

CLASSIFICATION: CONFIDENTIAL

ANTI-MONEY LAUNDERING (AML) AND FRAUD POLICY

REVISION HISTORY

Version Number	Date	Summary of changes	Author
1.0	01/06/2025	New Policy drafted	Edward Mackrill

Approved by:
Gouloud Hammoud, Director

POLICY STATEMENT

Luminect Limited B.V (Luminect) is committed to ensuring that it has in place effective policies, controls, and procedures to ensure its compliance with the regulations for the combating of Money Laundering, the financing of Terrorism, and The Proliferation of weapons of mass destruction issued in implementation of article 2, paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification (NOIS), article 22, paragraph 3 of the National Ordinance on the Reporting Unusual Transaction (NORUT), sanctions National Ordinance (SNO) and Kingdom Sanction Act, with Curaçao Gaming Authority (CGA) as the officially appointed supervisory authority.

Luminect recognises the risks that its gambling business faces and has produced this policy to demonstrate how it will comply with all legislation and associated regulators' guidance. In particular, this policy seeks to ensure that at all times Luminect:

- Upholds the licensing objectives set out by our regulator, particularly the prevention of money laundering, terrorism and fraud
- Ensures that all staff are trained thoroughly and on an ongoing basis in relation to preventing money money laundering, terrorism and fraud
- Conducts customer due diligence in an appropriate manner
- Conducts ongoing monitoring of all customers and transactions
- Implements an ongoing assessment of risk, both at a customer level and on a business level
- Has processes in place to effectively manage, control, communicate and ensure compliance with this policy and all associated procedures

- Assesses and reviews the effectiveness of this policy at board level (or equivalent)

GOVERNANCE AND BOARD OVERSIGHT

Luminect's board of directors holds ultimate responsibility for AML compliance. This policy and the supporting risk assessments (Business and Customer) are reviewed at least annually, or sooner where material risks or regulatory changes are identified. Each review is documented and formally approved at board level to ensure accountability and alignment with the Curaçao Gaming Authority's governance expectations.

OVERVIEW

This policy is intended as a point of reference for all staff, in particular the Compliance Officer, Money Laundering Reporting Officer ("MLRO"), other Senior Management, Auditors, the Head of Customer Experience and all customer facing staff.

It incorporates a number of references to guidance issued by the CGA and outlines Luminect's policies and procedures that underpin and support the Legislation.

It is essential that all employees fully understand and implement this policy, in particular the requirements for Customer Acceptance Policy (CAP) Customer Due Diligence ("CDD"), Enhanced Customer Due Diligence ("ECDD"), ongoing monitoring and unusual transaction activity reporting.

**COMPLYING WITH THE LEGISLATION IS
MANDATORY**

**RESPONSIBILITY IS BOTH INDIVIDUAL AND
CORPORATE**

WHAT IS MONEY LAUNDERING?

Money laundering covers wide ranging circumstances involving any activity concerning the proceeds of crime and may include:

- Trying to turn value (e.g. money) raised through criminal activity into 'clean' money
- Possessing or transferring the benefit of acquisitive crimes such as theft and fraud, and funds generated from crimes like tax evasion (this includes possession by an offender of the proceeds of his own criminal activity)
- Possession or transferring stolen goods
- Being directly involved with criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property

- Criminals investing the proceeds of their crimes in the whole range of financial products

The terms 'proceeds of crime' and 'criminal proceeds' refer to all property from which a person benefits directly or indirectly, by being party to criminal conduct, for example, money from drug dealing or stolen in a burglary or robbery. This also includes property that a person gains by spending the proceeds of criminal conduct, for example, if a person uses money earned from drug dealing to buy a car or house or spends money from a bank robbery to gamble.

WHAT IS TERRORIST FINANCING?

Terrorist financing is the act of providing financial support or resources to individuals or groups engaged in terrorist activities. The funds may be used to purchase weapons, recruit new members, or carry out attacks. Financial Action Task Force or FATF defines terrorism financing as the transfer of cash to terrorists or terrorist organizations to carry out terrorist acts.

