IMPLEMENTING PROCEDURES

ISSUED BY THE FINANCIAL INTELLIGENCE ANALYSIS UNIT, IN CONJUNCTION WITH THE MALTA GAMING AUTHORITY, IN TERMS OF THE PROVISIONS OF THE PREVENTION OF MONEY LAUNDERING AND FUNDING OF TERRORISM REGULATIONS

PART II

REMOTE GAMING SECTOR

Issued: **19 July 2018**

1. INTRODUCTION

These Implementing Procedures are specific and applicable to anyone who is licensed to provide a service involving the wagering of a stake with monetary value in games of chance, including games of chance with an element of skill, *via* electronic means of distance communication upon request from the recipient of said services, with the opportunity to win prizes of money or money's worth ("licensees"). The application of anti-money laundering and countering the funding of terrorism ("AML/CFT") obligations limitedly to licensees providing a gaming service, does not exonerate other operators active within the gaming sector, including providers of critical gaming supplies, from the general obligation at law to ensure that entities with which they enter into a business relationship with for the latter to ultimately provide a gaming service are duly authorised or licensed in terms of law. If such an entity is not subject to these Implementing Procedures, such other operators active within the gaming sector should also ensure that the entity they are contracting with is of good standing and is subject to equivalent AML/CFT safeguards.

The purpose of this part of the Implementing Procedures is to focus on certain aspects of the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR") and their application which warrant further elaboration at industry-specific level in order to highlight certain aspects of relevance, and to ensure that they are understood and interpreted consistently by licensees. It is important to note that the omission of any reference in these Implementing Procedures to other AML/CFT obligations is not to be considered as tantamount to the inapplicability of the same. Moreover, in so far as the Implementing Procedures – Part I are not in conflict with these Implementing Procedures, they are still applicable to licensees.

2. The Risk-Based Approach

2.1 What is the Risk-Based Approach?

Licensees should be aware that the AML/CFT regulatory framework that is applicable to them as subject persons adopts a risk-based approach, i.e. it requires subject persons to adopt measures, policies, controls and procedures that are commensurate to the money laundering and funding of terrorism ("ML/FT") risks to which they are exposed to prevent and mitigate the said risks from materialising themselves.

The risk-based approach recognises that the ML/FT risks faced by each sector and each subject person are different, and allows for resources to be invested and applied where they are most required. It is diametrically opposed to a prescriptive tick-box approach and entrusts subject persons with significant discretion in its application. Thus, a risk-based approach envisages the application of checks that are proportionate to the assessed risk. High risk areas should be subjected to enhanced procedures, whilst simplified or reduced controls may be applied in areas of low risk.

How is this to be achieved? The risk-based approach envisages the application of a risk management process in dealing with ML/FT, including recognising the existence of risks, undertaking a risk assessment, and implementing systems and strategies to manage and mitigate the identified risks.[1]

2.1.1 The Risk Assessment

The cornerstone of the risk-based approach is the risk assessment which has to be carried out at different stages of a subject person's activities. This assessment allows the subject person to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. On this basis, the subject person will be able to draw up, adopt and implement AML/CFT measures, policies, controls and procedures that address any identified risks.

However, each customer exposes the subject person to different risks. A customer-specific risk assessment must therefore be carried out so that the subject person is able to identify potential risks upon entering into a business relationship with, or carrying out an occasional transaction for, a customer. This assessment enables the subject person to develop a risk profile for the customer and to categorise the ML/FT risk posed by such customer as low, medium or high.

Subject persons must subsequently apply the AML/CFT measures, policies, controls and procedures adopted in a manner that they address the specific ML/FT risks arising from the particular business relationship or occasional transaction. Thus, it is important that the said measures, policies, controls and procedures be sufficiently flexible to prevent and mitigate specific risks independently of the extent in which they may potentially manifest themselves. How these measures, policies, controls and procedures are to be applied to particular risk scenarios has to result from the subject person's Customer Acceptance Policy.

[1] *Section 2 of the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures.*

2.1.2 The Risk Areas

The risk areas that the business risk assessment as well as the customer-specific risk assessment are to look at can be divided into four:

- Customer risk;
- Product/service/transaction risk;
- Interface risk; and
- Geographical risk.

The form they may take within the remote gaming sector is explained in further detail in Section 2.2.2 hereunder.

2.1.3 The Risk Assessment as a Dynamic Tool

An effective risk assessment has to be a dynamic one. Subject persons have to ensure that they revise the same when there are significant developments within the environment within which they are operating and within their business structures/activities. Any such changes may affect the risk areas mentioned above and lead to the subject person being exposed to new ML/FT risks. Identifying the same through a revision of the risk assessment allows the subject person to take action to ensure that its measures, policies, controls and procedures are robust enough to cater for these. It is therefore important that subject persons always take into consideration any supranational, national or sectoral risk assessment that may be available when conducting and revising their own specific risk assessment.

Even the customer-specific risk assessment has to be revised when the business relationship entertained with the customer undergoes changes. Once the customer has started to use his account, it is important that the subject person monitors this activity to ensure that it is in line with the customer's profile. Any changes in the customer's pattern of activity must be analysed to determine whether an update of the customer's profile is necessary. The level of monitoring should be commensurate to the risk posed by the particular customer, but systems should also be in place to detect developing risky situations.

2.1.4 Unchanging High Risk Situations

It is important to note that independently of the risk assessment carried out by the subject person, certain instances may still be deemed to be high risk. One such instance is dealing with Politically Exposed Persons ("PEPs"), their family members or close business associates ("persons linked thereto"). In such cases, the regulatory framework itself sets out the measures to be applied to adequately address the risks arising from dealing with the said individuals. This aspect is considered further in Section 3.4.

2.2 Application to the Remote Gaming Sector

2.2.1 The Business and Customer-Based Risk Assessments[2]

All licensees are required to carry out a business risk assessment to identify the ML/FT risks they are exposed to and ensure that the measures, policies, controls and procedures adopted are sufficiently robust to prevent and mitigate the same. The business risk assessment has to be documented and approved by the Board of Directors (or equivalent) of the licensee, and made available to the FIAU and/or to the MGA upon request. The document itself must identify the document version, the date of the latest revision, and the date when the document was last approved by the Board of Directors.

The MGA has completed a sectoral ML/FT risk assessment which enabled it to identify some risk factors that licensees are to take into account when drawing up their business risk assessment. Risk factors within the remote gaming context are considered further in Section 2.2.2. hereunder. Licensees have to also take into consideration and factor in their business risk assessments the outcomes and recommendations of any Supranational and/or National Risk Assessments that may be issued from time to time.

Licensees are expected to revise their business risk assessment whenever there are changes to the environment within which they are operating and within their business structures/activities. Thus, situations such as a widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered should lead to a revision of the business risk assessment. The same applies when the licensee changes its structure or undertakes major operational changes. In the absence of any of the above, licensees have to assess their business risk assessment at least once a year, to evaluate whether any changes thereto are necessary.

Licensees may engage external consultants to assist them in the drawing up and the revision of their business risk assessments. However, it will be necessary for any report, findings and conclusions to be adopted by the licensee who retains responsibility to ensure it complies with its obligation to carry out a business risk assessment.

As regards the customer specific risk assessment, this is to be carried out either prior to the carrying out of an occasional transaction or, in the case of a business relationship, not later than thirty (30) days from when the pre-established threshold set out in Section 3.3.2 is met. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be similarly adjusted.

2.2.2 Risk Factors Specific to the Remote Gaming Sector

i. Customer Risk – The risk of ML/FT may vary in accordance with the type of customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. A customer having a single source of regular income will pose

[2] *For a better understanding of subject persons' obligations relative to the conduct of risk assessments, licensees are to have regard to Regulation 5 of the PMLFTR. Additional insights into the risk-based approach can be derived from the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures.*

a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income streams.

ii. Product/Service/Transaction Risk – Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it on his own or in collusion with others. The use by customers and the acceptance by licensees of specific funding methods should also be treated as high risk factors. This includes cash and other similar or anonymous payment methods that may not leave or disrupt the audit trail, and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The exceptional use by a customer of accounts held or cards issued in the name of third parties is also to be regarded as a high risk factor. Conversely, where a customer transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of ML decreases – these credit or financial institutions are themselves subject persons and one would expect that as part of their CDD obligations they would monitor on an on-going basis any account or card activity.

The sector-specific risk assessment has allowed the MGA to obtain an indication of the risks associated with various products/services/transactions, which indicators have been included in Appendix I to this document, to assist licensees in the conduct of their business risk assessment and the evaluation of the product/service/transaction risk they are exposed to. Licensees are also to refer to the European Commission's Supranational Risk Assessment Report[3], which also includes product-specific risk identification and risk typologies for gambling which may be of assistance. Notwithstanding this, it is understood that each of the licensees' games, payment methods, and technology systems may vary. The above assessments may be taken as indicative of risk profiles, however the point of a risk-based approach, is a subjective assessment by the subject person of the ML/FT risks posed, and any deviation may still be acceptable as long as this is properly justified through an adequate assessment of the ML/FT risk posed (e.g. poker is considered as being an inherently high risk product due to the possibility of collusion between players but the risk it presents may be revised downwards if the poker system used by the licensee has internal, as against external, controls and restrictions which do not allow, or significantly reduce the possibility of, collusion to take place).

iii. Interface Risk – The channels through which a licensee establishes a business relationship and/or through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction. Channels that favour anonymity increase the risk of ML/FT if no measures are taken to address the same. While situations where interaction with the customer takes place on a non-face to face basis will no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the licensee adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations.

