more focused on hiding the destination and ultimate purpose of otherwise lawful or mixed-source funds. Despite this difference, both activities frequently utilize comparable financial mechanisms, including the use of structured transactions, cash couriers, wire transfers, or prepaid cards.

Furthermore, the execution of terrorist financing does not necessarily depend on large-scale funding. Modest contributions, accumulated gradually through a series of minor transactions, may suffice to sustain or initiate terrorist operations, making such activity difficult to detect without enhanced monitoring and due diligence.

C. Proliferation Financing

Proliferation Financing (PF) refers to the financial support or facilitation of activities connected to weapons of mass destruction (WMDs), including nuclear, chemical, or biological arms. This encompasses the funding of processes such as development, production, acquisition, transportation, stockpiling, transfer, brokering, or export of such weapons, their delivery systems, and associated materials. PF presents a significant threat to global security, often involving complex, cross-border networks designed to evade international sanctions and regulatory controls.

CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with this Policy may lead to serious repercussions. Employees who breach AML obligations may face disciplinary measures, up to and including termination. On an organizational level, non-compliance can expose the Company to legal liabilities, including substantial fines, regulatory sanctions, and possible criminal proceedings.

In addition to legal and financial risks, such violations may result in reputational harm, loss of licensing, heightened regulatory oversight, and deterioration of key business relationships, all of which jeopardize the Company's ability to operate effectively.

2. THE RISK-BASED APPROACH

WHAT IS THE RISK-BASED APPROACH

In alignment with FATF recommendations, Lucky Star applies a risk-based methodology within its AML compliance framework, tailored to the unique risk landscape of the online gaming sector.

This strategy enables the Company to prioritize resources and mitigation efforts proportionate to the level of risk identified.

As part of this approach, the Company performs an initial risk assessment focused on potential exposure to money laundering, terrorist financing, and proliferation financing (ML/TF/PF). Based on this analysis, Lucky Star designs and enacts appropriate internal controls, policies, and procedures, this Policy included to address and reduce such risks. Higher-risk scenarios require enhanced due diligence and stricter controls, while lower-risk cases may warrant simplified measures.

Lucky Star remains committed to ongoing review and refinement of its risk management framework. This includes maintaining comprehensive documentation of risk evaluations, decisions made, and the rationale behind chosen measures. In addition, the Company actively evaluates risks associated with the adoption of new technologies and gaming offerings that could be exploited for ML/TF/PF purposes.

BUSINESS RISK ASSESSMENT

As an integral element of its AML, CTF, and CPF compliance framework, Lucky Star relies on a structured Business Risk Assessment (BRA) process to proactively identify and manage threats related to money laundering, terrorist financing, and proliferation financing. The BRA framework underpins the Company's ability to implement a proportionate, risk-sensitive approach to its operations.

This assessment encompasses a broad range of internal and external risk factors, including but not limited to customer profiles, geographic exposure, product offerings, and service delivery channels. Each factor is analyzed in terms of probability and potential severity, following which risk-specific controls are devised and applied. Findings and mitigation strategies are formally documented and submitted to senior management, with relevant disclosures made to supervisory bodies where required.

BRA exercises are not static but are conducted on a recurring basis to ensure the Company's risk profile remains current and accurate. Significant operational changes—such as the rollout of new payment instruments, expansion into new jurisdictions, or changes in customer demographics—automatically trigger a reassessment of business risks. Likewise, regulatory updates or the launch of new games that materially alter the Company's risk exposure will prompt targeted revisions to the BRA.

Lucky Star also ensures that the outcomes of these assessments inform broader strategic planning, compliance priorities, and internal training programs, reinforcing a risk-aware culture across all business units.

CUSTOMER RISK ASSESSMENT

As part of its broader risk management system, Lucky Star employs a detailed Customer Risk Assessment

(CRA) mechanism designed to evaluate the exposure the Company may face when engaging with individual clients. This process begins at the onboarding stage, where each new customer is initially assessed to determine their Customer Risk Rating, based on both provided and verified data. This rating forms the basis of the customer's risk profile and directly informs the intensity and frequency of future monitoring.

Rather than applying a uniform approach to all customers, the Company tailors its due diligence and monitoring efforts in accordance with the level of risk identified. Customers classified as high-risk undergo enhanced scrutiny and more frequent reviews throughout the lifecycle of the business relationship. The CRA serves as a dynamic tool, updated as new data emerges or risk indicators shift.

The evaluation of customer-related risk forms part of a broader analytical structure that also includes product and service risk considerations. Both domains are assessed according to several overarching risk dimensions:

A. Customer Risk

The Company examines the customer's personal and financial characteristics, behavioral patterns, and any inconsistencies between observed activity and declared information. Indicators of elevated customer risk include:

- Presence of multiple or unverified income sources;
- Irregular or non-transparent financial activity;
- Classification as a Politically Exposed Person (PEP);
- Unusually high or disproportionate levels of gambling expenditure relative to declared assets;
- Use of third parties to conduct gambling transactions—often a tactic to obscure ownership of funds or circumvent customer due diligence;
- Other anomalies suggesting the potential misuse of the gaming platform for concealment or obfuscation.

