ProgressPlay

R1

Fraud Control, Know Your Client (KYC), Anti-Money Laundering (AML) & Pay-out Management Procedures

ProgressPlay

Version	1.24
Date Created	14.4.2021
Author(s) of Document	Tal Spielmann, Adam Adamou
Purpose of Document	The document defines: • How the company goes about minimizing its exposure to Fraud • How it identifies its customers • What measures are taken to limit the company's exposure to Money Laundering and the reporting requirements in this regard how settlements towards players are carried out.
Security Class	Confidential
Authorized by	Itai Loewenstein

REVISION HISTORY

Version	Date of Issue	Author	Security Class	Changes	Approved By
1.0	01.11.12	Ian Cilia	Confidential	Initial Release	Itai Loewenstein
1.1	04.02.13	Ian Cilia	Confidential	Yearly review	Itai Loewenstein
1.2	16.08.14	Ian Cilia	Confidential	Update in view of UK license	Itai Loewenstein
1.3	16.08.14	Ian Cilia	Confidential	Update following legal review	Itai Loewenstein
1.4	05.09.14	Ian Cilia	Confidential	Update to section 9.3	Itai Loewenstein
1.5	26.01.15	Dganit Avital-Cohen	Confidential	Updates for UK license	Itai Loewenstein
1.6	05.03.15	Dganit Avital-Cohen	Confidential	Updates for UK license	Itai Loewenstein
1.7	24. 03.15	Ian Cilia	Confidential	Update to section 9.1.	Itai Loewenstein
1.8	01. 06.15	Ian Cilia	Confidential	Update for Malta Gaming Authority	Itai Loewenstein
1.9	07. 10.15	Dganit Avital-Cohen	Confidential	Update replacement of the company MLRO	Itai Loewenstein
1.10	21. 10.15	Dganit Avital-Cohen	Confidential	Update to Pay-out Management procedure	Itai Loewenstein
1.11	07.05.16	Taisia Chris	Confidential	Clause 9.1 updated	Itai Loewenstein
1.12	10.08.16	Taisia Chris	Confidential	Updated main sources of the policy and the EDD	Itai Loewenstein
1.13	07.02.17	Taisia Chris	Confidential	Yearly Review	Itai Loewenstein

ProgressPlay

1.14	14.09.2017	Anna Kassai	Confidential	Update in accordance to 4th AML Directive	Itai Loewenstein & Nicholas Gatt
1.15	10.07.2018	Anna Kassai	Confidential	9.2 Monitoring procedure update	Itai Loewenstein & Nicholas Gatt
1.16	26.11.2018	Ioanna Ivanenko	Confidential	Review	Itai Loewenstein & Nicholas Gatt
1.17	08.01.2019	Anna Kassai	Confidential	Adding Close loop payout and PayPal	Itai Loewenstein
1.18	10.05.2019	Anna Kassai	Confidential	Updating in line with LCCP	Itai Loewenstein
1.19	28.07.2019	Anna Kassai & Adam Adamou	Confidential	Updating Mr Adamou's appointment & EDD review	Itai Loewenstein
1.20	10.10.2019	Anna Kassai	Confidential	Review	Itai Loewenstein
1.21	16.02.2020	Anna Kassai	Confidential	8.5 Record Keeping added	Itai Loewenstein
1.22	21.05.2020	Anna Kassai & Shani Frankfurt	Confidential	Additional COVID-19	Itai Loewenstein
1.23	22.07.2020	Shani Frankfurt	Confidential	Review	Itai Loewenstein
1.24	14.04.2021	Tal Spielmann	Confidential	Review	Itai Loewenstein

ProgressPlay

Contents

Progressplay Ltd. is hereinafter referred to as "the company."

1.0 OVERVIEW

The company adheres to strict codes of conduct in order to protect the company's good standing, instil trust with the customers, comply with regulatory requirements and fulfil its ethical responsibility. The company warrants that it will:

- Identify and verify customers prior to establishing a business relationship
- Deal only with customers who have registered an account
- Comply with regulatory requirements and industry best practice
- Do its utmost to ensure that no funds are accepted which originate from illegal activities
- Prevent all cases when its Services might be used as a tool in Money Laundering

2.0 PURPOSE

This document defines the Fraud Control, Know Your Customer (KYC), Anti Money-Laundering (AML) and Payout Management procedures. The procedure defines:

- How the company goes about minimizing its exposure to Fraud;
- How it identifies its customers;
- What measures are taken to limit the company's exposure to Money Laundering (ML) and Funding of Terrorism (FT) and the reporting requirements in this regard;
- How the company classifies its players in term of AML and Countering Terrorist Financing (CTF);
- How settlements towards players are carried out.