[3] *The European Commission published its Supranational Risk Assessment Report on the 26th June 2017.*

A number of technological measures are available to licensees, allowing the same to establish whether or not the customer providing the relative identification details is actually the person he alleges to be. Alternatively, licensees are required to implement additional measures, on a risk-sensitive basis, to sufficiently counter the above mentioned risks. Licensees are guided towards section 3.2 below which provides examples of the technological as well as alternative additional measures which they may adopt to prevent and/or mitigate such risks.

With specific reference to the use of electronic databases, it is to be noted that these only allow for determining whether the identification details provided correspond to those of an actual person but they do not provide sufficient comfort in establishing whether the customer is that individual. Hence, additional measures as referred to in section 3.2 to ensure the veracity of the player's declared identity are to be undertaken.

The interface risk also increases where the customer does not interact directly with the licensee but there is present a third party who involves itself in the placing of wagers on behalf of the customer and/or the withdrawal of winnings. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations. The use of physical establishments by a licensee to extend its network and provide gaming services to customers on its own behalf (i.e. the licensee's) is not considered to be an outright high-risk indicator, subject to certain pre-requisites as set out in Section 3.3.1 being met.

iv. Geographical Risk – The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of a customer have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/FT.

2.3 Risk Scenarios

To understand the level of risk inherent to their business, licensees can make use of risk scenarios, i.e. what would be the likelihood that a customer would be able to launder proceeds of crime through the licensee's undertaking and what would be the impact thereof on the licensee's activities. In so doing, licensees should consider some of the methods used for the said purpose:

i. A perpetrator uses gambling sites to deposit illicit funds and to request the pay out of winnings or unplayed balance. Legitimate online gambling accounts are credited with dirty funds (deposit) followed by gambling on only small amount of funds (including very low volatility games) or transferring the remaining funds to a different player, or to a different online gambling operator. The remaining funds are cashed out as if they were legitimate gambling earnings.

ii. Criminals may use several "smurfs" betting directly against each other using dirty funds. One of the "smurfs" will receive all the funds as an apparent winner, who will then cash out the funds as it they were legitimate gambling earnings.

iii. Criminals may purchase online casino accounts containing funds already uploaded by non-criminal players at a higher price than the real one. They may also invent and bet on fictitious (non-existing) matches or events to ensure winnings.

iv. Purchasing of winning tickets especially where betting is involved.

The above are only indicative examples and licensees should consider whether there are additional ways in which they may be abused for ML/TF purposes.

3. CUSTOMER DUE DILIGENCE

3.1 The Importance of Customer Due Diligence

The determination of a customer's risk profile is essential to allow a licensee to apply a level of Customer Due Diligence ("CDD") commensurate to the identified ML/FT risk. CDD is intended to allow the licensee to know who its customer is and to build a customer profile on the basis of which the licensee would be able to assess the customer's activity to identify any unusual behaviour. Any such behaviour has to be questioned and, if it is found to lead to a suspicion of ML/FT, it also needs to be reported to the FIAU. The documentation and information collected will then assist the authorities in any analysis or investigation of the suspected instance of ML/FT.

3.2 The CDD Measures

CDD consists in four measures:

i. **Identification and Verification of the Customer -** Identification consists in the collection of a series of personal details on the customer. Verification on the other hand consists in confirming the personal details collected for identification purposes through the use of data, information and documentation obtained from independent and reliable sources.

The personal information to be collected, and the extent of verification to be carried out, is to be determined on the basis of risk[4]. Thus, a licensee may vary the identification and verification procedures in accordance with the risk posed by the respective client. The standard identification procedure consists in the gathering of the following personal details:

(a) name and surname;
(b) permanent residential address;
(c) date of birth;
(d) place of birth;
(e) nationality; and
(f) identity reference number where applicable.

However, in low risk scenarios licensees may limit identification to the three personal details set out in (a) to (c) above[5]. On the other hand, in high risk situations, it is possible that a licensee considers the collection of additional personal details as necessary to mitigate the higher risk of ML/FT. Whatever decision is taken, it is however imperative that the identification and verification procedures adopted enable the licensee to determine at all times that the customer is who he claims to be and that they are effective to counteract the risk of identity fraud and impersonation.

Moreover licensees may have systems in place, (including systems implemented for on-going monitoring purposes as stated further on hereunder), which enable them to

[4] As regards the timing of CDD measures licensees must have regard to Section 3.3.2 hereunder.
[5] The personal details to be collected in low risk situations are also the ones which, in terms of Section 3.3.2. (ii) hereunder, a licensee is required to collect at registration stage.

corroborate the location or other personal details of the customer. Where through the use of such systems the licensee detects inconsistencies in the personal information provided by the customer, the licensee's identification and verification processes should consider whether additional identification and verification measures are required. By way of example where an IP address or the location of a bank issuing a credit card used by the customer suggest one or more links to a country other than the customer's country of residence, the licensee has to question this further and assess whether additional identification checks are necessary.

Invariably and in all circumstances verification should be carried out using data, documents or information obtained from an independent and reliable source. Thus, verification can be carried out either by requiring the production of, or obtaining, documents such as identification documents or else through electronic means which allow a licensee to determine to his satisfaction that the customer is who he declared himself to be, or a combination of both, bearing in mind the ML/FT risk to which the licensee is exposed through the particular business relationship or occasional transaction.

Licensees are prone to deal with customers on a non face-to-face basis which, as already indicated in Section 2.2.2 (iii), is an aspect to be taken into consideration to determine the risk of ML/FT the licensee is exposing itself to when entering into a given business relationship or carrying out an occasional transaction. Given these particular circumstances, in using documentary and/or electronic sources for verification purposes licensees are to note the following:

a. Documentary Sources – As a rule, verification of identity has to be carried out by making reference to a government-issued documents containing photographic evidence of the customer's identity (e.g. passport, identity card, driving licence etc.). Where any such document does not allow verification of one's residential address, a licensee can instead refer to and obtain any of the following documents which should not be more than six months old:

    - a recent statement or reference letter issued by a recognised credit institution;
    - a recent utility bill for a service installed and provided at a residential property;
    - correspondence from a central or local government authority, department or agency;
    - a record of a visit to the address by the licensee;
    - an official conduct certificate;
    - any other government-issued document not mentioned above; or
    - the mailing of correspondence via registered mail or by means of a courier which allows the subject person to obtain documentary evidence that the correspondence was effectively delivered at the residential address provided by the customer and signed for by the same.

Documents used for verification purposes need not be obtained as hard-copies but it is also possible to obtain the same electronically through electronic mail, audio-visual means etc. What is important is that documents are clear, legible and of good quality.

As stated earlier, but without prejudice to the general rule in the previous paragraph, licensees may also vary the extent of verification depending on the risk posed by the particular business relationship. In low risk situations it is possible for a licensee to verify a customer's identity on the basis of government issued documents or alternative but reputable information sources, even where these do not contain photographic evidence of one's identity (e.g.: birth certificates, licences issued by government or public authorities, bank statements etc.). However, photographic evidence of identity would still be required where the licensee considers a relationship to be low risk on the basis of its adoption of technology which compares photographic evidence on documents with the customer's actual facial features. Otherwise, the licensee may have to reconsider how it has rated the risk arising from the non face-to-face aspect.

When using documentary sources for verification purposes, licensees are to ensure as much as possible that the documents obtained are authentic or reproduce authentic ones. The authenticity of some documents may be easier to assess than that of others. For example, government-issued identification documents such as identity cards and passports can be checked against standard official templates, and licensees may also be in a position to visually check if the documents include the security features usually present on the same. On the other hand, documents issued by financial institutions, utilities undertakings etc. do not lend themselves so easily to authenticity checks. These checks may be carried out either by the licensee itself or through software programmes which can be in-built in the means used to provide the identification document(s).

Verification requires not only the production of documents but ensuring that the individual providing the document is the one referred to therein. There are circumstances in which the licensee is able to determine as much on the basis of information in its possession (e.g. geo-location information, IP address data, funding method data etc.) which allow it to corroborate the information contained in the documents provided by the customer. Biometric checks, whether carried out through the channel used to convey the verification documents or otherwise, can also be used to confirm that the individual providing the document is the one described therein.

Where the licensee is unable to satisfy either aspect of verification, it is expected that he will undertake additional measures to establish this link. Thus, apart from obtaining identification documents, which in a non face-to-face context would be passed on as copies, a licensee has to determine whether additional, or Enhanced Due Diligence, measures need to be taken. These Implementing Procedures provide examples of measures which subject persons may adopt in such instances though this list is not intended to be exhaustive. Some of these measures include requesting additional identification documents, requiring a first payment through an account held by a customer in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone, or other means, and

requiring it to be returned etc. Different measures may be adopted as long as a subject person is able to demonstrate that they have an equivalent effect.

b. Electronic Sources – These include sources like E-ID (or Bank-ID) and electronic commercial databases. Even in this context, licensees have to consider the question of reliability. Sources which are considered as equivalent to official government documents are to be considered as bearing the same level of reliability. When using electronic commercial databases it is important that licensees consider what sources of information are feeding into the database so as to ensure that these are sufficiently extensive, reliable and accurate, and, in any one specific case, what sources are returning a positive and/or negative result on the customer. Thus, a licensee needs to understand the parameters for searches carried out using these kind of databases as well as how the provider ensures that data is kept current and up to date.