B. Product/Service Risk

The inherent risk of particular games, features, or payment options is also assessed. Certain products and transactional behaviors are more susceptible to abuse for money laundering (ML), terrorist financing (TF), or proliferation financing (PF). Risk indicators in this category may include:

- Anonymous or opaque funding methods, such as prepaid cards or virtual assets;
- Abnormal account behavior, such as sudden spikes in betting volume or limited gameplay activity following deposits;
- Peer-to-peer gaming setups where players may collude or influence outcomes, increasing the risk of manipulation;
- Transfers between accounts or the operation of multiple wallets by a single user;
- Frequent modifications to linked payment methods, especially involving unverified sources;
- Games operated jointly across platforms, such as shared poker environments involving multiple operators, which may complicate monitoring and attribution of activity;
- Electronic wallets (e-wallets), particularly those not licensed in reputable jurisdictions or those accepting direct cash deposits. Some e-wallets mask transaction details, preventing the gaming

operator from seeing the true origin of funds, thus providing opportunities to conceal gambling behavior or its financing;

- Use of fraudulent identities or financial instruments, including compromised accounts or fabricated personal data used to bypass controls.

Through the integration of these customer and product risk factors, Lucky Star ensures that each client relationship is evaluated not only at the point of onboarding, but throughout its duration. This ongoing assessment supports the Company's obligation to identify suspicious behavior early, apply appropriate risk-based controls, and comply fully with applicable AML/CTF/CPF regulations.

C. Geographical Risk

When evaluating risk, Lucky Star closely examines the geographic dimensions of customer relationships and transactions, recognizing that jurisdictional factors can significantly influence exposure to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). The geographic location of the customer, along with their nationality, residence, and place of birth, are all considered potential risk indicators.

Jurisdictions characterized by weak financial oversight, systemic corruption, or inadequate AML/CTF/CPF frameworks are subject to enhanced scrutiny. In assessing geographic risk, Lucky Star references authoritative external sources, including—but not limited to—the following:

- FATF's list of High-Risk Jurisdictions subject to a Call for Action;
- FATF's list of Jurisdictions under Increased Monitoring;
- CFATF Public Statements;
- U.S. Department of State's International Narcotics Control Strategy Report (INCSR), particularly jurisdictions of concern or primary concern;
- European Commission's list of high-risk third countries with strategic deficiencies in their AML/CTF/CPF systems;
- Sanction lists issued by the U.S. Office of Foreign Assets Control (OFAC);
- Reports by credible sources identifying jurisdictions that support or harbor terrorist entities;
- Transparency International's Corruption Perceptions Index.

Lucky Star maintains an ongoing process of monitoring these resources and updates its customer due diligence (CDD) procedures accordingly. Where applicable, heightened due diligence measures are imposed to mitigate risks stemming from high-risk jurisdictions. (Refer to Appendix I for applicable lists.)

D. Delivery Channels Risk

In addition to geographic considerations, Lucky Star assesses the risk associated with the delivery channels used to initiate and conduct customer relationships and transactions. Channels that enable anonymity or eliminate face-to-face interaction inherently present higher risk, particularly in digital environments.

Examples include:

- Remote onboarding processes without video verification;
- Payment systems that obscure the origin of funds;
- Automated transaction mechanisms with limited real-time oversight.

To mitigate these risks, the Company applies enhanced verification procedures and implements monitoring tools to detect suspicious patterns associated with non-transparent or indirect customer interactions. Where full mitigation is not feasible, the Company may opt to restrict or refuse access to certain products or services based on the assessed channel risk.

3. CUSTOMER ACCEPTANCE POLICY

Lucky Star adheres to a strict Customer Acceptance Policy, structured in line with applicable legal and regulatory frameworks, the Company's internal Business Risk Assessment (BRA), and its zero-tolerance approach to financial crime. The admission of new customers is subject to a risk-sensitive evaluation process designed to prevent the onboarding of individuals involved—directly or indirectly—in unlawful activity or behavior incompatible with the integrity of our operations.

Eligibility Requirements

- Access to Lucky Star's services is restricted to individuals who satisfy all of the following baseline conditions:
- The applicant is a natural person (corporate entities and other legal persons are not permitted);
- The applicant is at least 18 years of age;
- The applicant resides in a permitted jurisdiction not subject to national or international restrictions;
- The applicant acts solely on their own behalf and registers only a single account;
- The applicant is the legal and beneficial owner of all payment methods used;
- The applicant has accepted the most recent version of the Company's Terms and Conditions, Privacy Policy, and other applicable policies;
- The applicant has been fully identified and verified in accordance with AML compliance standards, including checks on identity, age, residence, and risk profile;
- The applicant has passed all due diligence reviews, including (where applicable) verification of the source of funds and source of wealth.