3.0 SCOPE

This procedure applies to all the stages of the customer lifecycle. Different parts of the procedure apply at different stages:

- At registration identify email address, age, identity, and profession/occupation;
- Account and document review to verify address;
- Payout to verify legitimate transactions;

- Ongoing monitoring for suspicious transactions;
- Closing account (if applicable);
- Dormant accounts (if applicable).

4.0 POLICY BASIS

These main sources of the policy are:

- Fifth Anti-Money Laundering Directive [European Union, came into force on January 10, 2020, Remote Gaming Regulations (2004) [Malta] Prevention of Money Laundering and Counter Terrorism Financing Act, as amended by legal notice 105 of 2008. [Malta];
- Implementing Procedures Part II issued by the FIAU and MGA, in terms of the provisions of the prevention of Money Laundering and Funding of terrorism regulations. For the Remote Gaming Sector (19th July, 2018) [Malta];
- The Proceeds of Crime Act 2002 (POCA)2 Gambling Commission;
- The prevention of money laundering and combating the financing of terrorism. Guidance for remote and non-remote casinos Fifth edition (January 2020);
- UK Gambling Commission Risk Assessment ‘Money Laundering and terrorist financing risk within the British gambling Industry’ (June 2019);
- UK Gambling Commission Covid-19 Guidance & FAQ’s publication (30th March 2020);
- ‘Gambling Commission instructs tighter measures to protect consumers during lockdown’
- UK Gambling Commission ‘Customer Interaction – Additional formal guidance for remote operators during COVID-19 outbreak’ (12 May 2020);
- UK Gambling Commission Findings published from time to time.

5.0 RESPONSIBILITY

The MLRO / NOMINATED OFFICER and the Key Official are responsible for ensuring the Fraud Control, KYC and AML Procedures whilst the COO is responsible for the Payout Management Procedure. They are also responsible for ensuring the plan is kept up to date and that employees are aware of the procedure. The Directors take responsibility for ensuring that regulatory compliance is at the heart of the Company and therefore, the AML procedure is approved by the Board of Directors.

****Additional COVID-19 measurements****

Due to the Covid-19 pandemic and implications, it was the responsibility of the Company and all of its employees to leave no doubt when assessing the customer affordability and ensure that the customers will not be permitted to lose up to and beyond his/hers assumed level of available funds. Therefore, the Company has given **an additional** consideration to customer affordability, by implementing the Affordability Check, including on-going monitoring, as described in detailed in the Affordability Check Policy and Procedure. Moreover, in order to perform this Affordability Check, triggers have been revised in order to ensure they will not be hit and be at levels which is sufficiently risk-based.

6.0 RISK BASED APPROACH

The company adopts a risk-based approach to Anti Money Laundering and Countering the Financing of Terrorism. This means that measures and monitoring will be applied in accordance the ML / FT risks posed to the Company. In this manner it can be ensured that resources are directed to the areas which pose the greatest risk of ML / FT.

Each player is categorized into Low, Medium or High category in terms of risk. The categorization is carried out in accordance to the following and added to the player's files.

	Low	**Medium**	**High**
Documents status	Verified	Not verified	Not verified
Deposit amount	< €2000	€2000 - €5000	€5000<
Withdrawal	No	Yes	Yes
Payment Method	Credit Card (non-UK customers only), Debit Card, Trustly	Alternative Payment Methods	
Number of Deposit Methods	Same method	2 different methods	3 or more different methods

As part of the Company's risk control, once a day the Risk Department monitors the list of accounts under the High category.

The Risk Based Approach is informed by the UK Gambling Commission Risk Assessment 'Money Laundering and terrorist financing risk within the British gambling Industry' (January 2020).

7.0 MONEY LAUNDERING REPORTING OFFICER

The appointed for the company under the Gambling Commission's licence is:

Name: **Adam Adamou**

Email: Adam@progressplay.com

Mobile: +357-99593920

The appointed for the company under the Maltese Gambling Authority's licence is:

Name: **Adam Adamou**

Email: Adam@progressplay.com

Mobile: +357-99593920

8.0 KYC PROCEDURE

Know Your Customer Procedures are followed to achieve the following objectives:

- Allowing only legitimate customers to register an account; e.g. blocking minors, players from blocked countries etc.;
- understand the potential risks associated with the customer;
- confirming that customers are who they say they are, through available tools;
- monitoring customer accounts and transactions for illegal activities;
- blocking duplicate accounts;
- Understand the potential risks associated with the customer.