   Moreover, the use of electronic sources may still require licensees to undertake additional measures to ensure that the individual whose identity has been confirmed on the basis of these sources is one's actual client. This would be the case when making use of electronic commercial databases as, in the absence of in-built automated checks, a positive result only means that there is an individual whose personal details correspond to those provided by the client but not that the client is that individual. On the other hand, electronic sources like E-ID and Bank-ID, which can be accessed only through the use of credentials held by a specific individual, are deemed to provide a sufficiently strong link and therefore no additional measure needs to be undertaken.

There may be situations where the sources used for verification purposes may not contain any reference to the residential address of the customer. In these cases, a licensee may either request an additional document to verify the residential address provided, or it is possible that the licensee already has information such as IP addresses, device location information etc. which corroborate the residence of the customer. The latter may come especially helpful where verification is carried out using E-ID and the licensee may find it particularly difficult to request a documentary source to verify the customer's residential address.

ii. **Identification and Verification of the Beneficial Owner –** Subject persons in general are also required to identify and verify the identity of the beneficial owner. As a general rule, licensees should make sure that customers are registering an account to play and transact on his/her own behalf. This can be achieved by including specific wording in the terms and conditions that a registering player must explicitly accept, together with a declaration in the form of a tick box that a player is registering to play on his own behalf. Licensees are not expected to merely rely on the said declaration but have to ensure that their ongoing procedures allow for the detection of possible instances where the player is actually playing on behalf of third parties.

It is acknowledged that in the majority of cases licensees will not encounter situations involving beneficial owners. However, these situations cannot be excluded completely as licensees may be entertaining business relations with one or more players funded by a syndicate. In such circumstances, where the funds being wagered are collected from

multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and licensees would therefore have to identify them and verify their identity.

Where the licensee's business model includes registered player accounts used by companies (corporate accounts) as a means to hedge matchbook exposure, together with business models such as the ones explained in 3.3.1 below, the applicable beneficial ownership requirement relates to the beneficial owners of the companies/operators registering those accounts, without prejudice to any other requirements included in these Implementing Procedures. Licensees are furthermore required to distinguish between an ordinary gaming account belonging to a consumer, and such other accounts being of a different nature.

iii. **Obtaining Information on the Purpose and Intended Nature of the Business Relationship** – CDD requires that a subject person understands why a prospective customer is seeking to acquire a specific service or product from the same. Within the context of the remote gaming sector, the purpose behind the opening of a gaming account is quite self-evident and, limitedly to this aspect, it is not required that licensees obtain any additional information from their customers.

However, this CDD measure also requires the development of a customer business and risk profile, the key element being having sufficient information available so as to allow the detection of unusual activity in the course of a business relationship.

To this end, licensees have to collect sufficient information and, where it is necessary, documentation to establish a customer's source of wealth as well as his expected level of activity. Source of wealth consists in determining the activities which generates the customer's net worth and whether the same justifies his projected and actual level of account activity: it is not and should not be considered as a forensic accounting exercise.

As to the extent of the information that licensees are to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment. Where the risk is medium or lower, a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can suffice. Social media can also be used as a source of information. However, where the risk of ML/FT is higher or licensees have doubts as to the veracity of the information collected, the information obtained would need to be supplemented by means of independent and reliable information and documentation.

In developing a customer business and risk profile, licensees may also consider using statistical data to develop behavioural models against which to eventually gauge a customer's activity rather than collect source of wealth information. Where a licensee opts to adopt this approach, it can use data collected from the following sources:

a. Official economic indicators such as average national income, average disposable income etc. issued by national public bodies or reputable financial institutions. These

indicators should allow a licensee to determine the average wagering power of players from a given jurisdiction.

Or

b. Data collected over a period of time by the licensee itself and which allows the licensee to create the profile of an average player. It is important to note that the reference is not to the statistical data on the individual player (which would still be useful for on-going monitoring purposes) but to statistical data obtained from a range of players. Licensees should therefore only use this specific alternative where their customer-base is wide enough to allow the creation of an average profile. New licensees would therefore not be expected to use this method unless they are able to obtain gaming data from another licensee offering the same games within the same markets and having a similar business model to the one being adopted by the new licensee.

It is important to note that the use of statistical data is incompatible with high risk situations as the transactional pattern will fall outside the average behavioural model. In such circumstances licensees would have to collect source of wealth information as set out above.

In developing a customer business and risk profile, licensees would be laying down the groundwork necessary for the scrutiny of activity required to meet part of their on-going monitoring obligation as explained hereunder.

iv. **On-Going Monitoring** – In carrying out on-going monitoring of a business relationship, licensees have to:

a. Ensure that the documents, data or information held are kept up-to-date, i.e.:

1. Obtain fresh identification documents when the expiry date of identification documents held on file is reached. This can be done on a risk-sensitive basis or be linked to specific trigger events.

2. Question the data and information already in its possession whenever any inconsistencies with the same arise however noticed.

This is not a requirement to carry out CDD afresh but to ensure that a licensee's knowledge of the customer and the information in its possession is kept up to date. Licensees should determine on a risk sensitive basis whether any new information needs to be verified or whether changes are so substantial as to require the carrying out of its customer risk assessment and/or its CDD afresh.

And

b. Scrutinise the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the licensee's knowledge of the customer and his business and risk profile. Where a licensee notices that a customer's account

activity is not in keeping with what it knows or expects from the customer (e.g. activity not justified on the basis of a customer's source of wealth or not in keeping with the average profile or account activity noted to date, activity does not reflect a customer's usual transactional patterns etc.), the licensee has to question this unusual activity and, where necessary, establish what is the source of the funds used for the said activity.

Unlike source of wealth, source of funds relates to how the funds used for a particular transaction were obtained by the customer. As long as a transaction falls within the profile of the customer and his regular activity, there is no need for subject persons to obtain specific information and documentation on the same; it is only where a transaction presents a departure from the known or expected behaviour of a customer that a subject person is required to question the same. The subject person is to understand what the reason for this divergence is and obtain sufficient information and documentation on the matter, which might include establishing the customer's source of funds. It is also one of the situations in which the risk profile of the customer may have to be revised.

Depending on the extent of the divergence noted and the reasons provided by the customer, licensees may have to reconsider their initial risk assessment and, to the extent that they were conducting on-going monitoring based on statistical data, collect specific information and, if applicable, documentation on the customer's source of wealth.

As with anything else, the level of on-going monitoring will inevitably depend on the risk profile of the customer but even in low risk situations there must be a degree of oversight taking place to ensure that the business relationship still warrants to be considered as a low risk one. A change in circumstances may lead to an eventual re-evaluation of the risk the licensee is exposed to and intensify the CDD measures undertaken.

3.3 Applying the Customer Due Diligence Measures

3.3.1 Business Relationship v Occasional Transaction

A licensee will be considered to be a subject person whenever it is providing services to a customer so that he may wager a stake with monetary value in a game of chance, including those with an element of skill. Licensees are most likely to entertain business with customers who are predominantly individuals and who act in their own name and on their own behalf. In so doing, licensees open an account for all, or at least the great majority, of their customers. This is considered to be indicative of a relationship that is expected to have or has an element of duration and therefore it is considered that there subsists a business relationship between the licensee and its customer. Subject to what is stated in Section 3.3.2 hereunder, whenever there comes into a being a business relationship licensees are to apply CDD measures.

Whilst it is acknowledged that the possibility of licensees carrying out occasional transactions is somewhat remote, it is important to note that in the eventuality of this scenario materialising itself, licensees are still obliged to apply CDD measures albeit not all of them. In the case of occasional transactions, i.e. whenever a licensee is to carry out a transaction outside of a business relationship,

the licensee would only be expected to apply the initial two CDD measures indicated in Section 3.2 (i) and (ii) above. Whenever an occasional transaction presents a high risk of ML/FT, it is further recommended that the licensee identifies what is the source of the funds used.

Licensees at times make use of physical establishments to extend their customer reach. Where the customer only makes use of the terminals present within the physical establishment so as to open an account in his own name with the licensee or to use such an account, the interaction between the two would still be considered to be a business relationship subject to the requirements envisaged in this section.