Exclusion Criteria

- Customers will be denied access or have their accounts closed if they meet any of the following disqualifying criteria:
- Presence on any recognized sanctions list (e.g. UN, EU, OFAC);
- Residence in or links to jurisdictions subject to full or partial sanctions;
- Risk rating exceeding the Company's accepted threshold;
- Use of falsified, incomplete, or fraudulent documentation;
- Attempts to obscure identity or open multiple accounts for circumvention purposes;
- Refusal or failure to provide required documents or information within the timeframe set by this Policy;
- Indications of involvement in money laundering, terrorism financing, or other financial crimes;
- Inclusion in self-exclusion registers, whether internal or as required by relevant licensing authorities;
- Registration under clearly fictitious, fabricated, or unverifiable identities.

Due Diligence

Prior to establishing any customer relationship, Lucky Star undertakes comprehensive due diligence checks. This includes identity verification, screening against sanctions and watchlists, and assessment of customer-supplied data against risk criteria. Politically Exposed Persons (PEPs) are subject to enhanced scrutiny at onboarding.

The Company retains full discretion to request additional information at any stage of the customer lifecycle. Should the customer fail to meet documentation or verification obligations in the timeframe prescribed, Lucky Star reserves the right to suspend or terminate the business relationship without further notice.

4. CUSTOMER DUE DILIGENCE (CDD)

Lucky Star enforces comprehensive Customer Due Diligence (CDD) protocols to ensure full compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations, as well as to safeguard the transparency and integrity of its operations. CDD measures are applied both at the onboarding stage and throughout the customer relationship, particularly when risk indicators are present.

CDD must be conducted in the following circumstances:

- **Threshold-based Transactions:** When a player conducts financial transactions (e.g. deposits or withdrawals) amounting to Cg. 4,000 or more. This assessment includes both individual transactions and cumulative activities forming a recognizable pattern. Daily transaction reviews are carried out to capture all qualifying activity, including peer-to-peer transfers.
- **Suspicion of ML/TF:** Any indication or suspicion of money laundering or terrorist financing triggers immediate CDD, regardless of transaction size.
- **Doubts About Identity Data:** If previously collected identification information is found to be incomplete, inconsistent, or potentially inaccurate, renewed CDD procedures are initiated.

Registration and Identity Verification

At the time of registration, each customer is required to provide a complete and accurate profile. The following personal data is collected:

- Full legal name;
- Date and place of birth;
- Residential address;
- Nationality;
- Identity number.

To validate the information provided, customers must upload a **government-issued photo ID** (e.g. passport, identity card, or driver's license). Documents must clearly display the customer's name, date of birth, and photograph. Instructions for document submission are communicated through the customer's registered contact details.

If documents are in a language not understood by the Company, a **certified translation** of the relevant portions may be requested. In such cases, the customer is expected to submit either an official bilingual document or a certified true copy accompanied by a verified translation.

Proof of Address and Supporting Documents

Documents lacking a photograph, such as government-issued correspondence, may still be accepted for the **verification of residential address**, provided the address is clearly stated. Additionally, Lucky Star may request any of the following as proof of residence, ensuring they are dated within the past **six (6) months**:

- Utility bills (electricity, gas, water, fixed telephone);
- Recent bank account statements.
- Ownership and Third-Party Use Restrictions

To comply with AML obligations, Lucky Star must verify that customers are acting exclusively on their **own behalf**. Players are required to declare that they are not using their account to facilitate transactions or gameplay for any third party.

However, reliance on self-declaration alone is insufficient. The Company employs ongoing **transaction monitoring mechanisms** to identify behavior consistent with proxy use or third-party access. If detected, such activity may result in account restrictions, suspension, or closure.

To enforce these standards, Lucky Star has introduced a range of internal controls designed to detect and prevent misuse:

- **Payment Method Ownership Check:** Deposits are permitted only from payment instruments legally owned by the customer;
- **Rejection of Third-Party Payment Sources:** Transactions involving payment methods not registered in the customer's name are declined;
- **Withdrawal Verification:** Customer identity is revalidated prior to the processing of any withdrawal, ensuring consistency with onboarding records.

ENHANCED DUE DILIGENCE (EDD)

Where a customer is assessed to pose an elevated risk of money laundering (ML), terrorism financing (TF), or proliferation financing (PF), Lucky Star applies **Enhanced Due Diligence (EDD)** measures. These enhanced procedures are designed to provide a deeper understanding of the customer profile and ensure intensified scrutiny of their activities throughout the duration of the business relationship.

EDD is not applied uniformly; it is tailored based on the nature and level of the identified risk, ensuring that monitoring efforts are proportionate and effective.

EDD procedures are automatically triggered under any of the following conditions:

- **High-Risk Jurisdictions:** The customer resides in or is otherwise connected to a country identified as having significant deficiencies in AML/CTF/CPF enforcement, high levels of corruption, or subject to international sanctions.