8.1 Registration

Before being able to gamble on the site, a customer needs to first register an account. On registration the customers are asked for the following details:

- Full Name (First name and Family name);
- Date of birth - No customers under the age of 18 are allowed to register an account. The system does not allow persons under 18 to register an account;
- Address and country of residence. Players from restricted countries are not allowed to register. (The list of restricted countries is provided to all employees.);
- Contact telephone number;
- Valid email address;

- Occupation/profession.

In order to verify the email address/phone number of a player the company is using the following method:

- Upon registration, a player's account will be temporarily activated;
- The company will send a "branded" e-mail/SMS to the player with a PIN code to activate his account.

Once the above information is received the fraud department will screen the information for any false or suspicious information, possible duplicate accounts, self-exclusion lists, Politically Exposed Persons and sanction lists.

Players from restricted countries are not allowed to register. The IP address from where the traffic originated is tracked by the company's back office software. Should traffic originate from countries which are on the list of restricted countries, the account will be blocked.

Should the checks indicate that a duplicate account has been registered; the account is suspended until further checks are made to determine whether or not this is indeed a duplicate account. If the checks prove that the account is indeed a duplicate account, the account will be closed.

8.2 Age and ID Verification – Preventing access to Gambling by Children and Young Persons

No customer under the age of 18 is allowed to register an account. The system does not allow persons under 18 to register an account as date of birth would make the player younger than 18 the registration system prevents the player from finalizing his process. When a player deposits using Mastercard, Visa or Diner's Club and the name on the registration match those of the card owner, the age can be verified since such cards are only issued to persons over 18.

8.2.1 Under the Gambling Commission's Licence

As per required by the Licence conditions and codes of practice (LCCP) 17.1.1, the company has the responsibility of verify, as a minimum, the name, address and date of birth of a customer in order to establish their identity, and before permitting them to deposit or gamble.

This means that the Identity and age of the customer is verified before the customer is able to:

i. Deposit any funds into their account;
ii. Access any free-to-play version of gambling games; or
iii. Gamble with the company either using their own money or bonus funds.

8.2.2 Under MGA's Licence

Until the age verification process is satisfactorily completed, the customer is not permitted to withdraw winnings from the account. In addition, if money is deposited in a customer account using any type of payment method other than a credit card (non UK customers only), an age verification is carried out. If age verification has not been satisfactorily completed, then (i) the customer account will be frozen, and (ii) no further gambling will be permitted via the account until age verification has been successfully completed. In addition, the company reserves the right at any time to request from the customer evidence of age and if satisfactory proof of age is not provided, then the above mentioned consequences will apply, mutatis mutandis.

In the event that it is found that the customer is under the age of 18, or the legal age as determined by the laws of the country where the customer lives (whichever is higher), then the company shall close the account and return to the customer any money paid in respect of the use of the services of the company, but the winnings shall not be paid and will be confiscated.

A number of tools are available on the market which can assist in the age and identification verification. The company is using, where required for the purposes of age verification, third party services such as GB Group's ID3 verification tool.

8.3 Duplicate accounts

Players are only allowed to hold one account per [white label] brand. During the registration process, the details are checked for possible duplicate accounts. In case a customer attempts to create a duplicate account, the system prevents the creation of a secondary account. Should the customer alter the registration details in order to circumvent the checks, and future checks indicate that a duplicate account has been registered; the account is suspended until further checks are made to determine whether or not this is indeed a duplicate account. If the checks prove that the account is indeed a duplicate account, the account will be closed.

Should the risk management department have any doubts about any of the information submitted at registration stage or have any doubts whatsoever, further identification verification should be carried by requesting supplementary documents from the player. The documents requested are:

- Proof of Identity: Picture of a Photo ID – for example: Passport or Driver's License;
- Proof Of Address: Picture of a recent utility bill or bank statement (no older than 3 months) showing the issue date, name and address;

- Proof Of Payment Method: Picture/Screenshot of the payment method use.

Should the fraud department still not be satisfied, they should ask for further documents. If in doubt the MLRO should be consulted.

8.4 Due Diligence

Player KYC and due diligence shall be ongoing and conducted on a risk-sensitive basis in situations, which by their nature, represent a higher risk of Money Laundering or Financing of Terrorism. Risk Operations Manager is responsible for setting out a matrix which scores risk according to criteria which influence the risk rating.

8.4.1 Customer Due Diligence

1. Under the Gambling Commission's Licence

   Customer due diligence verification will be applied on all accounts upon first deposit.