On the other hand, if the customer makes use of an account held by the operator of the physical establishment to carry out occasional transactions with the licensee, the licensee has to ensure that the AML/CFT policies and procedures applied by the physical establishment allow for the identification and verification of the customer once the relative threshold is reached, as set out hereabove. Where these physical establishments are located in a jurisdiction other than Malta but are (i) subject to regulation and supervision; and (ii) have to meet AML/CFT obligations equivalent to those envisaged under Directive 2015/849/EU ("the Directive"), the licensee may consider that it is meeting its own AML/CFT obligations under Maltese law if it ascertains itself that the operator of any such physical establishment is effectively complying with AML/CFT obligations equivalent to those envisaged under the Directive as applicable in that other jurisdiction. Hence, the licensee is expected to:

i. Ensure that the operator of the physical establishment is of good standing and repute;

ii. Identify the operator of the physical establishment (including verifying the identity of the same) and ensure that there are no obstacles to the effective implementation of AML/CFT requirements by the said operator;

iii. Obtain a copy of the AML/CFT policies and procedures adopted by the operator of the physical establishment and ensure that it understands what these actually entail;

iv. Be provided with the details of any customers identified by the operator of the physical establishment, together with any other CDD information and or/documentation collected by the operator of the physical establishment and requested by the licensee; and

v. Scrutinise the activity taking place through the physical establishment's account and ensure that the operator of the physical establishment does not adopt practices which allow the circumvention of its AML/CFT obligations.

In the event that the above conditions cannot be met, licensees are to carry out CDD measures with respect to each customer making use of the account held with the licensee by the operator of the physical establishment.

3.3.2 Application, Extent and Timing of CDD Measures

Regulation 9(1) of the PMLFTR provides that CDD measures are to be applied when carrying out transactions amounting to Euro two thousand (€2,000) or more, whether carried out within the context of a business relationship or otherwise. The moment in time when CDD obligations (as well as

the obligation to carry out a customer risk assessment as per Section 2.2.1) are triggered and have to be applied by the licensee is therefore to be determined as follows:

i. In the case of an occasional transaction, the obligation to carry out CDD will be dependent on the value of the said transaction reaching or exceeding Euro two thousand (€2000). Licensees will themselves subject to the said obligation also in the case where they execute a series of transactions which, though individually below the said threshold, would cumulatively meet or exceed the Euro two thousand (€2000) threshold.

   Transactions are considered as linked if for example they are carried out by the same customer through the same game or in one gaming session. In this context, the licensee has to identify the customer, verify his identity and, if deemed high risk, consider determining what is the source of the funds used for the said transactions. It is left to the individual licensee to determine if these measures are to be carried out when the player wagers his stakes or when he collects any winnings. It is to be remarked that carrying out CDD at the earliest possible can limit situations in which a licensee receives tainted funds and subsequently finds it hard to dispose thereof.

ii. The Euro two thousand (€2,000) threshold is also applicable in situations where the customer opens an account with a licensee, leading to the establishment of a business relationship between the two. Thus, CDD measures are not in principle applicable until the said threshold is reached. However, to ensure the proper functioning of AML/CFT controls, licensees are required to apply a minimum level of CDD measures prior to the said threshold being reached. Thus, simultaneously with the opening of an account, licensees are to identify (but are not obliged to verify the identity of) the customer by collecting the personal details which in terms of Section 3.2(i) are set as the minimum applicable in case of low risk business relationships.

   Moreover, even before reaching the €2,000 threshold, licensees are to have systems in place which allow them to apply a level of on-going monitoring. Through these systems, licensees should ensure that:

   a. They are able to determine the moment in time when the Euro two thousand (€2,000) threshold is met;

   b. The player does not avoid the application of CDD measures by circumventing the Euro two thousand (€2000) threshold *per* account. Thus, it would be expected that licensees have systems in place as already described in Section 3.2 (i), which may include systems that detect IP addresses, device location etc., so as to disallow the opening of multiple accounts by the same person, whether under his own name or using the identities of third parties, be they real or fake;

   c. They are able to deny the application for the opening of an account by a person who has inputted manifestly false details; and

   d. They are able to detect instances which give rise to a suspicion of ML/FT as referred to in Section 3.7 hereunder.

Given the limited nature of on-going monitoring to be carried out at this stage, there is no requirement for licensees to create a customer business and risk profile. Thus, there will be no need for any source of wealth information to be collected at this stage. However, if licensees already notice inconsistencies at this stage between the information provided by the customer and any other information they may acquire through interacting with the same, they are to question these discrepancies and take any remedial action they deem necessary.

As regards the Euro two thousand (€2,000) threshold, this is to be applied vis-à-vis funds deposited onto an account, whether in a single transaction or a number of transactions adding up to the said amount. To the extent that a licensee can distinguish between customer deposits and funds made available by the licensee itself, such as bonuses given by the licensee itself, or winnings accumulated onto an account on the other, the Euro two thousand (€2,000) threshold is to be calculated only on the basis of deposits made by the customer. The Euro two thousand (€2,000) deposit threshold can be calculated either:

a. On a daily basis taking into account all deposits effected by a customer since the establishment of the business relationship; or

b. On the basis of a rolling period of one hundred and eighty (180) days.

In the latter case, a licensee would have to consider whether a customer's overall deposits in the previous one hundred and eighty (180) days have met or exceeded the Euro two thousand (€2,000) threshold, with licensees being able to make said determination either each time a customer effects a deposit or at the end of each day in which a customer effects one or more deposits.

Once the Euro two thousand (€2,000) threshold is reached, licensees have to carry out a customer risk assessment in terms of Section 2.2.1 and meet their remaining CDD obligations. The latter consists in completing the CDD measure set out in Section 3.2(i), carrying out the CDD measures referred to in Section 3.2 (ii), where applicable, and (iii) strengthen their on-going monitoring regime to ensure they are able to scrutinise customer activity on the account for any usual activity. However, based on the risk inherent in a business relationship or occasional transaction and to the extent allowed by law, a licensee may want to vary the extent of the CDD measures undertaken.

The extent of the CDD measures applied may therefore vary on the basis of risk but must always be commensurate to the risk inherent in a given business relationship or occasional transaction. Enhanced Due Diligence ("EDD") is to be applied whenever the licensee identifies any high risk situations. This entails taking more stringent steps in the application of CDD which may include collecting more detailed information on source of wealth and source of funds purposes as well as any additional measures deemed necessary to mitigate the risks identified through the customer risk assessment. The latter may include the application of additional measures to ascertain and verify the identity of the customer as referred to in Section 3.2(i) above.

Not only does risk impinge on the extent of the information to be collected for source of wealth purposes but it is also possible that in situations where the level of activity is minimal the obligation to collect said information will be delayed until a change in activity occurs. For example, a customer who manages to reach the Euro two thousand (€2,000) threshold over a year will present a lower level

of risk than one who reaches the said threshold over a period of a week. Considering that most people have the ability to wager this amount over a year, obtaining information on the source of wealth would not be of any added value to assist in addressing any form of risk. However, like any decision taken in the course of applying the risk-based approach, it is important that any determination made by the licensee be properly documented.

In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the licensee obtains any necessary information from the customer concerned. However, until such time as the licensee obtains the necessary information and documentation from the customer to meet its CDD obligations, the customer is not to be allowed to effect any withdrawals from the account independently of the amount involved. Moreover, if following the lapse of thirty (30) days from when the Euro two thousand (€2,000) threshold is met, the customer has not made the requested information and documentation available, the licensee is to terminate the relationship as described in Section 3.6 hereunder.

As regards on-going monitoring, licensees are to vary the same so that it is brought in line with what has already been stated in Section 3.2(iv) hereabove.

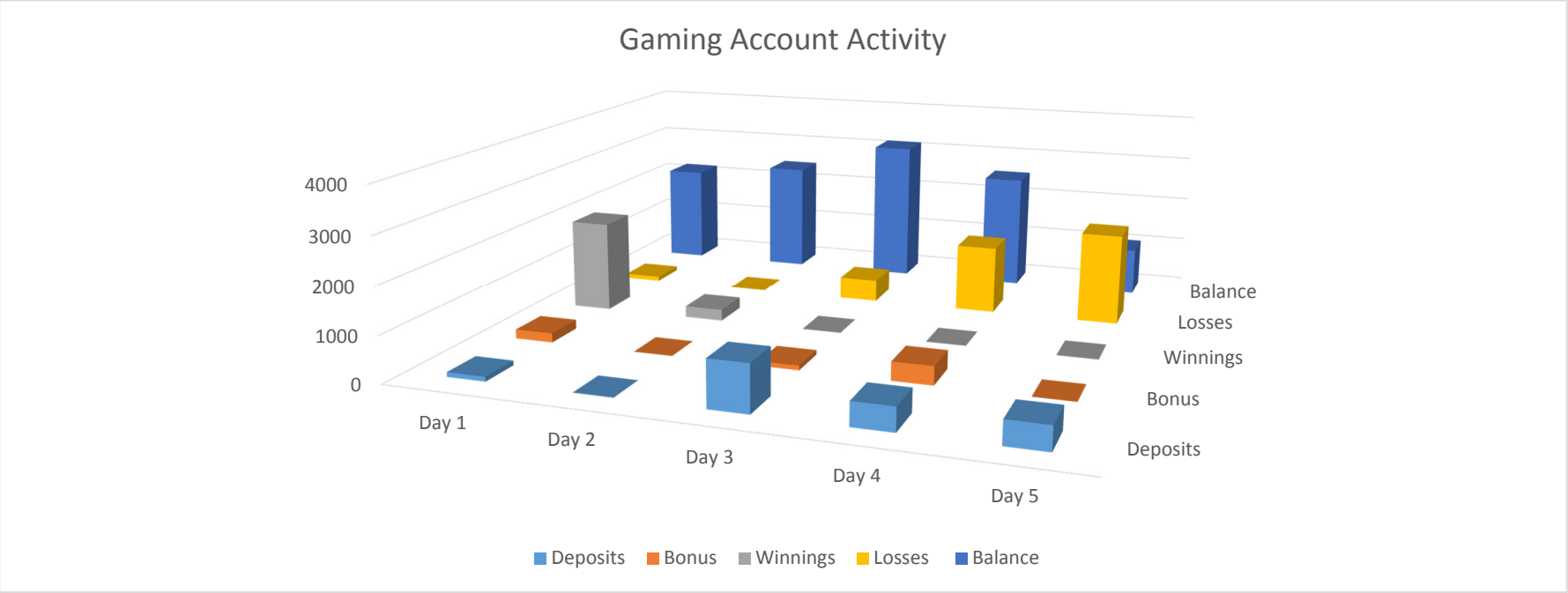


Fig 1 **Euro 2000 Deposit Threshold Determination**

Threshold is reached upon on Day 5 when the total deposits made by the Player reach €2,100 even though on Day 1 (a) the player had €2,000 in winnings and (b) his account balance was already in excess of €2,000.