The list of jurisdictions which are deemed to be high risk includes without limitation Afghanistan, Algeria, Angola, Bulgaria, Burkina Faso, Cameroon, Côte d'Ivoire, Cuba, Democratic Republic of the Congo, India, Indonesia, Iran, Iraq, Haiti, Kenya, Laos, Lebanon, Liberia, Libya, Mali, Monaco, Mozambique, Myanmar (Burma), Namibia, Nepal, Nigeria, North Korea, Pakistan, Russian Federation, Somalia, South Africa, South Sudan, Sudan, Syria, Tanzania, Ukraine (Crimea, Donetsk, Lugansk), United Arab Emirates, Vanuatu, Venezuela, Vietnam, Yemen

- **Politically Exposed Persons (PEPs):** The customer holds or is linked to individuals holding prominent public roles—such as senior government officials, judiciary members, or military leaders—thereby increasing the risk of politically linked financial misconduct.
- **Products or Channels That Promote Anonymity:** Transactions or services which inherently reduce transparency, such as those using anonymous payment instruments or digital assets, may elevate exposure to illicit activity.
- **Innovative or Unfamiliar Business Models:** New technologies, product offerings, or delivery mechanisms—particularly those without a proven risk profile—can introduce previously unidentified vulnerabilities requiring close oversight.

To effectively mitigate higher-risk profiles, Lucky Star may implement one or more of the following enhanced due diligence measures:

- **Expanded Customer Background Checks:** Collect additional personal data including employment details, historical addresses, and information derived from reliable public or commercial sources to build a more comprehensive profile.
- **Clarification of Relationship Purpose:** Obtain more detailed insight into the customer's intentions for engaging with the platform, their expected gaming behavior, and financial activity patterns.
- **Verification of Source of Funds (SOF) and Source of Wealth (SOW):** Require customers to provide specific documentation or declarations substantiating the origin of their funds and accumulated assets. Acceptable sources include, but are not limited to:
 - Salary or employment income
 - Retirement or pension disbursements
 - Property or asset sales
 - Dividends or returns from investments
 - Gambling-related profits
 - Inheritances, gifts, or compensation awards
 - Savings built over time

In cases where risk persists over time, Lucky Star may request SOF/SOW updates **on a recurring basis**, even in the absence of new activity.

- **Transaction-Level Clarification:** Seek explanations from the customer regarding the purpose and justification for specific transactions to verify they align with the established customer profile.

Timeline for Compliance and Non-Compliant Documents

In accordance with AML regulatory obligations, Lucky Star enforces strict timeframes and procedures when a customer reaches the cumulative transaction threshold of Cg. **4,000**. If a customer fails to submit fully compliant documentation **within 30 days** of reaching this threshold, the Company shall terminate the business relationship and evaluate whether the circumstances warrant the submission of an Unusual Activity Report (UAR) to the Financial Intelligence Unit (FIU), particularly where there is a reasonable

presumption of money laundering (ML) or terrorist financing (TF).

While the Customer Due Diligence (CDD) process is underway, the customer is allowed to retain access to their account. However, transactional capabilities will be restricted based on how the threshold is triggered:

- Deposits reaching the threshold: Further deposits or withdrawals will be suspended. The customer may continue gameplay using their existing balance.
- Withdrawals triggering the threshold: In such cases, the account will be fully locked, suspending all activity—including gameplay—until the required documentation is reviewed and verified.

Handling and Escalation of Non-Compliant Documents

Should a submitted document fail to meet the Company's verification standards, it must be flagged immediately by the responsible compliance personnel. The staff member must perform a comprehensive assessment to identify the precise reason for non-compliance—such as invalid issue dates, poor image quality, or discrepancies with previously submitted data.

Once the deficiency is identified, the customer must be promptly informed and requested to provide acceptable documentation without delay. No further processing of the customer's CDD will occur until compliant documents are received.

All related actions—starting from the detection of the non-compliance, through internal assessments, communications with the customer, any escalations to senior management or compliance officers, and the eventual resolution—must be thoroughly documented in the customer's file. This detailed audit trail is essential for regulatory reporting and future internal or external reviews.

TARGETED FINANCIAL SANCTIONS

Lucky Star upholds a strict commitment to complying with all applicable targeted financial sanctions, particularly those imposed by the United Nations (UN) and the European Union (EU) concerning individuals or entities linked to terrorism financing or the proliferation of weapons of mass destruction. These obligations mandate the freezing of assets and funds of listed parties and require the Company to maintain robust internal mechanisms to detect and respond to such cases.

To ensure full compliance with the applicable sanctions regime, Lucky Star has implemented the following key controls:

- Sanctions Monitoring: The Company continuously tracks and incorporates updates to sanctions regulations, including any amendments to national decrees and international frameworks, and ensures their immediate operational implementation.
- Customer Screening Procedures: Sanctions screening is conducted both on an ongoing basis and in response to certain events ("trigger events"). At a minimum, screening is performed:
 - At the initial registration of a new customer;

- When the customer submits a withdrawal request;
- Upon modification of personal information or payment details.
- Detection and Escalation: If sanctions screening results in a confirmed match, Lucky Star will activate its internal sanctions response protocol, which includes freezing the affected funds and assets in accordance with the procedures outlined in the Sanctions National Ordinance.
- Mandatory Reporting: In every confirmed sanctions match, Lucky Star shall immediately report the matter to the Financial Intelligence Unit (FIU) and fully cooperate with the competent authorities in accordance with legal obligations.