   In order to verify the customer's account before participating in the company's services, the customer's account is sent for a Digital KYC check upon before first deposit. Each account is electronically verified by a 3rd party tool provided by GB Group (https://www.gbgplc.com/). Depending on the result, the following is the process is:

   - Pass2 – means that the account was verified via 2 databases, meaning the CDD verification was successful and the customer is allowed to deposit;

   - Pass - means that the account was verified via 1 database, meaning the customer is allowed to deposit but the CDD verification is needed. Upon Pass result, an automated e-mail is sent to the customer to request documents for verification. In case no response is received until the €2000 threshold, the account will be automatically soft blocked (meaning the customer has option to access his account however, they cannot make any further deposit or place any bets);

   - Fail or Refer – they are sent to the 2nd level of checks. In order to verify the account, the customer is required to upload verification documents (Driving Licence, Passport, Utility bill) which are sent to IDScan for Document Verification.

In case the documents get verified the customer can proceed to deposit. In case the Document Verification fails, the accounts are manually checked.

2. Under MGA's Licence the following checks need to be done:

   Customer due diligence verification will be applied on all accounts that reached the € 2,000 transactional threshold (accumulated deposits and withdrawals).

   i. funding was done by means of a verified credit card

   ii. the following documents are submitted:

   - Proof of Identity: Picture of a Photo ID – for example: Passport or Driver's License
   - Proof Of Address: Picture of a recent utility bill or bank statement (no older than 3 months) showing the issue date, name and address
   - Proof Of Payment Method: Picture/Screenshot of the payment method use

The following events will trigger due diligence procedures and the account will need to be verified further:

- Attempt to change account details like address, email or other details;
- Attempts to withdraw using a method other than the one used to fund the account.

8.4.2 Enhanced Due Diligence

When the customer is not physically present for identification, a higher risk of ML is posed. The following events will trigger the Enhanced Due Diligence checks and procedure:

- The customer reaches the accumulated lifetime amount of €3000 deposit/withdrawal threshold;
- Attempt to change account details like address, email or other details;
- Attempts to withdraw using a method other than the one used to fund the account;
- Player is a PEP (Politically Exposed Person);
- Country of origin associated with higher credit card fraud;
- Sudden changes in account activity e.g. the volume of transaction increases suddenly;
- Any suspicious submitted documents that were required and look suspicious or unreal;
- Anyone who deposited with a card that can't be paid back to the card and asks the money to the bank or any alternative payment method.

The following documents are requested as part of the EDD:

- Proof of Identity: Picture of a Photo ID – for example: Passport or Driver's License;
- Proof of Address: Picture of a recent utility bill or bank statement (no older than 3 months) showing the issue date, name and address;
- Proof of Payment Method: Picture/Screenshot of the payment method use

Furthermore, the following checks are done:

- Sending the player for an enhanced KYC check with GB Group where we use an enhanced check and the player is confirmed against 2 databases by the GB Group;

Verify or certify the documentation supplied and running an Internal Fraud Check where we do a full open source check on the customer including but not limited to, where customer lives, the property, the area, a full check on IPs, the salary, whether the person owns any companies via companies house and a full social media check including Linkedin, Facebook and any other open source information we manage to find Third party EDD checks GB Group (https://www.gbgplc.com) , 192.com (http://www.192.com) , Risk Screen (https://www.riskscreen.com).

8.4.4 Internal Fraud Checks

An Internal Fraud Checks, as well as the AML Checks, are being performed as part of the Affordability check. The Fraud Check consists of the following:

- Enquiries are made into the source of customer deposits;
- All customers are requested to submit proof of income to substantiate customer responses, i.e. Source of Funds (SOF). Proof of income may include Savings, Salary, Returns from Investments/Dividends, Value/ Sale of Property, Inheritance, Lottery Wins/Gambling Wins and/or any other valid proof of income.
- A risk assessment is carried out to ensure there is no discrepancy between the customer's income and the amount of deposits the customer is making.
- Additionally, using open source information and proof of income an estimate of the customer's net worth is made. To do this Progressplay Ltd assesses the estimated Net worth of the customer's monthly salary, any additional funds and property value whilst deducting estimated out goings and compares this sum to customer losses.

