

Know Your Customer Policy

Crayon B.V.

1. Customer Risk Assessment (CRA)

After the identity verification of a client, a risk profile is formed based on the clients' behavioural patterns. This behavioural pattern is examined through the transaction activity and the type of game-play the client opts for. The CRA is also carried out throughout the business relationship.

After the behavioural pattern is analysed, every customer is given an internal classification as defined by the Customer Risk Assessment (CRA). If suspicious behaviour is observed, evidence will be recorded on the customer profile, and Enhanced Due Diligence (EDD) is applied.

Customers undergo an ongoing ML/FT Risk Assessment from the start of the business relationship and thereafter based on:

- customer type;
- products/services used (e.g. sportsbook);
- transactions/payment systems;
- delivery channels; and
- geographical origin of the customer and/or payment method.

Upon registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to establish a risk profile, which is essential to enable the operator to apply a certain level of Customer Due Diligence (CDD), commensurate to the ML/FT risk posed. This monitoring is maintained, and the risk level may be reconsidered, depending on changes in customer's activity and to establish the point of reaching the relevant due diligence requirements thresholds. A customer's risk profile is key in obtaining relevant information pertaining to the customer, and maintaining a constant diligence on customer risk.

On the basis of the CRA the appropriate level of CDD can be applied, as stipulated in

the Client Acceptance Policy (CAP).

2. Client Screening

An overview of the Client screening is provided in this policy; kindly also refer to the PEP, Sanctions and Negative Media Policy for more information.

As a licensed entity, the company recognizes the importance of the customer profile and has in place practices to comply with the laws and regulations concerning identification, verification and screening of the Client for sanctions, political exposure and negative media . Upon initiation of the first deposit within the account registration, the Client will be immediately screened using a third party provider being Dilisence and block any Clients who are a positive PEP, Sanction or negative media match. Following registration, the company's list of Clients is automatically scanned by Dilisence on a weekly basis .

Positive matches and those Clients who cannot be discounted as a positive match on the information provided by Dilisence shall be investigated through open sources to obtain further information about the match and immediately inform the MLRO by following internal reporting procedures. The MLRO may appoint anyone within the department to investigate such matters. The company reserves the right to request further documentation concerning any possible match in order to verify or discount the suspicion. If a positive match is confirmed due to the match meeting several criteria, such matches will be reported to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Nationality

The MLRO has the responsibility of ensuring that the screening is being carried out as instructed; to achieve this, sampling of the data shall be carried out and recorded accordingly.

2.1 PEP / Sanctions Lists Checks

Customers are also to be screened to confirm that they are not included on Sanctions Lists. Customers are asked on first deposit to confirm whether the customer is him/herself, or is a family member of, or known associate to, a person that is considered a Politically Exposed Person ("PEP"). The customer is further checked to confirm PEP status once the relevant thresholds are hit, or the customer's profile is considered to be higher than low risk. PEP screening is carried out prior to the initial engagement.

Customers matching any one of these categories are to be automatically considered as a high-risk profile and appropriate measures taken to ensure that the business

activity with them is not of an ML/FT nature. Sanctioned individuals cannot be accepted as customers. Refer to **PEP / Sanctions Lists Procedure** and **Customer Acceptance Policy**. PEP and Sanctions List checks will be carried out against the software Dilisence

It is the reporting entity's responsibility to perform ongoing checks of its client database against the international lists of designated persons/ entities/ groups to make sure the reporting entity is not permitting/ facilitating access to funds to the ones mentioned on the sanctions lists. The primary sanctions list reporting entities must check against are UN, EU, USA-OFAC lists (expanded below), local lists of all jurisdictions where online gaming and gambling activities are provided and/or clients are accepted, and/or any other lists applicable at present, and/or which may become applicable from time to time.

Instances of sanctions screening:

- during initial client/player registration;
- daily;

The Company shall ensure that it shall not do business with terrorists or suspected terrorists, or other sanctioned persons or companies. Published lists should be checked, being as follows;

- US Treasury Office of Foreign Assets Controls Specially Designated Nationals and Blocked Persons Lists
- EU sanctions lists
- For PEP's: Transparency International Corruption Perceptions Index/ www.knowyourcountry.com

Although due diligence is required for every PEP, as measures required may vary, and the level of diligence is different according to scenarios, such as:

- Type of function carried out by the PEP
- The country from which the PEP originates
- The transactions that the PEP carries out

In the case of PEP's, the following checks are carried out:

2.2 Negative Media

Negative media shall be deemed as information or intelligence, whether proven factual or alleged, related to serious financial crime, Terrorism, fraud, narcotics, or any crime that has an element of or could lead to ML/FT. Negative Media Screening is to be conducted when establishing a business relationship with a Client. Instances where a Client is connected to Negative Media, will be evaluated prior to granting a business relationship.