The difference between money laundering and terrorist financing

There are significant similarities between the movement of terrorist property and the laundering of criminal property, however, there are also some key differences.

Often, only small amounts of money are required to commit individual acts of terrorism. This therefore increases the difficulty of tracking the terrorist property. Furthermore, terrorism can be funded from legitimately earned income. This makes it extremely hard to identify when legitimate funds become terrorist property.

In order to combat terrorist financing, we are under an obligation to report any suspicious and unusual transaction activity to the authorities, specifically the Financial Intelligence Unit ("FIU") in Curaçao. This will enable law enforcement agencies to investigate our suspicions and take requisite action if necessary, for example by freezing assets.

WHAT IS PROLIFERATION FINANCING?

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, including both technologies and dual-use goods used for non-legitimate purposes.

As such, should any Luminect employee suspect customer information or behaviour to be that of proliferation financing activity, they will follow the Unusual Transaction Report (UTR) procedures.

MONEY LAUNDERING REPORTING OFFICER AND OTHER RESPONSIBILITIES

The MLRO responsibilities include, but not limited to, designing and implementing the AML program, ensuring compliance with Curaçao laws and regulations, creating policies and procedures and organise staff training.

The MLRO is under a statutory obligation to consider any information received through our internal reporting procedures and determine, considering all relevant information known to him and the company, whether a specific transaction gives rise to grounds for knowledge or suspicion that a person is involved in money laundering and/or terrorist financing.

Upon any such determination, the MLRO has a further statutory obligation to consider whether a disclosure to the FIU is required. Such disclosures must be made as soon as practicable. Subject to when the internal UTR is received, the MLRO has set SLAs of acknowledging internal UTRs within 24 hours of receipt and completing the review of those internal UTRs within 48 hours of receipt.

Luminect's MLRO has the overall responsibility for dealing with money laundering-related issues on behalf of the company. It is therefore important that in the event that any unusual transaction activity is identified, all areas of the business raise their concerns with the MLRO. Furthermore, all Unusual Transaction Reports (UTR) / Disclosure Forms must be sent to the MLRO at the email address mlro@luminect.com for consideration as to whether there is a need for formal disclosure to the FIU.

KEY COMPLIANCE FUNCTIONARY (KCF)

In accordance with the licensing conditions set by the Curaçao Gaming Authority (CGA), Luminect has designated a Key Compliance Functionary (KCF) responsible for ensuring adherence to all AML/CFT regulatory requirements.

The role of KCF is held by the same individual who also serves as the Money Laundering Reporting Officer (MLRO). This dual appointment ensures continuity and accountability across the compliance function. The appointed individual is qualified and empowered to act as the primary contact for the CGA and the Financial Intelligence Unit (FIU), and has direct access to senior management and the board.

RISK-BASED APPROACH

By adopting a risk-based approach Luminect ensures that measures to prevent and mitigate money laundering, financing of terrorism and proliferation of weapons is applied in policies, procedures and controls.

When applying the risk-based approach Luminect:

- Assess the risks of money laundering or terrorist financing occurring
- Implement appropriate policies, procedures and controls
- Monitor and improve the effectiveness of the policies, procedures and controls
- Document the risk assessment conducted

Risk factors specific to the Gambling Sector are:

- Customer risk
- Geographical risk
- Product, Service and Transaction risk
- Delivery Channel risk

Luminect undertakes both Business Risk Assessment and Customer Risk assessment. Undertaking risk assessments is not a one-off exercise. It is an ongoing responsibility that should be repeated and updated frequently such that we can ensure that we are considering all information available to us on each occasion.

BUSINESS RISK ASSESSMENT (BRA)

Luminect undertakes a Business Risk Assessment and assesses it at least once a year to evaluate if any changes are required with consideration the outcomes of the National Risk Assessment of the jurisdictions we operate in. It is also assessed and revised whenever there are changes to the risk environment, such as new payment methods, new markets, regulatory news and/or changes and technological developments.