These measures form an integral part of Lucky Star's broader AML/CFT compliance framework and reflect its zero-tolerance approach to financial crime and regulatory breaches.

POLITICALLY EXPOSED PERSONS

In the context of anti-money laundering and counter-terrorism financing compliance, Politically Exposed Persons (PEPs) represent a category of individuals who, by virtue of their prominent public positions, may present a heightened risk of involvement in bribery, corruption, or other forms of financial crime. Lucky Star acknowledges and applies enhanced scrutiny to such individuals in accordance with international best practices.

A person shall be classified as a PEP if they are or have been entrusted with a notable public function, excluding lower-level or middle-ranking positions. This category includes, but is not limited to:

- Heads of state or government, ministers, deputy and assistant ministers;
- Legislators, including members of national parliaments or equivalent governing bodies;
- Senior officials of political parties in a decision-making capacity;
- Judges of supreme, constitutional, or other high-level courts whose rulings are generally final;
- Senior audit officials and central bank board members;
- High-ranking diplomats, including ambassadors and chargés d'affaires, as well as senior military officers;
- Executives in state-owned enterprises, such as members of the board, directors, or senior managers;
- Top officials of international organizations, including members of boards or individuals with equivalent responsibilities.

In addition to the primary category, certain persons are also to be treated as PEPs due to their personal or professional association with individuals occupying these roles. This includes:

- Immediate family members, such as spouses or partners, children and their spouses or partners, and parents;
- Close associates, such as individuals known to share joint beneficial ownership in legal entities or arrangements, those with significant business relationships with a PEP, or individuals who

serve as the sole beneficial owner of a legal structure established for the benefit of a PEP.

These extended definitions are critical for ensuring thorough due diligence and for mitigating risks associated with undue influence or misuse of public office for private gain.

CDD Measures Specific to PEPs

Lucky Star maintains a robust framework for the identification and management of Politically Exposed Persons (PEPs), as well as individuals who are their relatives or close associates (RCAs). This process is designed to mitigate the elevated risks associated with such individuals and is aligned with international AML/CTF/CPF standards.

Identification of PEPs

At the initial stage of onboarding, all new customers are screened against trusted databases and watchlists to determine whether they are classified as a PEP or an RCA. This screening forms part of the Customer Due Diligence (CDD) process and is mandatory before any relationship can be formalized.

Screening continues throughout the duration of the customer relationship. If a customer's status changes and they are subsequently identified as a PEP, enhanced measures will be implemented within **30 days** of detection.

Senior Management Approval

No business relationship with a PEP—whether a newly onboarded customer, an existing one, or an individual engaging in occasional high-value transactions—shall be commenced or continued without prior approval from **senior management** or the **Compliance Department**. This ensures an additional layer of oversight for high-risk relationships.

Assessment of Source of Wealth and Funds

To mitigate misuse of public office or illicit enrichment, Lucky Star takes proactive steps to understand and verify the financial background of identified PEPs:

- A written declaration regarding the **source of wealth** (SOW) must be provided by the customer.
- The SOW declaration is independently assessed through publicly available data. Where this is insufficient, the Company will request supporting documentation to substantiate the declared origin of funds.

Ongoing Monitoring

Enhanced ongoing monitoring is mandatory for all PEP relationships. This includes, but is not limited to:

- Regular review of transaction activity to ensure alignment with the customer's known financial

background;

- Closer analysis of **spending patterns**, to detect inconsistencies or unexplained financial behavior;
- Periodic reassessment of risk based on any changes in the customer's profile or status.

Risk-Based Considerations

The extent and intensity of measures applied to a PEP will depend on several risk factors, such as:

- The **public function held** by the PEP (e.g. seniority, influence, exposure);
- The **country of origin**, particularly if it has high corruption risk or weak AML regulations;
- The **nature and volume of transactions**, and whether these are proportionate to declared income or assets.

Consequences of Non-Compliance

Failure to complete the necessary EDD procedures for newly identified PEPs within the 30-day window will result in termination of the business relationship. This measure ensures that Lucky Star does not maintain relationships with customers whose risk profile exceeds its stated tolerance or compliance capacity.

5. ONGOING MONITORING

To ensure continuous compliance with AML/CTF/CPF regulations and to uphold the integrity of its operations, Lucky Star maintains a dynamic and structured monitoring framework. This involves two core components: periodic customer profile reviews and ongoing transaction surveillance.

Customer Profile Monitoring

Lucky Star conducts scheduled reviews of customer profiles to confirm that all information obtained during initial due diligence—such as identification data, source of funds (SOF), and the stated purpose of the business relationship—remains accurate, complete, and relevant.

As part of this periodic assessment, the following actions are taken:

- Validation of CDD information and identification documents.
- Reconfirmation of declared SOF and updates where applicable.
- Review of external sources (e.g., adverse media, regulatory or legal developments) to assess any reputational or compliance-related concerns.
- Screening against updated sanctions lists and PEP databases.

Examination of the customer's transaction history to identify anomalies or behaviors inconsistent with the declared profile.