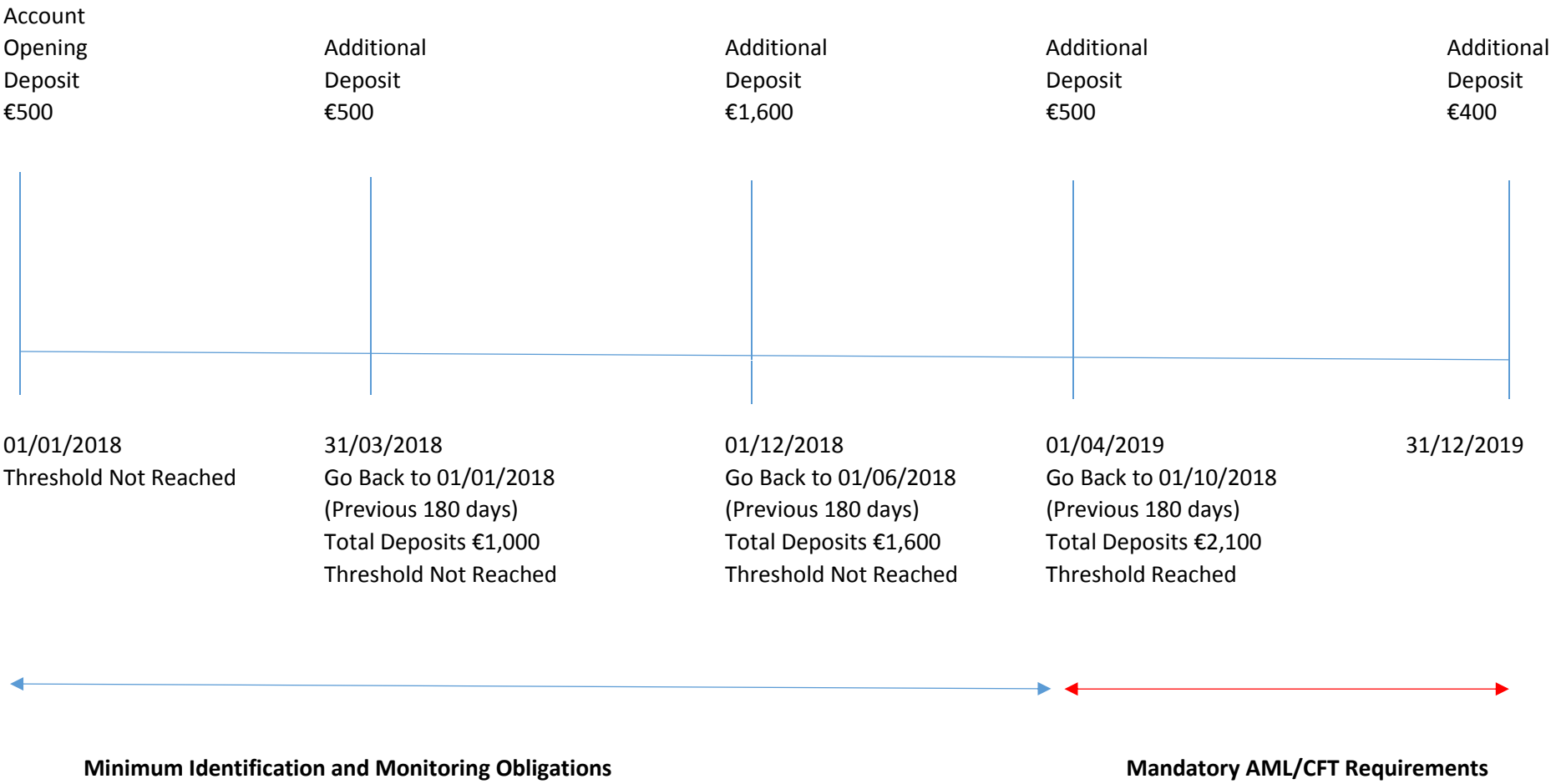
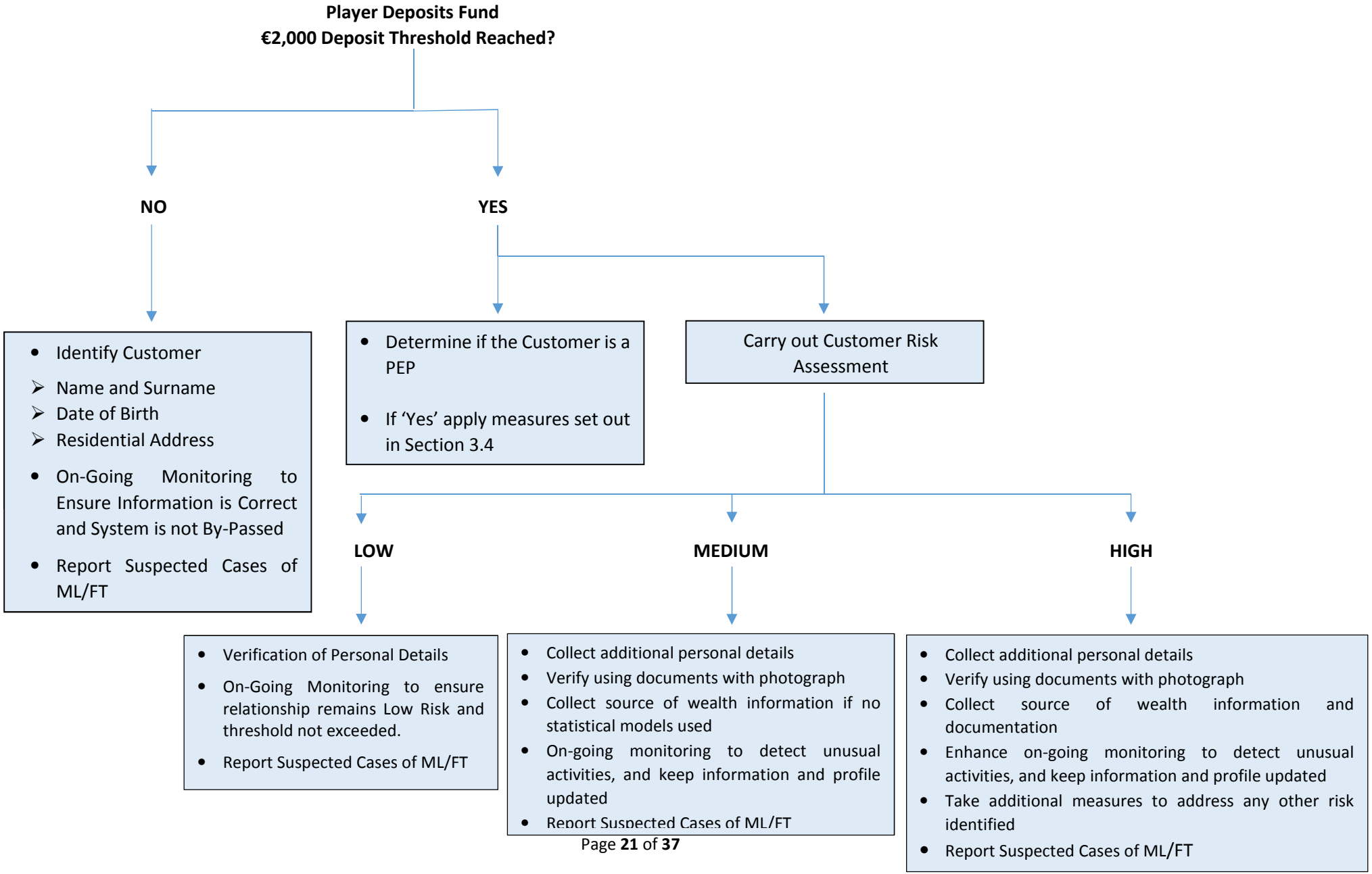


FIG. 2 Application of the Rolling Period

FIG. 3 Customer Due Diligence Obligations



3.4 Politically Exposed Persons

Situations involving so-called 'Politically Exposed Persons' ("PEPs") require the application of EDD measures, independently of the outcome of the customer risk assessment. This entails having to determine whether a customer is a PEP or otherwise and, should this be the case, apply of the following pre-established EDD measures:

i. Obtain senior management approval to service the PEP;

ii. Establish what is their source of wealth and, where applicable, their source of funds; and

iii. Conduct enhanced on-going monitoring of the customer's activity.