The BRA is documented and approved by the board of directors/ senior management.

The Business Risk Assessment is covering:

- The methodology adapted
- The reasons for considering a risk as a low, medium or high risk
- The outcome of the BRA
- Any information sources used

CUSTOMER RISK ASSESSMENT (CRA)

Luminect carry out Customer Risk Assessments on its customers throughout the different stages of the business relationship. The CRA will assess the particular risks Luminect will be exposed to providing its products to the customer and create a risk profile that will be considered to determine the proper level of Customer Due Diligence check to be conducted.

Further details are found in the Customer Acceptance policy below.

CUSTOMER ACCEPTANCE AND CUSTOMER DUE DILIGENCE (CDD)

Business Relationship

The establishment of a business relationship brings with it a number of obligations. We consider a business relationship to have been formed when:

- A customer opens an account with us, and/or:
- When we start to track a customer's gambling data.

Customer Due Diligence

We are required to apply CDD measures when we:

- Establish a business relationship

- Know or reasonably suspect money laundering and/or terrorist financing
- Doubt the veracity or adequacy of documents, or of information previously obtained for the purposes of identification or verification
- In relation to any transaction that amounts to NAf. 4,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked
- At other appropriate times to existing customers on a risk-based approach
- Whenever we become aware that the circumstances of an existing customer relevant to our risk assessment have changed

We are also expected to take the following into account when determining when it is appropriate to apply CDD measures to *existing* customers:

- Any indication that the identity of the customer, or of the customer's beneficial owner, has changed
- Any transactions which are not reasonably consistent with our knowledge of the customer
- Any change in the purpose or intended nature of our relationship with the customer
- Any other matter which could reasonably affect our assessment of the money laundering or terrorist financing risk in relation to the customer

We have introduced the following steps to ensure that we are complying with our obligations to conduct CDD:

Duplicate accounts

We only allow customers to create one account with us per site. This account must be in their own name. We do not accept corporate accounts or accounts created on behalf of someone else.

We have a number of controls in place to help us to identify duplicate accounts, which seek to identify matches in First Name, Last Name, DOB, IP and Payment method.

Any duplicate accounts identified will be closed in line with our terms and conditions.

Identification and age verification

When a customer registers with any of Luminct's online gaming websites at a minimum the following information is collected to identify the customer:

- Full name
- Permanent residential address (including country of residence)
- Date of birth

In high-risk scenarios at a minimum below further information will be collected:

- Place of birth
- Nationality
- Identity number

When a customer makes the first deposit, we will screen against PEP, Sanctions and Adverse media databases and a provisional risk rating will be assigned based on the information provided. This is explained in more detail below.

Where verification of the above information is necessary, customers will be prompted to upload Proof of Identity ("POI") and Proof of Address ("POA") documents to our website which will then be sent to our Customer Experience team for manual verification. For more details on acceptable documentation please see **Appendix 1**.

Payments

Luminect will only accept payments from accounts held with financial institutions or through payment providers and does not accept cash deposits/withdrawals, transfers between accounts or offer credit to customers. We will also block any card issued from a FATF high risk jurisdiction.

It is not permitted to deposit from accounts not in the customer's name.

Crypto Assets (Digital Currencies)

At present, Luminect does not accept payments or withdrawals via cryptocurrencies. Should this policy change in the future, we will introduce appropriate safeguards in line with FATF guidance, including the use of blockchain tracing tools, implementation of the Travel Rule, and specific KYC measures for crypto wallet ownership. The AML policy will be updated accordingly and submitted to the CGA for approval.

Closed Loop

Luminect operate a 'Closed Loop Policy' when it comes to withdrawing funds. Customer's depositing into their account using one payment method will be forced by our system to withdraw back onto that same payment method.