The frequency of these periodic reviews is determined based on the customer's risk rating:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

Transaction Monitoring

In addition to scheduled reviews, Lucky Star performs real-time and retrospective transaction monitoring to detect unusual or suspicious activity. This ensures that all customer behavior aligns with the Company's expectations based on known customer profiles.

Monitoring efforts are focused on:

- Customers deemed **high-risk**;
- **Large or complex transactions**;
- Transactions involving **high-risk jurisdictions**;
- Patterns of behavior that significantly deviate from the customer's historical activity or initial stated purpose.

Specific red flags triggering closer scrutiny include:

- Gambling patterns that are inconsistent with prior behavior or risk profile;
- Large, rapid, or frequent deposits and withdrawals that raise suspicion;
- Attempts to withdraw funds to **unverified or third-party accounts** (which are strictly prohibited);
- Requests to **transfer winnings or account balances to third parties** (also prohibited).

This dual-layered monitoring system enables Lucky Star to respond promptly to risk indicators, adapt its controls, and report any suspicious activity in accordance with applicable regulations.

6. RELIANCE ON THIRD PARTIES TO PERFORM CDD

Lucky Star acknowledges that in certain circumstances, aspects of the Customer Due Diligence (CDD) process may be delegated to qualified third parties. While this can streamline onboarding and enhance operational efficiency, the Company remains ultimately responsible for ensuring that all regulatory requirements are fully met.

CONDITIONS FOR RELIANCE

A. Scope of Third-Party Involvement

Reliance on third parties is limited to specific CDD components, namely:

- Identification and verification of the player's identity using reliable and independent documentation or data sources.
- Verification of the beneficial owner, including understanding the ownership and control structure (where applicable, such as for legal entities).
- Clarification of the purpose and intended nature of the customer relationship.

B. Conditions for Acceptable Reliance

For Lucky Star to rely on a third party, the following conditions must be strictly met:

1. Immediate Access to CDD Information:
 - All relevant CDD information and documentation must be made available to Lucky Star by the third party without delay.
2. Formal Agreement in Place:
 - A written agreement must be concluded between Lucky Star and the third party. This agreement will clearly outline:
 - The third party's obligations to share CDD records on request;
 - The mechanisms for ongoing cooperation and oversight;
 - The right of Lucky Star to test the arrangement periodically.
3. Regulatory Standing of Third Party:

The third party must be:

- Subject to supervision or monitoring by competent authorities in its jurisdiction;
 - Compliant with international AML/CFT standards;
 - Equipped with procedures to apply and document effective CDD and record-keeping.
4. Independent Customer Relationship:

The third party should already maintain a direct business relationship with the customer independent of

their interaction with Lucky Star and must conduct its own CDD, not merely act as a pass-through.

C. Retained Responsibilities

Even when CDD measures are outsourced, Lucky Star remains fully responsible for:

- Performing a customer-based risk assessment;
- Identifying PEPs and applying appropriate EDD measures where applicable;
- Conducting ongoing monitoring of transactions and customer activity;
- Ensuring that third-party reliance does not compromise the effectiveness of the AML program.

D. Country Risk Considerations

Before entering into any reliance arrangement, Lucky Star will evaluate the jurisdiction in which the third party is located. This evaluation ensures that the country:

- Has effective AML/CFT frameworks;
- Is not listed among high-risk or non-cooperative jurisdictions;
- Offers an appropriate level of regulatory oversight over the third party.

This due diligence is critical to safeguarding the integrity of Lucky Star's compliance efforts.

DISTINCTION FROM OUTSOURCING

It is important to clearly distinguish between reliance on third parties and the outsourcing of Customer Due Diligence (CDD) measures.

In the case of outsourcing, Lucky Star contracts a service provider to carry out certain CDD tasks on its behalf, under its direct control and according to its internal procedures. Although these functions are delegated, full legal and regulatory responsibility remains with Lucky Star.

To ensure compliance, any outsourcing arrangement must meet the following conditions:

- The service provider must be reputable, reliable, and sufficiently resourced to carry out the delegated functions;
- A formal written agreement must be in place, clearly outlining the responsibilities of both Lucky Star and the service provider;
- Lucky Star must retain full and immediate access to all records and documentation generated or obtained through the outsourced functions;
- Regular performance assessments—both quantitative and qualitative—must be conducted to verify that the outsourcing arrangement is functioning effectively and in accordance with expectations.

RESPONSIBILITIES FOR CUSTOMER ONBOARDING

All customer onboarding activities, whether carried out directly by Lucky Star, through an agent, or via a group entity, are treated as being performed by Lucky Star itself.

Accordingly:

- All customers, regardless of how they are onboarded, must be subject to the same CDD standards and AML/CFT controls;
- Lucky Star is fully responsible for ensuring that all onboarding channels apply its AML policies, procedures, and risk assessment measures consistently;
- The Company must provide adequate oversight and training to agents or group entities to ensure uniform application of AML compliance obligations.