Licensees may carry out or, in the case of (iii) above, implement these measures at any point in time between the establishment of the business relationship and the point in time when the €2,000 threshold is met, but not later from the lapse of thirty days from when the said threshold is reached. In the case of an occasional transactions licensees have to carry out the said measures, in so far as they are applicable, prior to carrying out the transaction in question.

Screening for PEP status has to be carried out regularly but it is important that this is done within thirty days of the €2,000 threshold being met, even where licensees may have already screened customers to determine if they were PEPs earlier on in the course of the business relationship. Should a customer who had not been identified as a PEP at on-boarding stage result to have become one, the licensee concerned has to carry out or implement the measures described in paragraph (i) to (iii) above within the thirty day window, failing which it would have to terminate the business relationship with the said customer as described in Section 3.6 hereunder.

Moreover, licensees are to note that:

i. The information required to determine whether a customer (or its beneficial owner) is a PEP can be obtained either from the customer himself (e.g. by completing a standardised self-declaration as to his status and, to the extent which may be applicable, that of his beneficial owner) or by using reliable electronic databases to screen their customer database.

   However, where a licensee relies on the customer to disclose and declare whether he is a PEP or otherwise, the licensee is required to (a) provide the customer with guidance as to what is meant by a PEP, including by providing him with a definition of the said term; and (b) confirm on a risk sensitive basis the information so obtained.

   It is important that as part of the licensee's on-going monitoring procedures there be included the regular revision of a customer's PEP (or non-PEP) status as this can change over time. Each time new PEPs are identified, senior management approval has to be obtained for a business relationship to continue.

   As to the frequency of this revision, this is dependent on the risk inherent to the business relationship or occasional transaction when considering risk factors other than the

customer's PEP status – the more numerous the risk indicators, the higher the risk and therefore the more frequent the screening to be carried out.

ii. Where licensees are using statistical methods to establish a customer's risk and business profile as referred to in Section 3.2(iii) hereabove and a PEP's behaviour falls within the said profile, licensees may decide to establish his source of wealth and/or of funds only when his behaviour departs from said model. In the latter circumstance, as well as where the subject person does not adopt any such statistical methods, subject persons have to obtain information on the PEP's source of wealth and source of funds.

In such circumstances it would not be reasonable to merely rely on information provided by the customer but the licensee has to verify the same on the basis of independent and reliable sources. As to the degree of information or documentation to be obtained, this should be calibrated to reflect the overall risk of the relationship or occasional transaction and the volume of activity experienced.

iii. Even though situations involving PEPs are mandatorily subject to EDD measures, licensees are still required to carry out the Customer Risk Assessment referred to in Section 2.2.1. The occasional transaction or business relationship may present additional factors indicative of a high risk of ML/FT which the licensee may have to address through measures other than those which have to be applied when dealing with PEPs.

Licensees are to note that the obligations relative to PEPs are not limited to PEPs themselves but have also to be applied to their family members and persons known to be their close business associates.

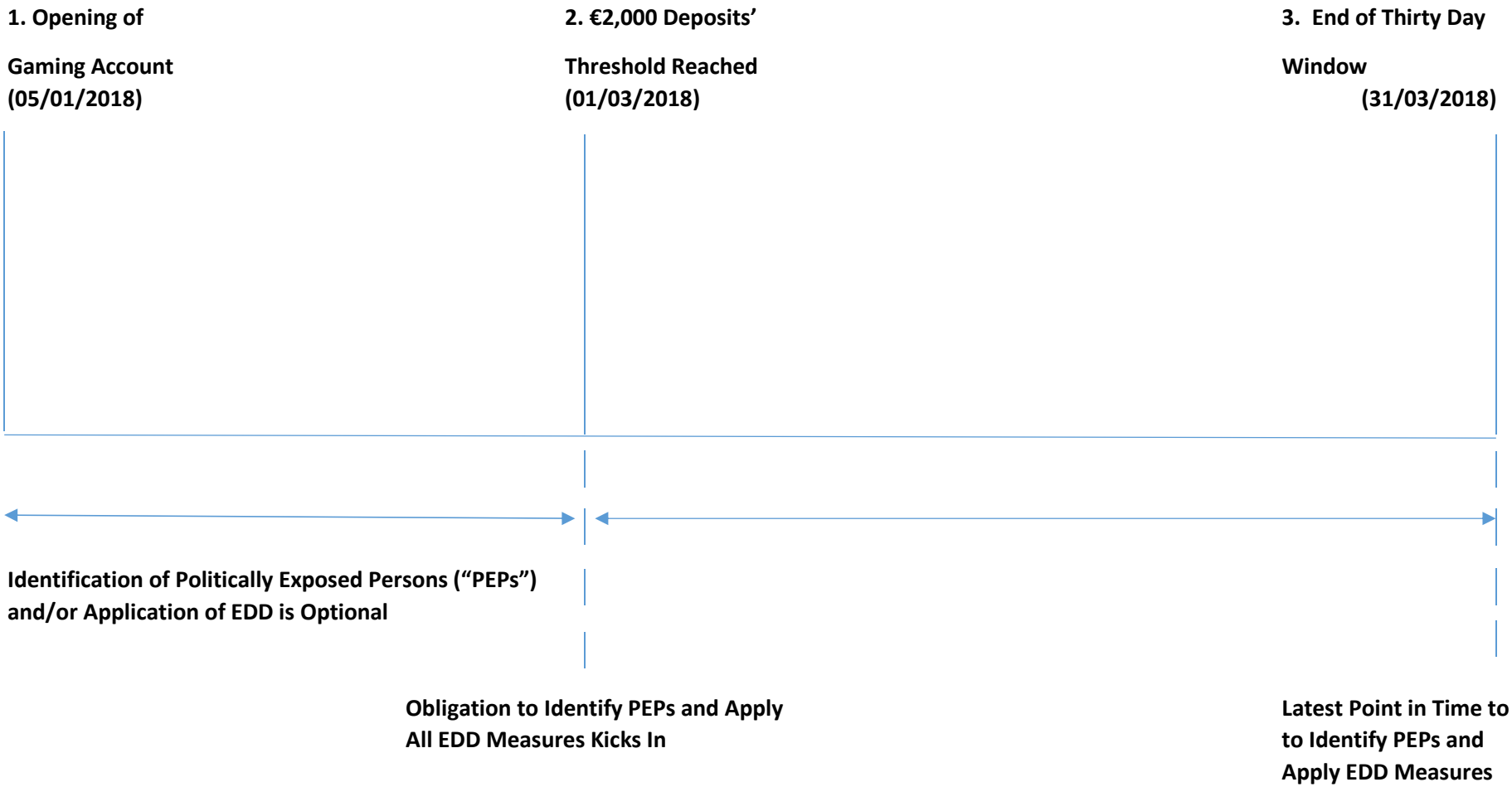


FIG. 4 Politically Exposed Persons – Timeline

3.5 Application of CDD Measures to Existing Customers

Licensees may already have a number of existing business relationships in respect of which they have to apply CDD measures. Given that it may not be possible to do so at once, licensees can carry out this review on the following basis:

i. Licensees are to consider whether any pre-existing procedures they may have been applying are sufficient to meet their CDD obligations as explained in this document. To the extent that this is the case, licensees can continue applying the same while paying special attention to their on-going monitoring obligations as set out hereabove.

ii. Where a licensee had no pre-existing procedures that satisfy their CDD obligations, or the procedures in place did not satisfy all of the said requirements, the licensee is to determine whether an existing customer has already met the Euro two thousand (€2000) threshold. In so doing, licensees may either have regard to all the deposits effected in the course of the business relationship or apply the same rolling period referred to in Section 3.3 hereabove.

iii. Where the said threshold has yet to be met, licensees are to consider these business relationships in the same manner as business relationships opened following the transposition of the Directive into Maltese law. Thus, they are to ensure that they have duly identified the customer and that they are carrying out the necessary level of on-going monitoring as provided for situations where the €2000 threshold has not been met as set out in Section 3.3.2(ii).

iv. Where the Euro two thousand (€2000) threshold has already been met, licensees are to apply their new revised procedures to their existing customers on a risk-sensitive basis but within a reasonable time period.

3.6 Inability to Complete CDD Measures

Situations may arise in which a customer will not be willing to provide a licensee with the necessary information or documentation even though the licensee may have repeatedly solicited him to forward said information or documentation. In this case, in addition to keeping a record of all the attempts made:

i. The licensee is to terminate its business relationship with the customer, i.e. it is not to allow any activity of any kind on the account held in the customer's name or provide any other service to the customer. To this end, a licensee may decide to either close the account or to keep it blocked and suspended in its entirety.

ii. The licensee is to consider whether there are any grounds giving rise to suspicion of ML/FT. The reluctance of the customer to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/FT. The licensee should consider all factors and information it has at its disposal, including for example the payment method used, the games played and the customer's playing trends and patterns, any information on the customer already held by the licensee, including his jurisdiction of residence, and information which can be obtained through sources such as the internet etc. If there are

grounds to suspect ML/FT, then the licensee has to submit a Suspicious Transaction Report ("STR") to the FIAU. Licensees are also to refer to Section 5.3 of this document.

iii. Where there are no grounds to suspect ML/FT or the transaction has not been suspended by the FIAU or by operation of the law, nor is there an attachment or freezing order, the licensee would have no reason rooted in the AML/CFT regime justifying the retention of any such funds.