When analysing Negative Media hits, we are looking at individuals that are both convicted and not fully convicted, meaning; allegations, cases under investigation pending the legal procedure, wanted individuals and any intelligence which gives rise to knowledge or suspicion that the Client is involved with ML/TF.

Negative Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offence raise concerns, they shall be raised with the MLRO or Deputy accordingly.

Negative Media is categorised as follows:

i) Financial Crime

2.2.1 Financial crime covers a wide range of activities, including ML and the FT. It may also include fraud, bribery, or insider trading. Financial crime is a broad and complex criminal field that may be covered in both traditional and emerging media.

ii) Violence

2.2.2 Violence involving Clients directly, or carried out on their behalf, may generate significant different types of adverse media, especially when part of a criminal enterprise. Violent crimes may be associated with political and workforce disputes, or wider patterns of human rights abuse.

iii) Terrorism

2.2.3 The financing of terrorism, any terror-related activities are liable to generate significant adverse media across a range of media outlets. Terror-related types of adverse media may range from the distribution of terrorist literature and encouragement to radicalization, to the direct perpetration of terrorist acts.

iv) Fraud

2.2.4 Fraud can be perpetrated in numerous ways and includes fraudulent letters, telephone calls, emails, and websites. Fraud can be both a civil and criminal offence and, while the majority of cases involve improper financial gain, it may also involve property or immigration.

v) Narcotics

2.2.5 Narcotics crimes involve not only the use or sale of drugs but also drug production and trafficking. Narcotics offences and associated news stories are often related to financial crimes, including ML and FT.

vi) Cybercrime

2.2.6 Any criminal activity involving a computer or networked device like a phone or tablet may be considered cybercrime and reported as such. Cybercrime is an umbrella-term describing activities used to facilitate other offences like digital financial crime, ML, fraud, and terrorism.

vii) Regulatory

2.2.7 Regulatory misconduct or non-compliance may constitute a crime in itself, or be an indication that Clients are involved in other types of criminal activity. The types of adverse media stories relating to regulatory offences frequently cross-over with financial crime.

viii) Property

2.2.8 Adverse media stories on property may involve activities such as burglary, theft, larceny, and arson, and constitute both civil or criminal misconduct. Property offences may vary greatly in scope and be reported in a wide variety of news media formats.

ix) Trafficking

2.2.9 Trafficking involves the transport of humans for the purposes of forced labour or sexual exploitation. A serious criminal offence, trafficking is often related to other offences, including terrorism and various financial crimes.

x) Sexual Crimes

2.2.10 Sexual crimes include a wide range of activity, from violence, abuse, and rape to the transmission or possession of illegal imagery. Sexual crimes are often in proximity to other offences, including ML and cybercrime.

Any of the offences indicated above, whether convicted or alleged, shall be evaluated and terminated accordingly if the media is deemed to be a positive match.

3. Risk Factors specific to the Gambling Sector

There are 4 risks which the BRA and CRA cover as a minimum. These are:

Customer risk

This is the risk of ML/FT which arises from maintaining relations with a given person. The assessment is generally based on the individual's economic activity and/or Source of Wealth (SOW). categories of customers who may pose a higher risk are as follows:

- Customers having multiple sources of income
- Customers with irregular income streams
- PEP's
- High spenders (as money can be derived from illegal activities)

- Disproportionate spenders (spending is inconsistent with the Company's knowledge of the individual's SOW)
- Improper use of third parties, use of others to avoid CDD measures and scrutiny
- Unknown customers
- Junkets

To this end, the Company sets an upper value of the customer's probable spending power, which if reached, will trigger further checks.

Geographical risk

This is the risk posed to the Company by the geographical location of the player and the SOW of the business relationship. Nationality and place of residence must be taken into account as the player may hail from a jurisdiction having lax AML laws, and also being a haven for terrorists. The Company consults the following sources for further information on the risk the player may pose;

- Countries on FATF list of high-risk jurisdictions subject to a Call for Action
- Countries on FATF list of jurisdictions under increased monitoring
- Countries on CFATF public statement
- Countries identified as jurisdictions of concern or primary concern in the US Department of State annual international narcotics control strategy report (INCSR).
- Countries on the European Commission list of third countries having strategic deficiencies in their AML/CFT regime
- Countries sanctioned by OFAC
- Countries identified by credible sources as hosting terrorist organisations within them
- Countries on the corruption perception index (Transparency International)
- The MLRO compiles a list of countries considered as high risk or low risk.