8.4.5 Declaration of Source of Funds (SOF)/ Source of Wealth (SOW)

The thresholds for Enhanced due diligence checks including asking the customer for a Declaration of SOF/SOW and subject to the above conditions are as follows:

1. Under the Gambling Commission's Licence:
   a. Upon the affordability limit in accordance to the customer's average salary. Incase the player didn't reach his spending limit:
   b. 10,000 life time deposit.
2. Under MGA's Licence the following checks need to be done:
   a. Net Deposits of €30,000 in total per network/per lifetime;
   b. Net Deposits of €25,000 in total per month;
   c. Net Deposits of €15,000 in total per week;

Net Deposits of €5,000 in total per day.

Where Net Deposit = All time Deposit – All time Withdrawal.

Subject to the above, customers must go through a mandatory enhanced due diligence check. As stated above, each customer, will have to go through an Internal Fraud Check.

*All thresholds in place are customized and subject to financial profile of the player which is determined pursuant to the Affordability Check .

If suspicious transactions are discovered or if losses are greater than Net worth, then the MLRO is informed an SAR will be created and submitted it to (i) under the Gambling Commission Jurisdiction to the NCA, 9ii) under the MGA's jurisdiction to the FIAU.

Customers that pass the due diligence are permitted to continue to deposit at the casino. The Company will always retain the right to carry out addition due diligence check should we see that the circumstances would make it necessary.

All records are kept on secure servers for a minimum of 5 years. It should be noted that all records are being documented in accordance with the Company's new Documentation and Record Keeping Policy.

8.4.6 Ongoing Monitoring

The company has the responsibility to continuously monitor its customer base in order to prevent potential ML/FT. It should be noted that the initial ML/FT and Fraud Checks are being performed as part of the Affordability Check, which allows the Company, in a very early stage, to achieve an improved risk-based, and enclose the risk of ML or FT.

Smaller transactions through a longer period of time might enable some customers to stay 'under the radar'.

The ongoing monitoring includes the following:

- scrutiny of transactions undertaken (including, where necessary, the source of funds) to ensure that the transactions are consistent with the casino's knowledge of the customer;
- undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying CDD/EDD measures up-to-date;
- the MLRO's responsibility to review transactions on a daily basis and to send a summary report to the management about the account reviews. (As per the company's Daily AML review procedure).

Should any suspicious arise, the MLRO should send a request to the Head of Risk Team to investigate the account further and if necessary to request further documentation from the customer.

8.4.7 Politically Exposed Person (PEP)

A Politically Exposed Person (PEP) is a term describing someone who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

In itself a PEP is not a concrete indication of ML/FT, however, due to the nature of the player transactions should be scrutinized in further detail. Nevertheless, the company is committed to avoid any possible risk thus, each player is checked through a third party database (GBG Group) for possible PEP. In case the company receives an alert of a player who might be a possible PEP, the PEP procedure should be followed.

8.5 Record Keeping

Please refer to our Documentation and Record Keeping Policy.

If there is a separate policy for this so why mention it here?

9.0 ANTI-MONEY LAUNDERING PROCEDURE

9.1 General Procedure

The AML procedure aims to satisfy the following requirements:

- Identification Know Your Customer (KYC) and Customer Due Diligence (CDD);
- Internal record keeping;
- Reporting;
- Employee training.

To this end the Company shall:

- Appoint Money Laundering Reporting to MLRO / NOMINATED OFFICER;
- Note that if the appointed Nominated Officer/ MLRO is temporarily unavailable, another PML may deputise in line with The Prevention of Money Laundering and Combating Terrorism - July 2017 Guidance. All employees and service providers must be notified of the temporary change and be provided with contact details for the deputy MLRO/Nominated Officer;
- Notify the Financial Intelligence Analysis Unit (FIAU) or National Crime Agency (NCA) of the appointed MLRO / NOMINATED OFFICER ;
- Keep records of all registered players;
- Keep the required identification and transactional records as defined by laws, regulations, guidance notes and implementing procedures;
- Establish the identity of all players as detailed in the KYC procedure;
- Categorize each player into Low, Medium or High risk categories. Ensure the policy is updated to reflect the changed regulatory environment;
- Provide adequate training to employees involved and maintain documentary evidence of such training;
- Monitor transactions for any suspicions of M) and F) activities; why only initials and if only the initials why delete the L and T?

- The MLRO / NOMINATED OFFICER shall report any suspicious transactions to the FIAU (Financial Intelligence Analysis Unit) by means of a Suspicious Transaction Report. Such report can be filed directly from the FIAU website: http://fiumalta.org/report-suspicious-transaction or the NCA site: https://www.ukciu.gov.uk/(zwmftuuaccdousrniimr4g55)/saronline.aspx;

- Co-operate with Authorities in their effort to prevent and detect criminal activity;

- The MLRO or the Compliance Officer is to inform the UK Gambling Commission of the unique reference number issued by the FIAU (Malta) of the FIAU institution issued in Malta in respect of each Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) submitted by the operator within five working days of receipt of the unique reference number in line with requirement 15.2.1 point 24 of the License Conditions and Codes of Practice for the reporting of Key Events. Key events can be reported securely online at the Commission's website through our eServices system www.gamblingcommission.gov.uk;

- It is important to note that cash transactions are strictly prohibited.