Thus, where funds are to be remitted back, the licensee should:

a. Consider whether there is any other legal impediment to the remittance of the funds; and
b. Remit the funds to the same source through the same channels used to receive the funds.

In the event the licensee is unable to remit the funds to the same source through the same channels, it will inevitably have to request fresh instructions from the customer. In the event that these instructions give rise to a suspicion on the part of the licensee, it should submit a STR and suspend the remittance pending the FIAU expressing its opposition or otherwise to the said transaction.

In the circumstances described above, whenever a licensee is remitting funds it is also, to the extent that this may be possible, indicate in the script/instructions accompanying the funds that these are being remitted due to their inability to complete CDD.

3.7 CDD and Suspicions of Money Laundering or Funding of Terrorism

In the event that in the course of a business relationship or in carrying out an occasional transaction, a licensee develops a suspicion or has reasonable grounds to suspect that activity on an account or a customer is linked to ML/FT, the licensee has to immediately meet all CDD requirements independently of the point in time when said suspicion arises. **Any timeframe or threshold, whether set by law or by the licensee itself, are rendered inapplicable and the licensee is obliged to submit a STR as soon as possible.**

4. RELIANCE, AGENTS AND OUTSOURCING

The AML/CFT regulatory framework does allow for the exercise of reliance, with the subject person relying on the information and documentation collected at customer on-boarding stage by any other person or entity in an EU Member State or a reputable jurisdiction who is subject to AML/CFT requirements and supervision equivalent to those required in terms of the Directive. In determining as much, a subject person can refer to FATF/Moneyval evaluation reports, IMF Country Reports etc.

4.1 Reliance

When exercising reliance, a subject person has to obtain the identification information from the third party it is relying upon but does not need to request the customer to provide it with any verification documents. However, the subject person must have an agreement with the third party being relied upon for any such documents to be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Moreover, the subject person remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring. Licensees will be able to exercise reliance to meet their CDD obligations as long as the conditions described above are met.

4.2 Agency Relationships

In some instances, the regulatory regime applicable to the activities carried out by a subject person allows it to appoint agents as a means to extend their reach and carry on its business. Any business transacted by means of an agent is to be considered as business transacted by the subject person. As such any customer on-boarded or serviced by the agent has to undergo the same checks and controls as customers on-boarded and serviced by the subject person itself. It is therefore up to the subject person to ensure that its AML/CFT controls, policies, measures and procedures are applied to any such customer and the subject person may require that these be carried out by the agent.

Within a remote gaming context, an agency relationship would arise where the licensee makes use of physical establishments as set out in Section 3.3.1 as an extension of itself. In the instances set out therein, the physical establishment would allow a (prospective) customer to form a business relationship with, carry out an occasional transaction through or otherwise access the services or products offered by the licensees through the terminals present within the physical establishment.

4.3 Outsourcing

The appointment of an agent is to be distinguished from outsourcing where the subject person engages a third party service provider to implement AML/CFT controls, policies, measures and procedures rather than carrying out the same itself. It is highly unlikely that the third party so engaged would limit its activities to those contracted with the subject person and it is usual for the third party service provider to have a number of contracts with different subject persons for the carrying out of the same service/s on their behalf.

Where a licensee considers to outsource the implementation of its AML/CFT obligations, it is important that the licensee bears in mind that it will remain responsible at all times for compliance with the said obligations. Moreover, there are certain aspects that cannot be outsourced including

determining whether to on-board a customer or pursue a business relationship on the basis of risk and the MLRO function.

Additional conditions are also to be applied to outsourcing arrangements, including, but not limited to, ensuring that:

a. The service provider engaged is in good-standing and has the necessary resources to fulfil the requirements being outsourced;

b. The outsourcing arrangement has to be reduced in writing and clearly lay down what are the respective obligations of the subject person and of the service provider;

c. There will be periodical assessments of how the service provider is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively; and

d. That any information and documentation obtained by the service provider in carrying out the outsourced functions are accessible and available to the subject person.

The common element in all these cases is that the subject person, and therefore the licensee, remains always responsible for ensuring it is adhering to its AML/CFT obligations. It is to be noted that the purchase, or licensing, of software tools that assist a licensee in meeting its AML/CFT obligations is not considered outsourcing for the purpose of this section, as long as the person operating the software is the licensee itself, and not the software supplier.

5. REPORTING SUSPICIOUS ACTIVITY and TRANSACTIONS

5.1 The Money Laundering Reporting Officer

Subject persons are required to appoint a MLRO whose main responsibility is to consider any internal reports of unusual or suspicious transactions and, where necessary, follow up the same by filing a STR with the FIAU. The MLRO is also considered by the FIAU as its main contact point within the subject person and he is to act as the main channel through which any communications with the FIAU are to be conducted. Given these especially onerous obligations, the MLRO should be an officer of the subject person who enjoys sufficient seniority and command to be able to act independently of management.

The effectiveness of the MLRO depends on his being present where the subject person is actually conducting its activities, i.e. the jurisdiction from where the operations of the given licensee are being conducted and where the MLRO can have access to all the necessary information/documentation to effectively carry out his obligations.

5.2 Group Compliance Officer

In terms of Regulation 5(5)(c) of the PMLFTR, licensees have to consider whether, considering the nature and size of their business, it is necessary to appoint a Compliance Officer to oversee the daily implementation of its AML/CFT measures, policies, controls and procedures. In relation to a group consisting of two or more subject persons, it is possible to appoint a Group Compliance Officer responsible for overseeing the activities of all the entities forming part of the said group who may be assisted by other officials overseeing the implementation of AML/CFT obligations by individual group entities.

However, this does not apply in relation to the MLRO as each individual subject person must have its own separate MLRO, including where the subject person forms part of a group consisting of two or more subject persons, unless such entities are deemed to be a single subject person due to having a corporate group licence in terms of the applicable gaming legislation. This is due to the disclosure restrictions, and exemptions thereto, applicable to subject persons under the PMLFTR.

Whether or not a licensee takes advantage of the above, it is to be remembered that the FIAU considers the Maltese licensee as being responsible for compliance with its obligations under the Act, the PMLFTR and Part I of the Implementing Procedures.

5.3 Reporting Suspicious Activity and Transactions

Subject persons are required to have internal and external procedures providing for the reporting of suspected or known instances of ML/FT. The internal reporting procedures must allow for subject person's employees' to even report a suspected instance of ML/FT to the MLRO when their immediate superior is in disagreement with them. It will be then up to the MLRO to determine if the information available can be considered as sufficient for a STR to be made to the FIAU.

When the ML/FT suspicion is linked to a transaction still to be processed, it is important that the subject person refrains from carrying out the same, files a STR and delays the execution of the transaction for one (1) working day following the day on which the licensee files the STR. During this

time the FIAU has to determine and communicate to the subject person whether it objects to the execution of the said transaction. Where refraining from carrying out the transaction is not possible or doing so would prejudice an analysis or investigation of the suspected instance of ML/FT, the subject person may decide to proceed with the transaction's execution. The impossibility to refrain from processing a transaction must arise from the nature of the transaction itself and the subject person must then submit a STR to the FIAU immediately afterwards.

Licensees already had the obligation to report transactions they suspected to be linked to ML. However, as a subject person the reporting obligations of a licensee are to be extended as follows:

i. The filing of a STR is not limited to transactions suspected of ML but extends to any suspicion that the licensee becomes aware of in the exercise of his business that a person is linked to ML/FT or that ML/FT is being committed or may be committed independently of whether any transactions have taken place or otherwise.

ii. A STR has to be filed not only in suspected instances of ML but also in situations where there is a suspicion of FT or that funds are the proceeds of criminal activity.

iii. Reporting has to take place also when licensees have reasonable grounds to suspect that ML/FT may be taking place, this being a more objective ground for reporting. This implies that a further obligation to report arises where, on the basis of objective facts, the subject person ought to have suspected that ML/FT existed.

What kind of behaviour or transactions should alert licensees to a possible case of ML/FT and result in an internal report to the MLRO? There are red flags that may alert licensees but they are merely indicative and need not necessarily taken on their own point to ML/FT taking place. Red flags are not intended to automatically result in filing a STR with the FIAU but are merely indicators that should lead licensees to question the player's behaviour – it is only if there is no reasonable explanation for the same that an internal report is to be made to the MLRO for him to determine whether there is a suspicious of ML/FT and, if necessary, file a STR with the FIAU.

The following is a list of possible red flags which licensees may wish to consider:

- Customer does not cooperate in the carrying of CDD.
- Customer attempts to register more than one account with the same licensee.
- Customer deposits considerable amounts during a single session by means of multiple pre-paid cards.
- Customer deposit funds well in excess of what is required to sustain his usual betting patterns.
- Customer makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patters of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.

- Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Customer displays suspicious behaviour in playing games that are considered as high risk.