Product, Service and Transaction Risk

Some products are riskier than others, and pose a higher chance of ML/FT occurring through their use, through the use by customers and the acceptance of the company of specific payment methods. These include:

- Proceeds of crime - money from narcotics, theft etc
- Anonymous payment methods (such as use of Virtual Financial assets etc)
- Use of the operators accounts - these are only allowed to be used for gambling purposes and not to withdraw or deposit with minimal play
- Types of specific games (ex: roulette, craps).
- Use of customer accounts held in third party names
- Transfer of funds from one account to another
- Identity fraud

- Electronic wallets - not all e-wallets are licensed, and some jurisdictions accept deposits to e-wallets in cash.

The Company employs its best diligence in order to avoid situations such as the above from occurring within its corporation. The Company, together with the MLRO compiles a list of products which are considered as posing more of a high-risk, and employs measures in order to mitigate that risk, accordingly.

4. Risk Assessment - A dynamic approach

The Company conducts a risk assessment to assess ML/FT risks whenever a new product is introduced. This is done whenever:

- A new product is developed
- A new business practice emerges
- A new delivery mechanism becomes available
- A new or developing technology is used for both new and pre-existing products
- Targeting new markets

In such cases, a risk assessment takes place prior to the launch of a new product, business practice, delivery method, or the use of developing technology. This enables the Company to assess possible risk posed, and mitigate accordingly, or, decline to offer said new product.

Risk management is a continuous process carried out on a dynamic basis. Risk assessment is not an isolated event of limited duration. The MLRO shall undertake regular reviews of the characteristics of existing Clients, new Clients, services and the measures, procedures and controls designed to mitigate any resulting risks. These reviews shall be duly documented as per the Manual's requirements and form part of the company's Annual Money Laundering Report.

5. Customer Due Diligence

The Company does not allow accounts to be kept in anonymous or fictitious names. The Company identifies the player, asks for the player's name, and identifies the purpose for the business relationship. Without sufficient and concrete knowledge, the Company will terminate the relationship. The customer's risk profile is key for the Company to establish and maintain a business relationship whilst maintaining safeguards commensurate to the risk posed. Customer Due Diligence (CDD) is maintained throughout the relationship. This assessment is key in order to identify deviations from any expected behaviour. Any deviant behaviour is immediately reported to the Curacao FIU.

Customer Due Diligence (CDD) Measures include:

- collection of identification details;
- verifying the Identity of the Customer;
- determining the customer profile and levels of activity and adjusting the profile as and when necessary;
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the results of the risk assessment; and
- retention of records of these checks and update them when there are changes.

The company has the obligation to undertake CDD measures, when:

- players engage in financial transactions equal to or above NAF 4,000.
- Carrying out of occasional transactions equal to or above the monetary equivalent of NAF 4,000.
- There is a suspicion of money laundering or financing of terrorism
- The company has doubts on the veracity or adequacy of previously obtained customer identification data.

NB: a transaction may be a single transaction but may also be a series or a pattern, equivalent to or exceeding NAF 4,000.

6. Onboarding of New and Prospective Clients

This section describes the criteria for accepting new Clients based on their risk categorisation. Following a risk-based approach for every Client, it will be determined what level of due diligence is to be applied concerning identification, business relationship and transaction level. Where the level of risk is above the level the company is willing to accept, appropriate steps must be taken to mitigate the risk. If the risk cannot be mitigated to an acceptable level, the relationship must be terminated.

The user upon the inception of the account, shall provide the following identification information:

- First name
- Last name
- Date of birth
- Residence address (Building, street, city, country)
- Email
- ID Documentation:
 - Type of ID
 - The Expiry date of the ID
- Nationality
- Place of birth

The company interfaces with Clients non-face to face due to this the company has implemented mandatory verification for which tools and technology will be utilised to limit the risk from non-face to face. The internal controls and compliance management policy shall further indicate the testing of the said methods and four eye approach to further mitigate the risk of non-face to face interaction. The company shall reserve the right to block accounts and request alternative documentation should it be deemed necessary.

In order for the company to know it is dealing with a real person, documentation is required to corroborate as much as the information submitted as possible. The company shall obtain sufficient evidence of identity to verify the person is whom they claim to be (the reader may wish to note the sections above on CRA)

A Client's residential address is an essential part of their identity, and when it is not present on identification documents, it will have to be obtained separately (once the relevant due diligence level is reached).