In circumstances where it is not possible to return funds to a customer's deposit method, we will make all reasonable efforts to process withdrawals directly to the customers via bank transfer.

Ongoing CDD

We are under an ongoing obligation to monitor our customers after establishing a business relationship with them. Consequently, even if a customer has met minimum CDD Requirements, it is essential that we review their account regularly with a view to applying additional CDD measures.

To support this approach, we have introduced a number of triggers to ensure that we have a risk-based approach to CDD. These triggers will ensure a high standard of ongoing monitoring and must be reviewed by the MLRO on a regular basis.

We outline these triggers and the expected actions in the table below:

CDD Trigger	CDD Trigger Criteria	Action Required
NAf. 4,000 threshold	NAf. 4,000 in cumulative transactions	Complete Customer Risk Assessment (see Appendix 2) including PEP/Sanction check. Review account and request POI, POA Do not process withdrawals until received.
NAf 5,000 or more threshold	Daily transactions of NAf 5,000 or more	MLRO to complete a Risk Profile Review on the account to determine if UTR is required. Account not restricted unless deemed necessary
Deposit not wagered	Customer has made a withdrawal > NAf 1,000 (or equivalent amount in local currency) but has not placed bets to the value of their last deposit	Review account and consider whether any additional documentation is required. Do not process withdrawals until received.
Any ECDD trigger	As defined below under Enhanced Customer Due Diligence (ECDD)	ECDD required (see below) Review account and request POI, POA and copies of payment methods in use (if not already held). PEP/Sanction check.

If the requested information and documentation has not been received within 30 days from when the NAf 4,000 threshold triggered, the account will be fully restricted, and the transaction is reported to FIU if presumption of money laundering or terrorist financing exists.

Customer Risk Assessments

All new customers by default will be rated LOW risk. At the point a customers' transactions with us meet our NAf 4,000 CDD threshold it is essential that a **Customer Risk Assessment** is completed (see **Appendix 2**).

The completion of the risk assessment is straightforward. A weighted score will be given to each category. These scores will then be added together to calculate an overall risk score and a rating of LOW, MEDIUM or HIGH will be awarded to the customer. These risk ratings will be considered during future assessments and will determine the level of authorisation required.

Customer's rated HIGH risk at this point must be escalated to the MLRO immediately who will decide whether ECDD is required, or whether we wish to terminate the business relationship.

Customer Risk Assessments will be repeated whenever one of our ECDD triggers is hit (see below)

Any customers receiving a positive PEP match will be automatically rated as HIGH risk – this rating can only change if the customer is no longer considered a PEP.

Risk Profile Review

A Risk Profile review (see **Appendix 3**) must be completed by the MLRO following specified CDD and ECDD triggers, regardless of whether we decide to take any action.

The Risk Profile Review will contain the following:

- Customer Risk Rating (completed at NAf 4K threshold)
- Account details
- Financial activity
- Details of CDD/ECDD collected
- A review of gameplay
- A decision as to whether to continue with the business relationship
- A decision as to whether an Unusual Transaction Report (UTR) is required

ENHANCED CUSTOMER DUE DILIGENCE (ECDD)

We are required to conduct ECDD in instances where there may be a heightened risk of money laundering or terrorist financing. We have considered the Legislation and reached the view that ECDD should be conducted in the following circumstances:

- When a customer is identified as a Politically Exposed Person (“PEP”), or a close associate of a PEP
- In circumstances where we discover that a customer has provided false or stolen identification documentation or information and we propose to continue to deal with the customer
- In circumstances where a transaction is complex or unusually large, or where the relationship by its nature is considered to be one that presents a high risk
- In any case which, by its nature, can present a higher risk of money laundering or terrorist financing
- In any case where we have cause for concern about changes in the customer’s nature of play,
- which have not been addressed by further CDD measures

We have introduced the following steps to ensure that we are complying with our obligations to conduct ECDD.