In their considerations whether to submit a report to the FIAU, licensees are to bear in mind that AML legislation is intended to address and attack serious crime which usually either involves amounts that can be safely said to be other than minimal or circumstances which show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

Thus, by way of example, identity fraud and charge backs may give rise to ML but a licensee will only be subject to reporting obligations under AML/CFT legislation if they result in funds derived from these activities being deposited with or held by the licensee. However, in such situations licensees should not report single instances involving small amounts but are to consider whether they can detect a bigger pattern or scheme. It is to be remembered that the MLRO has to consider whether an internal report gives rise to a suspicion of ML by taking into account all relevant information which, in this instance, would include considering whether there are common denominators between repeated instances of chargebacks or identity fraud. These may include common or related persons, common IP addresses etc.

5.4 Reporting to the Relevant Authority

Licensees are considered as subject persons on the basis of the licence issued to them by the MGA. Hence, whenever in the course of any activity carried out in terms of the said licence, they come to know, suspect or have reasonable grounds to suspect ML/FT, they are bound to submit a STR to the FIAU.

However, when providing one or more games within given jurisdictions licensees may be required to obtain a licence or authorisation from the competent authorities of that jurisdiction, even though they may already be in possession of a Maltese licence. Thus, situations may arise where a licensee will hold multiple licences to offer the same game/s.

Where in such a scenario, a licensee comes to report an instance of known or suspected ML/FT, the licensee should consider whether the said knowledge or suspicion is related to an activity carried out on the basis of its Maltese licence or to an activity carried out on the basis of its additional licence. It is only in the former case that the licensee is obliged to file a STR with the FIAU.

The above only reflects the position in terms of Maltese law and is not to be considered as guidance as to what licensees' obligations may be in jurisdictions other than Malta. Licensees are strongly encouraged to seek out what AML/CFT obligations they may have in those jurisdictions where they are present.

5.5 Prohibition of Disclosure

The need not to prejudice an analysis or investigation into ML/FT is also at the basis of the non-disclosure obligations arising from filing a STR or receiving a request for information with the FIAU. Other than in exceptional cases which are provided for in Regulation 16(2) of the PMLFTR, a subject

person cannot disclose any details or information in connection with a STR or a request for information made by the FIAU.

Safeguarding the integrity of an analysis or investigation is also why caution is advised when a subject person takes action to terminate a relationship or otherwise block additional transactions following the filing of a STR. Drastic action should only be taken once the FIAU has been advised of the subject person's intentions as any unjustified action may alert the customer that he is being suspected of foul play. In such circumstances it would be more advisable to increase on-going monitoring and submit additional STRs to the FIAU on any other suspected instances of ML/FT.

Licensees should therefore be extremely careful on how they handle information related to STRs or to requests for information received from the FIAU, as well as how to deal with a customer that is the subject of a STR or a FIAU enquiry. Licensees may therefore find themselves in a very uncomfortable position, especially in situations involving transactions that are still to be processed and which may therefore expose the licensee to complaints or even legal action. In this regard, it is important to bear in mind that:

i. Pending transactions that are the subject of a STR cannot be processed for a determinate period of time following the submission of the STR. In part this is through the operation of the law and in part through the exercise of the FIAU's power to postpone transactions. If the period of postponement applicable by law (one working day following the day on which the licensee files the STR) expires and in the meantime the FIAU has not objected thereto or no court order has been issued, the licensee can proceed with processing the transaction if it deems the same to be appropriate.

ii. Licensees should also remember that they are not in a position to disclose to the customer or to third parties that they filed a STR in his regard or that he is the subject of a request for information from the FIAU. And this independently of any other regulatory or contractual obligation that the licensee may be subject to. Licensees may however disclose as much to the MGA, where they are required to provide information by law.

iii. Any action that the licensee may want to take following the submission of a STR has to be properly considered to determine whether this may prejudice the analysis being conducted by the FIAU. Thus, licensees should be careful if they decide to block or close a customer's account, and should seek guidance from the FIAU's analysts prior to undertake any such action.

6. FUNDING OF TERRORISM

6.1 Funding of Terrorism

FT is the process of making funds or other assets available, directly or indirectly, to terrorist groups or individual terrorists to support them in their operations. This may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations.

Another difference is that while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds and avails himself of the profits of crime, the terrorist's ultimate aim is to obtain funds and resources to support terrorist operations.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and its or his legitimate funding sources. While ML is concerned with obscuring the source of the funds, FT is mostly concerned with obscuring the end recipient of the funds.

6.2 Funding of Terrorism and Gaming through Means of Distance Communications

In so far as gaming through means of distance communications are concerned, it has to be borne in mind that licensees also have CFT obligations once the Euro two thousand (€2,000) threshold is met. In cases where a suspicion of FT arises even before the said threshold is met, as in any such case CDD and reporting obligations become applicable irrespective of the amount deposited by the customer.

The risk of FT in gaming is most likely to manifest itself at withdrawal stage. However, there may be indicators that a business relationship or an occasional transaction may expose the licensee to funding of terrorism risks even at inception stage. Examples include situations where (a) there is negative publicity implicating the customer with terrorism or organisations linked to terrorism; or (b) the customer has links to one or more jurisdictions or areas where terrorists are active or which are known to sympathise and support terrorists and terrorist organisations. The use of anonymous means of payment to fund an account in any such situation would further accentuate the risk of FT, especially when remitting funds withdrawn by the customer.

In the above situations it becomes imperative to carry out EDD even when the customer requests to withdraw the funds. Whatever the payment method used, it has to be ascertained that the institution to which the funds are remitted is situated in a reputable jurisdiction and has equivalent AML/CFT requirements as are applicable to the licensee. If the withdrawal is being made through a channel or a form that favours anonymity, the licensee has to the extent possible ascertain itself that it has established that the funds will eventually end up in the customer's hands.

APPENDIX 1

This appendix is intended to assist licensees in performing their assessment as to the level of risk posed by games, funding methods, and channels used. In the spirit of the risk-based approach advocated by the PMLFTR, the rating provided below is indicative, and not mandatory. It is understood that each of the licensees' games, account funding methods, and technology systems may vary in nature, and in their own ML/FT risks. Thus deviations from the below are possible as long as the risk assessment is well reasoned and thorough.

Risk mitigation measures adopted by a licensee to address the risk identified in specific items are also to be included in the risk assessment. The adoption of risk mitigating measures do not in themselves lower the risk identified, which is inherent to particular game, funding method or channel used, but are the means through which a licensee proposes to neutralize or manage the risk inherent in the said risk factors.

Furthermore, it must be noted that the risk categorisation of a particular business activity or customer cannot be derived solely from one of the below indicators, but by the accumulation of all the relevant indicators. For example, although peer-to-peer games are classified as being high risk, it does not mean that all of the licensee's players playing peer-to-peer games are automatically classified as high risk. Rather, the licensee needs to look at the player's risk profile in its totality.

FUNDING METHODS

	Low	Low-Medium	Medium	Medium-High	High
Bank transfers (EEA or equivalent safeguards)	X				
Debit/credit cards issued by banks (EEA or equivalent safeguards)	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-licensed payment service providers			X		
Non-EEA licensed PSP				X	
EEA-licensed PSP that can be funded with cash or quasi-cash				X	
Prepaid cards/vouchers[6]					X
Cash					X

[6] *The use of prepaid cards is subject to widely differing restrictions in different jurisdictions. The main risks relating to prepaid cards are that they can be bought using cash, that there are no checks on the person purchasing the card, that the person purchasing the card and the person using it may not be the same person; mitigating measures include limiting the denominations of the cards, restricting supply to well-supervised entities such as banks, identification and verification of the purchaser/user, methods used to prevent the redemption of multiple cards by the same person, effective methods preventing the same person from purchasing or redeeming multiple cards and more.*

Examples of mitigating measures:

- Jurisdictions of operation, and the regulatory environment relating to payments;
- Methods used in processing payment of winnings to players (including procedures used when payments cannot be performed to the account of origin);
- Methods used in identifying origin of payments (ex: confirming that the account holder with the bank, card-issuer, or payments institution is the same as the gaming account holder);
- Strength of the operator's payments and anti-fraud team;
- Effectiveness of the operator's technological tools in place to monitor and detect suspicious activity.

GAME TYPES

	Low	Low-Medium	Medium	Medium-High	High
Fixed odds games without hedging (ex: slots, lotteries, bingo)	X				
Fixed odds games where hedging is possible (blackjack, baccarat, roulette)			X		
Sportsbetting			X		
P2P games (ex: poker, betting exchange)					X

Examples of mitigating measures:

- Strength of the operator's anti-fraud and anti-collusion department;
- Other safeguards against collusion (ex: impossibility of a player choosing his or her opponent);
- Effectiveness of the operator's technological tools in place to monitor, prevent and detect fraud or collusion (ex: automated alerts on suspicious gameplay, chatroom/forum monitoring, dynamic and responsive risk management processes);
- Level of monitoring for sports integrity.

CHANNEL

	Low	Low-Medium	Medium	Medium-High	High
Remote & automated registration on an electronic platform without 3rd party intervention	X				
Facilitation of registration by a land-based intermediary				X	
Use of master account set-up					X

Examples of mitigating measures:

- Effectiveness of onboarding procedures and associated safeguards;
- Effective control over land-based intermediary and access controls;
- Techniques used for monitoring of player activity;
- Regulatory environment and effective supervision carried out by local authorities.