The KYC provided will be verified via agents who are trained and who will ensure that the documentation provided corresponds to the information currently held on the Client and that the KYC is valid. If the documentation provided is deemed not to be valid or sufficient, further documentation may be requested from the Client.

Following the risk-based approach, at onboarding, an automated risk assessment of the ML and FT risk posed by the Client is carried out based on the information provided by the Client and checks conducted. The risk assessment will rate the Client as low, medium or high risk, due diligence and ongoing monitoring will be carried out in proportion to this risk (as is explained by this document). If the risk is deemed Medium or High, further information and documentation is required from the Client. If the account is rated High Risk and is exhibiting trends or there is suspicion, knowledge or reason to believe it must be reviewed by compliance personnel and brought to the attention of the MLRO or deputy for approval and analysis.

7. Client Categorisation Criteria

Depending on the Client's category, factors such as the Client's background, type and nature of their business activities, their country of origin and the services they require shall be considered to examine and define their classification. Depending on the level of risk and the customer profile obtained regarding the purpose and intended nature of the business relationship, an adequate level of due diligence is to be applied.

The application of due diligence below shall be determined by risk and thresholds. The below Transaction Limits are deposits into the Client's gaming account, calculated annually from the first deposit over a calendar year (365 day period), with the threshold reset annually.

The customer due diligence (CDD) shall be carried out as follows, in accordance with the triggers and alerts held internally to ensure that the level of due diligence is commensurate with the level of risk of the customer.

Customer Risk Assessed Grade	KYC Level	Requirements	Transaction Limit & possible scenarios
LOW CRA Grade: Is important to notice that clients with a KYC Level 1 will not always be a CRA Low Grade.	Level 1: Simplified Due Diligence onboarding	- Email and Phone - Basic customer information • Official full name; • Date of birth (to calculate age) • Permanent residential address; • Nationality; • Residence • Identity / Passport Number • Identity/ Passport Expiry date - PEP, Sanction & Negative Media Check	LESS than NAF 4000 (or equivalent) Even if the operation stays below NAF 4000, the CRA Grade could be Medium or even High, in accordance with the results of the screenings and searches upon inception, as well as if the Customer triggered any alert on the risk score or transaction monitoring tools.

MEDIUM CRA Grade: Is relevant to notice that clients with a KYC Level 2 will not always be a CRA Medium Grade.	Level 2: Customer reaches NAF 4000 in deposits, due diligence is mandatory.	• Status of employment Drop down Status of employment which are: • Self-employed • Employed, • Public employee • Student • Retired • Part-time employee • Unemployed • Proof of Income (SOW/F) (dropdown is enough, unless High Risk source of income + information) • Gross annual income	1st scenario: Customer exceeding NaF 4000 or equivalent in 1. 2nd scenario: CRA Grade is considered a medium after the screenings and searches upon inception, even if the customer got a KYC Level 1 upon inception. 3rd scenario: . Customer (KYC Level 1) triggered an alert on the risk score or transaction monitoring tools that placed the Customer in a Medium CRA Grade. See Transaction risk (monitoring) alerts in the Risk Assessment excel file.
--	---	---	--

HIGH CRA Grade	Level 3: Enhanced Due Diligence onboarding	Above, plus: - Proof of income document (s indicating SOW/F (evidence of wealth and funds)	1st scenario: reaching the annual limit. 2nd scenario: The Customer was considered KYC Level 1 or 2, however a high alert on the risk score or transaction monitoring tools were triggered, then the Customer is a High in the CRA Grade. See Transaction risk (monitoring) alerts in the Risk Assessment excel file. 3rd scenario: Considering the results of the initial screenings or searches, perhaps it won't be possible to provide service to the Customer. An EDD is going to be conducted and they will decide if the services can be provided.
----------------	---	---	---

7.1. LEVEL 1

Level 1 customers will only be able to transact up to a maximum aggregate value of less than NAF 4000 or in one lump sum, Level 1 consists of the provision of the customer's:

- Full name
- Date of birth
- Permanent residential address
- Email address
- Age
- Sanctions and PEP searches

7.2. LEVEL 2

Level 2 consists of the requirements laid down in Level 1 and the verification of that information through the provision of the following:

Identification document:

- A valid unexpired passport.
- A valid unexpired national or other government-issued identity card.
- A valid unexpired residence card.