ECDD thresholds

Any customer, regardless of their level of play, may represent a higher risk of money laundering and/or terrorist financing such that the completion of ECDD is required. It is therefore critically important that all staff remain vigilant and monitor accounts for signs of any behaviour which raises suspicions of money laundering, terrorist financing or proliferation financing.

However, as a minimum, we consider that ECDD must be recorded where the customer has deposited a total of NAF 200,000 in the lifetime of their account. Once this threshold has been reached, the MLRO will receive an alert and determine what ECDD measures should be applied. This may include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

If, after a period of 1 month, ECDD checks have not been completed the customer's account will be closed.

Record of Conversations

On each occasion a conversation takes place with a customer in relation to ECDD it is important full transcripts are recorded. This will form part of our assessment process and evidence our adherence to prevention of money laundering and combating the financing of terrorism obligations.

For recording purposes, a conversation may take place orally, by email, by customer chat, by SMS or by WhatsApp. Details of these conversations will be referred to on the Risk Profile Review document.

Ongoing ECDD

In some instances, we may also become aware that a customer's circumstances have changed. For example:

- If we submit a UTR
- If we receive a notification from LexisNexis that a customer has been flagged during ongoing monitoring

In such cases, the MLRO may request that further ECDD be completed.

As part of all ECDD checks, two documents must be completed – a **Customer Risk Assessment (Appendix 2)** and a **Risk Profile Review (Appendix 3)**.

RETENTION OF ALL CDD/ECDD AND ASSOCIATED RECORDS

We are required to retain all records relating to CDD/ECDD for a minimum period of 5 years following the date that a business relationship ends. More information about retention periods can be found in our Privacy Policy.

POLITICALLY EXPOSED PERSONS (PEP's), SANCTION LIST

We have decided as a business that we will screen all customers against the Lexis Nexis PEP, Sanctions and Adverse Media database on first deposit.

Where a positive PEP or Sanctions match is identified, the customer's account will automatically be blocked and a decision taken as to whether to continue with the business relationship.

PEPs, PEPs by association, CEPs & SIPs

A PEP is an individual who is (or has at any time in the preceding year) been entrusted with prominent public functions (other than middle-ranking or more junior officials), an immediate family member of such person, or a known close associate of such person.

This status does not mean that these individuals cannot be transacted with, however it does place them into a high-risk category.

Examples of PEP's include:

- Heads of state, heads of government, ministers or other senior government officials
- Senior members of the judiciary/ Senior military officers

PEPs are of a status and position which increases the risk of money laundering. For example, through the risk of diverting government/public funds or through an involvement in bribery or corruption.

We are therefore required to ensure that we have appropriate systems and procedures in place to determine whether a customer is a PEP.

A person is no longer regarded as a PEP after they have left their office for one year. However, we will still apply a risk-based approach in our dealings with customers who have been identified as PEPs for the duration of our relationship.

PEPs by association are individuals linked to a PEP who share a family or friendship connection, alternatively, it may be a social or professional association.

Certain individuals may not be formally classified as a PEP but the nature of their business may make them a Commercially Exposed Person ("CEP"). Although such customers generally do not pose the same risks of money laundering as PEPs, it is important these are also escalated to the MLRO once identified.

Special Interest Persons ("SIPs") are individuals allegedly involved in criminal activity that fall under one of the following six categories:

- Corruption
- Financial crime (including Tax crime)

- Human trafficking / Organised crime

IMPORTANT: The business does not have the risk appetite to have confirmed SIPs, PEPs nor PEPs by association as customers. Acceptance of CEPS as customers will be treated on a case-by-case risk based approach depending on the outcome of any ECDD conducted.

It is important that all staff remain alert to situations which may suggest that a customer is a PEP, PEP by association, CEP or SIP. These situations may include:

- Receiving funds from a government account
- Correspondence on an official letterhead from the customer or related person
- General conversations with the customer
- News reports

Steps to take when dealing with PEP's

If a PEP has registered and already been prevented from depositing and playing by the system, the account will remain blocked pending further instruction from the MLRO

If you suspect that someone may be a PEP the MLRO should be notified immediately

The MLRO should consider whether there is a need for formal disclosure to the FIU.