7. REPORTING OF UNUSUAL TRANSACTIONS

UNUSUAL TRANSACTIONS RECOGNITION

Lucky Star places a strong emphasis on identifying and managing unusual transactions as part of its commitment to detecting and preventing money laundering (ML) and terrorist financing (TF). Staff are regularly trained to recognize such transactions by comparing customer activity to established profiles and behavioral patterns, and are required to escalate any suspicious findings through clearly defined internal channels.

Criteria for Identifying Unusual Transactions

In line with regulatory obligations, Lucky Star applies both **objective** and **subjective** indicators to determine whether a transaction is to be classified as unusual:

- **Objective indicators** are based on observable, measurable facts and automatically trigger classification as unusual without need for interpretation.
- **Subjective indicators** require a contextual assessment of the customer's behavior and financial activity, including the broader risk profile.
- All unusual transactions—regardless of the type—must be **promptly reported** to the Compliance Officer using the prescribed format, along with relevant supporting documentation (e.g., customer identification, transaction slips, chat logs, internal notes).

The Compliance Officer is responsible for maintaining an **organized, auditable record** of all reported cases. In instances where an internal alert is not forwarded to the Financial Intelligence Unit (FIU), the rationale must be thoroughly documented and signed by the Compliance Officer and/or a member of senior management.

Objective Indicators: Automatically Reportable Transactions

The following scenarios are **automatically deemed unusual** and must be reported:

- a. Transactions already flagged or reported to police or judicial authorities in relation to ML or TF activities.
- b. Any transaction—attempted or completed—involving individuals or entities listed under the **Sanctions National Ordinance (N.G. 2014 no. 55)**.
- c. Any single transaction or group of related transactions reaching or exceeding **Cg. 5,000.00 per game day**, including but not limited to:
 - Cashless or electronic transactions totaling Cg. 5,000.00 or more.
 - Deposits or withdrawals at or above the Cg. 5,000.00 threshold.
 - Purchase or redemption of gaming chips, tokens, or credits at or above the threshold.
- d. Any transaction that, based on available information, **raises a reasonable presumption** of involvement in money laundering or terrorist financing.

Examples of Suspicious Customer Behavior

The following customer behaviors may trigger a subjective assessment and are considered **red flags**:

- Refusal to cooperate with the Customer Due Diligence (CDD) process.
- Attempts to open multiple accounts under different identities or aliases.
- Frequent use of multiple prepaid cards for high-value deposits.
- Deposits far exceeding typical patterns without clear justification.
- Minimal gameplay despite large deposits, followed by large withdrawal requests.
- Repeated short-term deposits and withdrawals without economic rationale.
- Abrupt shifts in transaction sizes or betting patterns inconsistent with known behavior.
- Requests to transfer funds to third-party accounts or other players.
- Gambling activities that exceed what is reasonable based on the customer's declared income or wealth.
- Inquiries or actions suggesting an attempt to **bypass AML controls**, such as transferring winnings within the same gaming group.
- Suspicious conduct in connection with **high-risk games** (e.g., peer-to-peer poker, high-stakes roulette).

Lucky Star's proactive approach to transaction monitoring ensures that unusual activity is not only detected but addressed in a timely, compliant, and traceable manner, in alignment with FATF Recommendations and national legal requirements.

OBLIGATIONS FOR REPORTING

Lucky Star maintains a robust internal reporting framework to ensure timely detection, escalation, and documentation of any activities or transactions that may be associated with money laundering (ML) or terrorist financing (TF).

Immediate Internal Reporting Obligations

All unusual activities or transactions—including **attempted transactions**—must first be **reported internally**. Any staff member responsible for transaction monitoring is obligated to notify the Compliance Officer **immediately upon identification** of a suspicious or unusual transaction. The report must include:

- A clear description of the activity or behavior observed;
- Any immediate mitigating actions taken.

Staff Training and Awareness

All employees with customer-facing roles or access to customer data undergo **mandatory anti-money laundering training**. This training equips them to:

- Recognize suspicious behavior patterns and transactional anomalies;
- Understand indicators of possible ML or TF activities;
- Act on any knowledge, suspicion, or reasonable grounds to believe that a customer is attempting to use Lucky Star for illegal purposes.

If a staff member suspects or knows that customer activity may involve the proceeds of crime, they must file an **Internal Unusual Activity Report (IUAR)** with the Compliance Officer. This ensures that the employee has fulfilled their legal and regulatory reporting duties.

Timing Requirements for Internal Reporting

- Employees must submit an IUAR to the Compliance Officer **without delay and no later than 24 hours** after the execution of the relevant transaction or activity.
- If additional investigation is required, the Compliance Officer will initiate a **compliance review**, to be concluded **within ten (10) business days**.
- During the review period, the Compliance Officer may request supporting documentation or clarification from operational or customer support teams.

External Reporting to the Financial Intelligence Unit (FIU)

If, upon completion of the review, the Compliance Officer determines that the activity meets the threshold for external escalation, a **formal report will be submitted to the FIU Curaçao**.