- A valid unexpired driving licence; or,
- Other documents containing photographic evidence of identity that are not government-issued but which are nonetheless recognized as a legal means of identification by the national law of an EU or a reputable jurisdiction

7.3 3D liveness check or portrait photograph (“selfie”)

Should the customer risk assessment indicate that a customer poses a medium level of risk, the customer will be subjected to Customer Due Diligence (CDD) requirements. Level 3 is subject to the risk assessment and pre-threshold assessment, for which, if the customer risk is not that of a low. Level 3 will be immediately deployed holding all information in Level 1 and 2 accordingly. Level 2 CDD will be applied for customers transacting with an aggregate value of that is equal to or more than NAF 4000, or in those situations where the risk assessment indicates that the customer is likely to carry some risk towards and Level 2 and 3 are manually prompted:

The information to be provided by the customer at this stage shall be:

- Status of employment
- Proof of Income (SOW/F) (dropdown unless High Risk source of income)
- Declaration that customer is not involved in any activity prohibited by the CAP– we draft it, and customer accepts it (yes/no)
- Annual expected activity in NAF
- Gross annual income (source of wealth and funds)
- Jurisdiction of SOW/F (dropdown and back office to upload the proof of income document)

IF customer chooses SOW/F that prompt mandatory verification, the customer will be prompted to upload the proof of income document, and such is to be verified manually by the fraud prevention department

7.4 Origin of source of wealth and funds – Trusted (Green) or Not Trusted/High Risk (Yellow and Red) sources as per the Customer Risk Assessment

Type of Income	Verification Level on NAF 4000 or equivalent threshold	Rational

Sale of company	CDD – EDD if no online information can be obtained.	A sale of the company may be verified online. If such information cannot be corroborated, it shall be mandatory to have the information on the sale of the company following SoW/F verification section below
Inheritance	EDD	Inheritance is a non trusted source, client is to immediately be verified. and re-checked in the intervals related to ongoing monitoring
Loan	The customer has to provide evidence of the SOW/F indicated	Evidence is to be provided, clients may not play with funds derived from a loan especially by regulated entities. Loans between individuals are to be scrutinized and the donor of the loan is to be treated as a beneficial owner. One must we consider Responsible Gaming in such events along with ML/FT
Gift	The customer has to provide evidence of the SOW/F indicated	Evidence of the gift is to be provided holding also the rationale
Fixed deposit – Savings	Identification only required	Company dividends are a registered ledger hence are available on public sources. Client will be stopped NAF 4000 threshold

Funds generated from gambling / gaming winnings	The customer has to provide evidence of the SOW/F indicated	Winnings from other gambling are to be corroborated and the initial source of wealth and funds are to be obtained. Clients may easily come with a receipt of winnings of funds which have been laundered and such are used as a layering stage to A. Distance the funds from the source of origin. B. further legitimate the provenance of the funds.
Pension	CDD	Identification of funds would be required, should the threshold set in the CRA be reached.
Mining	The customer has to provide evidence of the SOW/F indicated	The crypto currency industry is a high risk as per the NRA and SNRA.
Salary income	CDD	In order to prevent a crime before it actually happens the 45% threshold is in place to question the client on the total SOW/F should this level be exceeded. The client will have the possibility to declare any further income.
Company profits/ distributed Dividend	Identification only required	Company dividends are a registered ledger hence are available on public sources. Client will be stopped upon reaching the NAF 4000 threshold

Sale of property	The customer has to provide evidence of the SOW/F indicated	Sale of property considering the jurisdiction and amount, may be substantial, evidence of such is to be provided.
------------------	---	---

Reference Colour	Required action
Green	No action required
Yellow	Alert is to be raised and verified manually. EDD if no information may be obtained. Upon verification the client is to be returned to a medium level of due diligence
Red	The customer has to provide evidence of SOF and SOW

7.4 LEVEL 3

It is pertinent to note that the Level 3 is the highest level of due diligence held on the customer. Level 3 shall be mandatory and shall be deployed when:

- The customer has exceeded the threshold set on the account
- If the customer has triggered any transactional or fraud triggers. See Transaction risk (monitoring) alerts in the Risk Assessment excel file
- The Risk assessment is that of a High
- Customer is from or has links to a high risk or non-reputable jurisdiction
- If any of the above are triggered, then the execution of Level 3 is mandatory. The requested documentation within this level is the verification of the source of wealth and funds
- Provision of a valid, recent proof income document detailing the wealth and funds of the customer as required on a case-by-case basis.
- Provision of further source of funds information should it be necessary to verify the transactions to be conducted by the customer.
- Provision of a valid, recent proof residential address document.
- Profession or Occupation

The threshold has been devised so no customer will exceed NAF 4000 or equivalent without prompting Level 3 due diligence. Should the customer not provide the information, the customer will not be able to further use the platform. The system shall deploy Level 3 automatically or in those cases where it is manually prompted by the agent reviewing the account.