Sanctions

Curaçao operate financial sanctions on persons and entities following their designation at the United Nations and/or European Union, and a domestic counter-terrorism regime, where the Government decides to impose financial restrictions on certain persons and entities. These restrictions are governed by various legislation; in circumstances where an asset freeze has been imposed it is unlawful to make payments to, or allow payments to be made to, designated persons.

By undertaking screening, we will ensure that we are not transacting with any such customers.

Ad-hoc searches of the LexisNexis' Compliance lens, PEPs, CEPS, CEPS, Sanctions and Adverse media database can be requested at any time by emailing the MLRO. For example, such checks may be warranted in circumstances where the following are identified:

- Individual or linked transactions which are complex or unusually large with no apparent economic or lawful purpose, including those relative to a relationship
- Unusual patterns of transactions with no apparent economic or lawful purpose, including those relative to a relationship
- Transactions which exceed our triggers and which have no apparent economic or lawful purpose, including those relative to a relationship
- Very high account turnover on an account that is inconsistent with balance

- Transactions which are significantly outside a customers' regular transaction activity

Ongoing monitoring

PEP & Sanction screening should not be a one-off event as the information held on these databases changes frequently. To mitigate this risk, all customers will be added to the LexisNexis' Compliance lens ongoing monitoring database and checked against PEP & Sanction databases every 24 hours.

Automated Monitoring Tools

Luminect uses a combination of manual reviews and automated tools to monitor for suspicious activity, particularly in relation to customer payments and financial behaviour. Our automated systems flag key risk indicators such as deposit anomalies, mismatched payment details, and high-volume transactions.

While gameplay and behaviour monitoring is primarily conducted manually by the Compliance and Risk teams, all alerts — whether system- or staff-generated — are reviewed and escalated to the MLRO where appropriate.

This hybrid approach ensures that high-risk activity is detected promptly while maintaining flexibility in how complex or context-specific behaviours are assessed.

REPORTING SUSPICIOUS / UNUSUAL TRANSACTION ACTIVITY

All staff are under a legal obligation to report any activity which they come across in the course of business that gives rise to knowledge of or a reasonable suspicion of money laundering and/or terrorist financing immediately to the MLRO. Such reports should be made on the UTR template (see **Appendix 4**). It is important that as much information as possible is provided when completing the UTR, particularly the reasons for the suspicion.

Once a UTR has been submitted, the MLRO will conduct an investigation and decide whether any additional information is required, what should be communicated to the customer and what action needs to be taken. Consideration will be given as to whether the UTR needs to be reported to the FIU and regulators notified accordingly.

It is not acceptable to complete a UTR on a customer due to a lack of ECDD and then simply continue the business relationship. ECDD must either be obtained or the business relationship terminated.

The MLRO must be informed prior to terminating any business relationship due to a lack of ECDD.

It is important that the reporting of UTRs is kept as confidential as possible, to avoid the risk of 'tipping off'.

Confidential records of all reported UTRs are kept by the MLRO.

Identifying Unusual Transactions

Identifying unusual transactions is key to the prevention and detection of money laundering.

All employees are required to make a report in respect of information that comes to them in the course of business:

- Where they know
- Where they suspect
- Where they have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing, including criminal spend, or attempting to launder money or finance terrorism.

It is impossible to provide a definitive and exhaustive guide to suspicious and unusual transaction activity. However, some examples may be:

- A customer who submits CDD documentation to us that we believe to be fraudulent
- A customer who deposits large amounts and after minimal play where significant funds have not been put at risk, seeks to withdraw the remaining funds
- A customer betting on both sides of an even chance bet at roulette
- A customer who changes their deposit methods (frequently changing bank accounts, debit cards, using foreign banks or requesting withdrawals to different sources).
- A customer whose style of play is significantly different to their usual style of play we would expect
- Atypical or uneconomical fund transfers from foreign jurisdictions
- Numerous accounts or attempts to open numerous accounts
- Level of funds incompatible with our knowledge of the customer's legitimate wealth
- Customers structuring their transactions such that they fall just below our trigger limits on frequent occasions
- Cashless transactions in the amount of NAF 5,000 or more (singular or multiple transactions), such as deposit or cash out.