9.2 Monitoring transactions for signs of ML and TF

There are a number of events which might raise suspicions of money laundering and which require further scrutiny. The following are a few examples:

- Player is a PEP (Politically Exposed Person) this is in itself is not a concrete indication of ML/FT, however due to the nature of the player transactions should be scrutinized in further detail;

- suspecting that an account is being controlled under a false identity;

- artificially splitting a withdrawal to remain 'below the radar' e.g. splitting a withdrawal of 10000 into 5 withdrawals of 2000 within a short time period with hope of avoiding raising requests for further identification;

- unexplained or unclear source of wealth e.g. student playing large volumes of money the source of which cannot immediately be ascertained;

- sudden changes in account activity e.g. the volume of transaction increases suddenly;

- aattempts to shift funds from one account to another – which is currently not possible at the company's accounts.

To monitor ongoing user behaviour, every 2 weeks the MLRO and the Head of Risk reviews users with High Risk AML categorization. In case the review deems the user a risk to the Company, further restriction will be imposed on the account until further verification is successfully completed.

9.3 Reporting Suspicion or Knowledge of ML or FT

Employees are required to make a report in respect of information that comes to them; When they know/ When they suspect/ When they have actual or reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing, including criminal spend. These obligations are collectively referred to as 'grounds for knowledge or suspicion'.
Any suspicions of ML or FT should be reported internally to the MLRO / NOMINATED OFFICER. These reports should be document by means of a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) [refer to Appendix A]. All SAR's and STR's should be submitted to the MLRO / NOMINATED OFFICER by means of email to Adam@progressplay.com . The MLRO / NOMINATED OFFICER will then investigate the report and decide if it is necessary to escalate the report to the Financial Intelligence Unit (FIAU).

Any suspicion of ML or FT should be reported internally to the MLRO / Nominated officer using the following procedure:

i. Place a temporary restriction (softblock) on the account (closing the account might tip off the customer – see 9.4);
ii. Leave a note on the back office stating that if the customer contacts support he/she should be referred to upper management. It is important not to leave any notes which indicate that the customer is under suspicion;
iii. The customer must not be told that their account is being investigated and no reference must be made to money laundering or criminal activity (see 9.4 *Tipping off* below);
iv. Check any related accounts and lock;
v. Fill in and submit Suspicious Activity Report (SAR) [refer to Appendix A];
vi. Send the completed forms to Adam@progressplay.com.

If you have any questions please contact the MLRO who will provide you with support: Adam@progressplay.com.

Once the above actions are taken, extreme care must be exercised in any customer interactions to avoid Tipping Off (refer to the next section).

9.4 Tipping off

It is extremely important that at no point is the customer to be informed that he/she is being investigated or that any transactions he/she made were flagged for suspicious activity. Such an action would qualify as 'tipping off'. Tipping off could unnecessarily alarm the client if following investigations it turns out that there is no suspicious activity going on, but more importantly it could forewarn anybody conducting criminal activity of the investigations and could prejudice investigations. If forewarned of an impending investigation a criminal could destroy evidence incriminating them. Tipping off is a criminal offence. No unnecessary staff should be informed of the suspicions; it is sufficient to initially just inform the MLRO. / NOMINATED OFFICER. It is also important not to take any action which might indicate to the person being investigated of the suspicions e.g. suspending account for no immediate apparent reason.

When a customer who is suspected of ML or FT makes contact with customer support, he/she is to be informed that he/she will be contacted shortly. Internally the case should be assigned to a Manager who will deal with the queries ensuring no tipping off takes place.

9.5 Failure to report

One should always keep in mind that failure to report a suspicious transaction when there are 'actual or reasonable grounds to suspect' ML/FT activities is also a criminal offence.

9.6 Suspected Fraud/Money Laundering involving employees

ML/FT activity and/or fraud can also be conducted by employees of the company. Should any activities of company employees raise suspicions of ML/FT or fraud, the same procedure should as with customer transactions should apply. The suspicious activity should be reported to the MLRO / NOMINATED OFFICER by means of an Internal Suspicious Transaction Report whilst avoiding tipping off and involving any unnecessary employees.