In those cases where the customer is manually prompted and does not reply within a 30-day timeframe, such cases will be escalated for further investigation, for which if warranted an SAR/STR will be raised.

In those cases where the trigger is done automatically, hence stopping the customer depending on the source of income chosen, thresholds and risk assessment. Should the customer not reply to the said information request, the account will be automatically blocked within 30 days and the funds are to be sent back stating failure to provide CDD documentation the block shall be of withdrawal within those 30 days and a hard block after. There should be an analysis and a record kept (via Excel) of the review of the account and why no SAR/STR has been raised. This data will also serve to know the number of accounts being blocked.

8. Measures relating to CDD- Procedural Controls

CDD measures are to be taken as follows:

- Identifying the player and verifying that the customer's identity, using reliable independent sources, documents, data or information
- Identifying the beneficial owner and taking reasonable measures to verify the beneficial owner such that the company is satisfied that it knows who the beneficial owner is
- Understanding and obtaining information on the purpose and intention behind the business relationship
- Conducting of ongoing due diligence on the business relationship and scrutiny of transactions undertaken are consistent with the Company's knowledge of the player, business risk, as well as source of funds.

The Company and its employees will not disclose that a report has been passed on to the FIU for further processing, as this is commensurate to "tipping-off" which is a criminal offence. If the Company and/or its employees fear that performing CDD will act as a tipping-off to the suspect customer, a report should be raised to the FIU in lieu of performing CDD.

The Customer Due Diligence Procedure defines the procedure used to carry out Customer Due Diligence including timeframes and/or values, when this will be triggered and in which cases Enhanced Due Diligence (EDD) will need to be performed (ex: if a transaction raises a suspicion of money laundering). CDD is necessary in order to enable the company to apply a certain level of due diligence in order to mitigate ML/FT risks. Any unusual behaviour is to be immediately reported by the subject person to the Curacao FIU, and the latter may decide to proceed

accordingly, with further steps, including prosecution.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their account restricted during this period.

The following also lists key points when conducting CDD:

Identification and verification of the player:

Identification refers to the collection of personal details of the player used to establish the identity of said player. When identifying the player, the following information should be collected:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number

In low risk scenarios, it may be acceptable to obtain details from (1-3). In high risk scenarios, additional personal details may be obtained.

Carry out a customer risk assessment

This is done to have sufficient information available to detect unusual activity in the course of the business relationship. At this stage, a provisional risk rating will apply. This is revised once further information is obtained. On the basis of the Customer Risk Assessment (CRA), the proper level of CDD can be applied, as stipulated by the Customer Acceptance Policy (CAP).

Verification of identity

This usually takes place on the basis of government issued documentation containing photographic evidence (passport, identity card, etc). where such a document does not include the residential address, the Company requests other documents (utility bill, rental agreement, bank statement). Verification can further be made by checking on social media, telephone directories, company registries etc. Verification is carried out by the company to assure itself that the customer is who he purports to be. If the company obtains foreign documents extra care should be taken in order to verify its authenticity.

The customer will be given a timeframe within which all requested documentation shall be provided. Should the CDD Procedure not be completed within the established timeframes the customer's account will be considered to have failed completing CDD and thus will be denied from any further activity. The raising of a Suspicious Transaction Report ("STR") is to be considered. Such a decision is to be taken and recorded by the MLRO.

Unless a STR has been raised and an appropriate period has passed in which the customer has still not completed CDD, the account may be closed, and deposited funds still present on the customer's account will be returned to the deposit method, where possible, less any charges incurred by the business for transmission to this destination.

9. Obtaining information on the purpose of the business relationship

This is one of the requirements of CDD – the development of the customer's risk profile to have sufficient information available to allow for the detection of unusual activity.

Where the risk is not high, a salary statement with some details (ex: nature of employment) can be sufficient. Social media can also be used as a source of information.

When the risk of ML/FT is higher, the company may require that the information is backed-up by independent and reliable sources, such as information from the Central Statistics Department, such as: average national income, average disposable income, etc. These pointers will allow the company to discover wagering power amongst jurisdictions.