All employees have a legal defence if they report to the MLRO where they have grounds for knowledge or suspicion of money laundering or terrorist financing. It is therefore important that this action is taken where such grounds exist.

TIPPING OFF

Once an internal or external report of unusual transaction activity has been made, it is a criminal offence to release information that is likely to prejudice an investigation that might be conducted following the disclosure.

This means that we can't disclose any details or information in connection with a report filed to the FIU. Caution is also to be taken if decision is to end the business relationship or otherwise block additional transactions. In such circumstances we will consider increased monitoring and submitting further reports to the FIU to avoid potential tipping off due to action taken on the account.

EMPLOYEE SCREENING AND ONGOING TRAINING

It is important to note that money laundering offences can be committed by both the customer and our own employees, depending upon their levels of knowledge or suspicion.

We use HireRight to screen all new employees prior to joining the business. These checks verify the data that candidates have provided in their CV's, applications, background forms and/or interviews.

Employee screening will be repeated as follows:

- When we appoint someone to a key position, as defined by our regulators
- After 5 years of continuous employment
- On the request of our MLRO

All customer-facing staff receive an enhanced internal on-boarding training and yearly refresher training. This training gives an overview of Luminct's approach to AML/CFT.

We also offer ad hoc training. This may be in the form of using a third-party provider to host and deliver the training, or an e-Learning course which can be completed. Records of attendance are kept on file.

INDEPENDENT AML REVIEW

To ensure continued compliance and operational integrity, Luminct's AML framework is subject to independent audit or internal review at least every 18 months. The findings of such audits are documented and presented to the board and, where applicable, shared with the CGA as part of ongoing supervisory engagement.

BRIBERY AND CORRUPTION

Bribery and corruption are serious offences that can lead to significant legal, financial, and reputational damage. It is therefore crucial that we take steps to address this risk.

Luminct prohibit all forms of bribery and corruption, including but not limited to:

- Offering, promising, giving, or accepting any bribe, kickback, or other improper payment or benefit, whether in cash or in kind, to any person, including public officials, to influence their actions or decisions.
- Using any improper means to obtain or retain business, including through the use of gifts, hospitality, or other benefits.

- Concealing or disguising the true nature, source, location, ownership, or control of any assets or funds.
- Failing to maintain accurate records, or making false or misleading entries in any record.
- Engaging in any other conduct that may constitute a violation of anti-bribery or anti-corruption laws or regulations.

Due Diligence

Luminect are committed to conducting due diligence on all employees, agents, and third parties who act on our behalf. This includes:

- Conducting background checks to verify their identity, qualifications, and reputation.
- Assessing their exposure to bribery and corruption risks.
- Monitoring their activities and transactions to detect any potential red flags.

Reporting suspicions

All employees are trained to report any concerns or suspicions of bribery or corruption to the MLRO immediately who will investigate all reports promptly (acknowledge within 24 hours of receipt and completing the review within 48 hours, subject to time of receipt), thoroughly, and impartially. We will take appropriate remedial action if we find any violations of this policy or applicable laws or regulations.