10.0 PARTNER DUE DILIGENCE

Prior to entering into a long term business relationship with any partner or supplier, in particular any WhiteLabels or intermediaries, the company will perform its own due diligence and probity checks. Note that there is a separate Company White Label Policy.

Before entering into any agreement with a third party the company will conduct due diligence checks as follows:

10.1 When the contracting party is and individual

Where the contracting party is an individual the following documents will be requested:

- ID verification: Passport, ID or government issued photo document;
- Address verification: a recent utility bill or bank statement;
- Open source checks.

10.2 When the contracting party is a Company

When the contracting party is a company the following notarized or certified documents (in English) will be requested:

- Certificate of incorporation;
- Registry of Shareholders;
- Memorandum & Articles of Association;
- Passport (visible) of all shareholders, ultimate beneficiary owner (UBO) and directors;
- A recent utility bill that must show personal address of all of the above;
- Open source checks;
- Credit Check.

11.0 KNOW YOUR EMPLOYEE (KYE) POLICY

The treat of Fraud, ML and FT can also come from within the company. The scope of this KYE Policy is to gain a good understanding of the employees of the company for the purpose of detecting conflicts of interest, money laundering, past criminal activity and suspicious activity.

11.1 Pre-Employment background checks

A very simple, and often overlooked, way of reducing the risk of internal fraud and ML/FT is to conduct pre-employment checks. Wherever possible the company should:

- Ensure that the employee is not a minor;
- All our staff especially management are required to have past relevant experience in the gambling arena other than customer support that is preferred but not mandatory;
- Ask for and verify with independent references which we speak with prior to recruiting;
- Verify prospective employee's personal information and background;
- For management or sensitive positions when required request a full background check including a police check.

11.2 Monitoring employee behavior

Monitoring employee behavior may also uncover possible indicators of fraud. The following are some warning signs which may indicate the presence of fraud:

- Mismatch between income and lifestyle;
- Taking few holidays or avoiding being away from work for long stretches of time;
- Working alone, at weekends or late;
- Secretive behavior;
- Reluctance to share information;
- Suppliers / customers insisting on dealing with a particular member of staff;
- Reluctance to delegate;
- Refusal of promotion;
- Refusal of task rotation;
- Regular override of standard procedures;
- Request for advance payments;
- Addiction to gambling, drugs or alcohol.

11.3 Processes and control

An effective way of identifying risk areas which are vulnerable to fraud is to first identify where the company's most valuable assets are. Once these assets are identified, the company will need to reduce chances of these assets being misused (opportunity). Processes and controls will need to be built in the routine business of the company in order to minimize the chances for fraud. Some example of what processes and controls can be implemented are managerial oversight of finance processes, ensuring that no one employee can transfer high value assets without sign-off, regular checks and reconciliation, audit of assets and financials, restricting access to key areas and CCTV monitoring in sensitive areas.

11.4 Investigating cases of fraud

An essential part of any investigation is ensuring proper evidence collection and proper maintenance of the chain of custody of the evidence collected.

The company needs to be sure it can identify:

- Who handled the evidence?
- What procedures were performed on the evidence?
- When was the evidence collected and/or transferred to another party?
- Where was the evidence collected and stored?
- How was the evidence collected and stored?
- For what purpose was the evidence collected?

12.0 PAYOUT MANAGEMENT

For cumulative transactions within the last 12 months of € 2,000 and over, the player is required to send the following information:

- Proof of Identity: Picture of a Photo ID – for example: Passport or Driver's License
- Proof Of Address: Picture of a recent utility bill or bank statement (no older than 3 months) showing the issue date, name and address
- Proof Of Payment Method: Picture/Screenshot of the payment method use
- The Licensee will only remit withdrawals to the same account from which the funds originated.

The company reserves the right to request the above documentation at much lower thresholds if any suspicious activity is noted on the account.

Company adheres to a Close-loop payout system, meaning, withdrawals will only be remitted to the same account from which the funds originated.

12.1 PayPal - Proportional Payouts

In case a customer uses multiple sources/payment methods to deposit and one of those method is Paypal, a Proportion Payout takes place. This means that the amounts paid out to the Paypal account is in proportion to the relative amounts the customer used to fund their account during the last six (6) months.

As an example:

40€ have been deposited using PayPal and 60€ using a debit card. By playing the cards right, the player increased his money tenfold. Now the player has 1000€ and wishes to withdraw the entire sum. 400€ would have to be withdrawn using PayPal (40% of the winnings) and the rest using the other payment method, in this example the debit card (600€ equalling 60% of the overall winnings).