- In cases involving **objective indicators** (e.g. exceeding monetary thresholds, links to sanctioned persons/entities), the report must be filed with the FIU **within 48 hours of the transaction**.
- For all other reportable cases deemed “unusual,” the Compliance Officer will also file a report **within 48 hours of concluding that the activity is suspicious**.

This dual-layered approach ensures full alignment with Curaçao’s AML/CTF regulatory obligations and promotes a culture of transparency, accountability, and prompt response to financial crime risks.

PROHIBITION OF DISCLOSURE

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

Lucky Star has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

KEEPING RECORDS

Lucky Star retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years. This ensures compliance with regulatory requests and allows for the reconstruction of individual transactions, including amounts and types of currency involved, when applicable, which may be needed for potential criminal investigations.

All documents collected through Customer Due Diligence (CDD) measures, such as copies of official identification, account files, and business correspondence, will be stored for at least five (5) years after the end of the business relationship or after the date of an occasional transaction.

Records are maintained in a manner that ensures their integrity, confidentiality, and accessibility, with access restricted to authorized personnel only. Electronic records are regularly backed up and stored in a separate secure location to prevent data loss.

After the retention period expires, records are securely disposed of to prevent unauthorized access or disclosure.

When properly requested by law, regulation, or court order, the Company shall provide documents, customer due diligence information, or enhanced due diligence materials as required.

8. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

COMPLIANCE OFFICER APPOINTMENT

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

Compliance Officer's Duties

The Compliance Officer shall be assigned the following key responsibilities:

- Designing and implementing the AML program.
- Ensuring compliance with local laws and regulations related to the detection and prevention of money laundering and terrorist financing.
- Reviewing adherence to the Company's policies and procedures.
- Organizing staff training sessions on various compliance-related topics.
- Analyzing transactions to determine if they meet reporting criteria based on the Ministerial Decree's indicators for unusual transactions.
- Reviewing all internally reported unusual transactions for completeness and accuracy, cross-checking with other sources.
- Maintaining records of both internally and externally reported unusual transactions.
- Conducting further investigations into unusual transactions when necessary.
- Preparing external reports of unusual transactions.
- Making necessary updates and improvements to the AML program.
- Staying informed on local and international developments regarding money laundering and terrorist financing, and recommending improvements to management.
- Preparing periodic reports on the Company's efforts in combating money laundering, terrorist financing, and proliferation financing.

AML MEASURES REGARDING EMPLOYEES

A. Due diligence

Employee due diligence is a process used to screen employees with the goal of identifying and minimizing Lucky Star's exposure to risks related to money laundering and terrorist financing. This process applies not only to the Company's direct employees but also to contractors and subcontractors. The scope and depth of due diligence are based on Lucky Star's risk assessment and the specific roles within the organization.

Any employee in a position that could potentially facilitate money laundering or terrorist financing must undergo screening. This applies to prospective employees before hiring, as well as to current employees

periodically. Regular updates and re-evaluations are crucial to maintaining an effective compliance program against money laundering, terrorist financing, and proliferation financing.

To screen current and potential employees, Lucky Star will:

- Identify the individual.
- Verify their identity.
- Confirm their employment history, including references.
- Assess their suitability for the role and evaluate any risks they may pose to the Company.

Positions that may make employees vulnerable to collusion or coercion by criminal organizations require more thorough checks. Lucky Star will evaluate whether the employee:

- Has a criminal record, verified through a police check.
- Is or has been subject to regulatory, judicial, or legal actions.
- Has used bankruptcy laws for personal gain.

B. Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

Lucky Star will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

Lucky Star will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

INDEPENDENT AUDIT

An independent audit function will be established to conduct an annual evaluation of the AML program. Qualified audit personnel will carry out the review, and all findings will be thoroughly documented.

The audit will cover key areas including:

- Reviewing the Company's AML, CTF, and CPF policies and procedures.
- Examining customer files to ensure compliance.
- Evaluating the effectiveness of compliance management.
- Testing transactions for adherence to AML standards.
- Assessing the adequacy and delivery of staff training.
- Verifying compliance with applicable laws and regulations.
- Reviewing the system's ability to detect unusual or suspicious activities.
- Interviewing employees involved in transaction processing and their supervisors.
- Sampling unusual transactions and checking compliance with internal and external reporting requirements.
- Evaluating the effectiveness of record retention practices.

Additionally, the audit will assess how effectively Lucky Star has addressed previous audit recommendations. All aspects of the audit scope and results will be documented, and any identified deficiencies will be reported to senior management, along with recommendations for timely corrective actions.

EXAMINATION BY THE CURACAO GAMING CONTROL BOARD

Lucky Star shall provide information and documentation related to its money laundering and terrorist financing policies and procedures to examiners from the GCB during inspections or upon request. The following materials must always be readily available and accessible:

- The approved and documented AML Compliance Program covering ML, TF, and PF.
- Records of the Company's Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that underwent further investigation.
- Records of any frozen accounts.
- A schedule of training sessions provided to staff on ML, TF, and PF.
- Assessment reports on the Company's AML/CTF/CPF policies and procedures from internal audits or external auditors.
- Customer files, including risk assessments, CDD documentation, customer acceptance details, and transaction records.