APPENDIX 1 - Acceptable documentation

Type	Examples
POI	• Passport / Driving Licence • National Identity Card
POA	• Utility bill (gas, electric, satellite television, landline phone bill) issued within the last six months • Local authority council tax bill for the current council tax year • Valid Driving Licence displaying address (if not already used for POI) • Mortgage Statement from a recognised lender issued for the last full year • Solicitors letter within the last six months confirming recent house purchase or land registry confirmation of address • House or motor insurance document
Payment Methods	• Front and back of card • Bank letter or statement confirming ownership of the card • Bank statement confirming ownership of bank account
SOE	• Full, unredacted bank/E-wallet statement (issued in the last 3 months) showing deposits made
SOW - Employment	• Copy of payslip • Confirmation of employment (e.g.employment contract or letter from HR)
SOW - Property Sale	• Copy of contract of sale / Written confirmation of sale • Bank Statement showing funds from sale
SOW - Inheritance	• Copy of Will or Grant of Probate • Written confirmation of inheritance signed by advocate/solicitor/trustee/executor
Savings	• Full, unredacted savings account statement issued in the last 3 months.
Lottery/Jackpot win	• Evidence of win / Winnings receipt • Bank statement showing receipt of funds from win

APPENDIX 2 – Customer Risk Assessment

Customer Risk Assessment		Score
Geographical Risk	Other Jurisdiction (0) FATF High-Risk Jurisdiction (5) Embargoed or Sanction Country (10)	
Payment Method	Debit/ Credit Card (0) Bank transfer (0) E-wallet (2) Third party payment method (5) Cash/ pre-paid card / Virtual currencies (10)	
Type of Customer	Verified with 1 account (0) Not verified / lack of documents received (2) VIP (2) PEP/SL (10)	
Transactional Risk	No concerning transactions, rounded amounts (0) Transactions of irregular values (2) High number of low value transactions in a short period of time (5) Low number of high value transaction (5)	
Gameplay Risk	Slots (0) Sports / Table games (1) Peer-to-peer games (5)	
0-4 = LOW 5-9 = MEDIUM 10+ = HIGH	Total score	

APPENDIX 3 – Risk Profile Review

ACCOUNT REVIEW	
CUSTOMER NAME	
USER ID	
NAME / USERNAME / EMAIL CHECK	
DUPLICATE SEARCH	
THRESHOLD TRIGGERED	
TRIGGER DATE	
REVIEW DATE	
REVIEWING AGENT	
CUSTOMER RISK SCORE & RATING	
NEW Customer Risk Score:	
NEW Customer Risk Rating:	LOW/MEDIUM/HIGH
ACCOUNT DETAILS	
REGISTRATION DATE:	
<i>Past 12 months:</i>	
Net Deposits: £	
Net Loss: £	
<i>Last Month:</i>	
Net Deposit: £	
Net Loss: £	
VERIFICATION	
ID Uploaded:	
POA Uploaded:	
ENHANCED DUE DILIGENCE CHECKS	
PART 1: ONLINE REVIEW	
Searches conducted:	
Outcome of review:	
PART 2: SOF & SOW (IF REQUIRED)	
Provided:	
Shows SOF/SOW received	
Shows SOF deposits to SpaceCasino	
SOW check:	
AML CONSIDERATIONS	
PEP & Sanctions:	
High-Risk Jurisdiction:	
Product played risk: (P2P Poker not offered)	

Monitored for AML triggers/indicators:	
AML Play Behaviour:	
OSINT	
Google Name + City/Town:	
Google Name + Key Search Terms:	
Facebook:	
Instagram:	
TikTok:	
LinkedIn:	
CLOSED LOOP	
Has the customer had any withdrawals?	
Have the withdrawals been made to the same deposit method?	
Have the withdrawals been made to the same deposit method?	
CONTINUE BUSINESS RELATIONSHIP?	YES/NO
UTR NEEDED?	YES/NO
AUTHORISED BY	
Name:	
Position:	
Date:	

APPENDIX 4 – UTR Template

Unusual Transaction Report

Customer details:

User ID	
Full name	
Address	
DOB	
Gender	
Occupation (if known)	
Email	
Phone number	
Account status	
Registration date	
Last log in	
Balance on account (including pending WDs)	

Reason for your suspicion (provide as much information as possible, use second page if needed)

--

Your name:

Date:

Completed Unusual Transaction Reports should be emailed to mlro@luminect.com