13.0 TRAINING

AML / CFT training should be provided to:

- all members of staff whose duties include the handling or monitoring of transactions;
- all Directors;
- Nominated Officer / MLRO.

13.1 Content of training

The training will include the following:

- Customer Due Diligence measures;
- Record keeping procedures;
- Internal reporting procedures;
- Internal Policies and Procedures for monitoring and control;
- Risk assessment and risk management;
- Monitoring;
- Legal provisions.

13.2 Nature of training

Training will vary according to the role the member of staff occupies and will include practical examples and ML and FT typologies.

Training will consist of a mix of internal and external training.

13.3 Frequency of training

Training will be provided at regular intervals and on the following trigger events:

- To new employees;
- To specific employees when there is a change in role which warrants different training;
- Changes in legislation;
- Annual Refreshment training.

13.4 Records of training

Records of all AML/CFT training provided to all staff will be kept. These records will include:

- the date on which the train was delivered;
- the nature of the training;
- names of members of staff attending the training;
- results of any assessment.

14.0 APPLICABILITY OF OTHER POLICIES

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

15.0 ENFORCEMENT

This policy will be enforced by the MLRO / NOMINATED OFFICER and CFO. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

ProgressPlay

16.1 APPENDIX A

SUSPICIOUS ACTIVITY REPORT

CONFIDENTIAL AML – SUSPICIOUS ACTIVITY REPORT			
Date:			
Submitted By:		**Department:**	
MAIN ACCOUNT			
Name of Client:			
Username(s):			
Account ID(s):			
ASSOCIATED / LINKED ACCOUNTS			
Name of Client(s):			
Username(s):			
Account ID(s):			
FULL REPORT to include reason for submission/details of suspicious transaction(s): *Continue on separate pages where needed*			
LIST OF SUPPORTING DOCUMENTS/ATTACHMENTS (if necessary):			
PLEASE SEND COMPLETED DOCUMENT IN CONFIDENCE TO THE AML TEAM. EACH SUBMISSION WILL BE ACKNOWLEDGED WITH A REFERENCE NUMBER. ***Do not to disclose to any other unauthorised person the existence of this report especially the customers concerned. Doing so may constitute a criminal offence.***			

16.3 APPENDIX B

DECLARATION OF SOURCE OF FUNDS

Customer information must be completed for each participant in the account, individually. For this document, the term “Player” always refers to the entity for which this application has been made, regardless of the legal description.

First Name: ______________________________ Last Name______________________________

Street Address: ___________________________________ City: ___________________________

Post Code: _______________________ Country______________________________

Telephone: ____

Email Address: ____

Date of Birth (dd/mm/yyyy): _________________________________

Employment Status: (choose one)

- Employed
- Self-Employed
- Retired
- Unemployed

Position: ____

Employer’s Name: ____

If you are self-employed, select your industry: Consumer Goods, Financial, Healthcare, Industrial Goods, Services, Technology, Utilities,

Other____

and

Products/services:____

□ I am: □ I am not a Politically Exposed Person (“PEP”). A PEP is an individual who holds or has ever held one of the following offices or positions: head of state or government; member of the executive council of government or member of a legislature; deputy minister (or equivalent); ambassador or an ambassador’s attaché or counsellor; military general (or higher rank); president of a state owned company or bank; head of a government agency; judge; or leader or president of a political party in a legislature. A PEP also includes close associates and immediate family members (mother or father; child; spouse or common law-partner; spouse's or common-law partner's mother or father and brother, sister; any other child of the individual's mother or father) of the PEP.

Financial Information

What is your total estimated annual income? GBP___________________________________

What is your total net worth? Please detail your income sources:

____ GBP

Do you own a property: ____

____

Have you ever declared bankruptcy? Yes / No

If Yes, provide date and details

____

_

Source of Wealth/Funds (choose one or more)

- Employment/Salary
- Loan
- Sale of property
- Pension
- Investment/Savings
- Pension
- Gift
- Inheritance
- Proceeds from Other Investments
- Other _________________

Please include copies of Source of Wealth/Funds along with this form.

Responsible Gaming:

Has gambling ever made your life unhappy? _________________

Have you ever gambled to get funds in order to pay debts or otherwise solve financial difficulties?

____

Have you ever sold anything to finance gambling?

____

Have you ever borrowed to finance your gambling?

____

Have you ever gambled to escape worry, trouble, boredom, loneliness, grief, or loss?

____

Agreed and accepted: ____

Signature: ________________________________Date: ___________________________