10. Ongoing and Transaction Monitoring

Ongoing monitoring is an intrinsic part of the Due Diligence process. It must be performed on all matters, regardless of the risk rating of the Client, to detect unusual or suspicious transactions. The primary objective of ongoing monitoring is to:

- The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds and that the funds are obtained from legitimate lines of business and not any business within the Customer Acceptance Policy and
- Ensuring that the documents, data or information held by the subject person are kept up to date.
- Keep- up-to date information used for CDD or EDD purposes (identity and verification documents); (the system will alert those instances where the documentation is about to expire);
- Stay alert to changes in the Client's risk profile and anything that gives rise to suspicion; and
- Monitor transactions for possible indicators of ML/FT.

The company shall examine, as far as reasonably possible, the background and purpose of all transactions that fulfil at least one of the following conditions:

- complex transactions that have no apparent economic or visible lawful purpose;
- large transactions that have no apparent economic or visible lawful purpose;
- unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
- transactions which are particularly likely, by their nature, to be related to ML/FT.

A manual review of the account can be conducted at the CDD threshold to ensure the client is properly assessed. Open source intelligence is also to be used and to corroborate SOW/F information provided this shall be carried out on those clients for which have raised concern in relation to the funding of the account or upon review. If there is a mismatch between the information provided by the Client and background research, this could lead to a ML/FT concern leading to the Client being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

Ongoing monitoring can trigger a further risk assessment of the Client due to transactional alerts, and if transactions are involved in the alert, they will be scrutinised to establish whether any suspicious activity or transactions are occurring.

A full review of the account will be conducted being as stated both on the identification and verification information and the transactions. A note shall be left on the system detailing what has been checked and the result of the checks carried out. Accounts can have their risk ratings increased via override, such will indicate that the account is to be reviewed more frequently.

Periodic Ongoing Monitoring

Accounts shall be periodically reviewed from the date of the last CRA based on the Client's level of risk:

- High Risk: 12 months
- Medium Risk: 24 months
- Low risk : 30 months

The above time frames are a backstop for when an account review is required. If the Client triggers before and a review is conducted, the periodic review timer restarts and is set from the date of the last Client review.

11. Timing of CDD Measures

A verification of identity is done when a customer engages in a transaction equal to or exceeding NAF 4000. All CDD measures would have been done when that threshold is reached. A minimum level of CDD is compiled prior to reaching that

threshold. Simultaneously with opening the account, the Company verifies the identity of the customer (as described above), and also conduct sanction/PEP screening. Once the threshold is reached, PEP screening is once again initiated, and a CRA is conducted. EDD is also carried out. The reader is invited to *vide* the explanation of EDD carried out by the Company.

Due Diligence must be carried out:

- Before establishing a business relationship with a Client. Due Diligence is to be conducted before allowing the Client to do any transaction of deposit funds onto the platform;
- Before carrying out a one-off transaction for a Client, i.e. those Clients who access the platform and conduct one transaction (which be treated as a business relationship);
- Where there is a reason to believe that Due Diligence carried out on an existing Client is inadequate;
- Where the Client's identifying details e.g. name or address, have changed;
- Where the Client has not been in regular contact with us;
- Where someone is purporting to act on behalf of a Client;
- Where suspecting ML or FT Client may be requested further documentation;
- Where the Client reaches the established thresholds
- SOW/F identification and verification shall be re-conducted periodically according to the Client's level of risk. High Risk Clients shall have SOW/F re-verified every 1 year and Medium risk clients every 24 months.
- EDD must be carried out when any of the situations in the 'Mandatory Enhanced Due Diligence' sub-section above occur.

12. Identification and verification of the Beneficial Owner

Identification relates to the collection of personal details. Verification relates to the confirmation of the veracity of said details. When identifying the player, the list as stipulated above on "identification of the player" should be followed.

The Company shall ensure that the account is used by the individual having opened it. This is done through explicit wording in the terms and conditions which the player is made to accept upon registration, including that the player is going to play on their own behalf, lest dire legal consequences arise, should the player be caught as having falsely accepted these terms. Ongoing monitoring from the Company's end shall ensure that these terms and conditions are being responsibly adhered to.

13. Enhanced Due Diligence (EDD)

A risk based approach shall be undertaken, more so for high-risk customers. EDD is conducted in several scenarios, such as:

- Residents of higher-risk geographical areas
- PEP's
- Products or transactions which may allow anonymity
- New products and business practices where the risk has not been sufficiently gauged, and further examination is required.

Applied measures tally with risks identified, such as:

- Obtaining additional information on the customer's occupation, previous address, and official information (such as info held on governmental databases)
- Obtaining additional information on the intended nature of the business relationship
- Obtaining additional information on SOW/F
- Obtaining information on the reason behind transactions (intended/performed)
- Obtaining additional clearance from higher management to continue with the business relationship
- Enhanced monitoring of the relationship
- Requiring the first transaction to be carried out through a bank with similar CDD standards.

14. Mandatory Enhanced Due Diligence

- EDD will be conducted in the following situations
- Clients with multiple revenue streams for which are not easily identified where the provenance of funds is originating from;
- Clients receiving funds to or from high-risk or non-reputable jurisdictions as per internal jurisdiction risk assessment.
- Clients who are from a high risk or non-reputable jurisdictions as per internal jurisdiction risk assessment (See the 'Jurisdiction Risk' section for more information on which jurisdictions are high risk);
- The Client attempts to deposit more than the allowed 45% threshold based on the user's Gross Income;
- If at the time the NAF 4000 threshold is reached, the Client is rated as medium risk (CDD), then the Client is only temporarily rated as a High Risk (EDD) until SOF/SOW is verified, at which point the Client goes back to medium risk (CDD). If the Client's SOF/SOW is not verified the account is suspended and the Client will remain on the EDD level. The Client if they wish to re-activate the account will have to provide SOF/SOW verification documentation;
- SOW/F shall be re-verified periodically according to the Client's level of risk High Risk Clients shall have SOW/F re-verified every 12 months.

- A manual review of the account is conducted inline with CDD and there is a mismatch on the SOW/F information provided by the client and background research. SOW/F verification is required to corroborate the information provided by the Client.
- Accounts following CRA has resulted in a High Risk;
- Accounts with a suspicious transaction pattern; or
- The Client is a PEP.

Clients at the CDD level shall be rated EDD temporarily until the SOW/F shall be requested if either of the above thresholds are reached. Once the client provides the relevant information the 45% threshold will be calculated on the verified amount of the client's SOW/F.

We can only request information from the Client which assists us in addressing a concern or understanding how the Client is financing their activity. The information required from the Client changes based on the changes in legislation in the different regions. Requesting more information will result in a legal defence.

If a Client refuses to provide any information or fails to provide the necessary information within the relevant time period, we will suspend the account and stop processing transactions. The case shall be raised further with the MLRO or designated individuals assigned to decide whether the case warrants further reporting to the relevant authority by analysing activity to identify knowledge, suspicion or reason to believe ML/FT.

15. Simplified Due Diligence

Simplified Due Diligence (SDD) is employed where the risk of money laundering is lower. Measures include:

- Obtaining only the player's identity (if the risks presented is lower)
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship - the extent of verification depends on the nature of the business relationship. In a low-risk scenario, bank statements, birth certificates etc may suffice.
- Reduction of the degree of monitoring, whilst still allowing for diligent monitoring.

The Company applies CDD measures to existing customers, on the basis of materiality of risk. The Company performs CDD regularly, at a minimum once yearly, depending on risk level. The Company evaluates whether the measures in place are sufficient to provide for appropriate CDD. In the case that the Company deems such measures to be sufficient, CDD is applied, and care is taken to ensure on-going monitoring obligations, as detailed above.

16. Termination of the business relationship

In the event that the obligations mentioned in the CDD measures section above cannot be met, the Company shall refrain from establishing a business relationship and/or a transaction with a given customer. In such a case, the Company shall block any further transactions and terminate the business relationship.

In a situation where the customer provides the requested information after the account is blocked, the Company's risk department shall assess whether the delay affects the ML/FT risk within the company vis a vis the given customer. The risk department shall also seek the feedback of the MLRO in such a situation. In the case where a suspicion of ML/FT exists, the Company shall file a report with the FIU.

If there is no reason to retain funds, these funds can be remitted back to the customer via the original payment method.

17. Reliance on third parties to perform CDD

The Company may elect to outsource its CDD function to a third party. The third party shall be subject to CDD and record-keeping obligations. The third party shall have a business relationship with the customer, independent of the relationship between the Company and the customer. The Company understands that the ultimate responsibility for CDD measures depends on the Company.

The criteria for such a relationship to be established shall be as follows:

- The Company has to obtain information concerning elements a-c of the CDD measures described above from the third party
- An agreement with the third party that copies identification data or other requested information relating to CDD requirements will be made available on request. Nonetheless, the Company understands that ultimate responsibility for conducting a CRA, determining whether a customer is a PEP and ongoing monitoring rests with it.
- Shall ensure that the third party provider is duly regulated, and has a proper functioning system where to conduct CDD.
- Regular periodical assessments of how the third party is conducting CDD and ensuring that this is done in accordance to extant practices.

The Company understands that ultimate responsibility for a correct procedure lies with it.

