

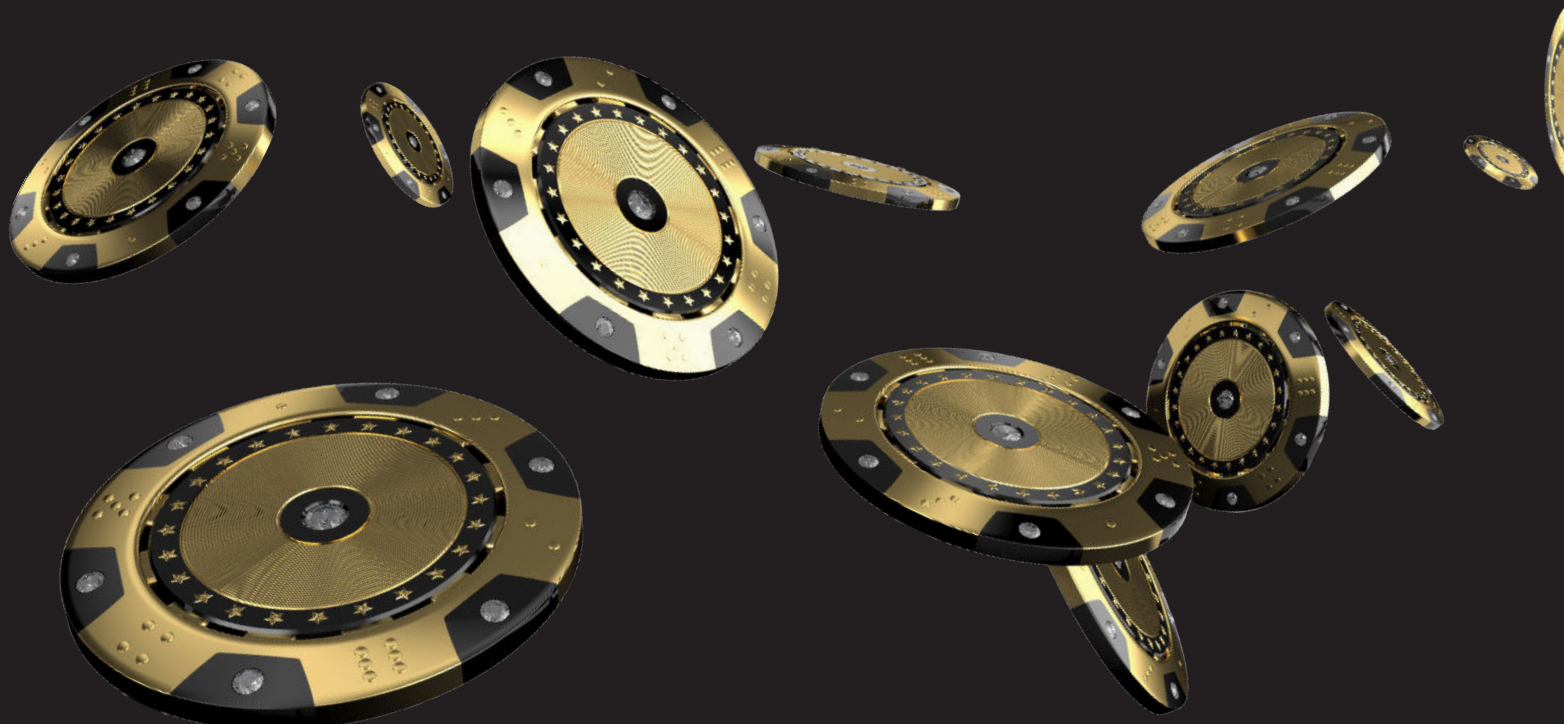
AML/CFT Knowledge, Awareness and Training in the Remote Gaming Sector

Thematic Review 2023



Contents

3	Glossary
4	Executive Summary
5	Scope of the Thematic Review
6	Methodology
8	Key Findings from the Thematic Review
8	Overall analysis
9	MLRO experience
11	Knowledge/awareness of AML/CFT legislation/guidance
14	The Risk-Based Approach
18	Customer Due Diligence
22	Application, Extent and Timing of Customer Due Diligence
25	Politically Exposed Persons
28	Inability to complete CDD
30	Outsourcing
32	Reporting Obligations
35	Training
37	Record-keeping
38	Conclusion
39	Annex I – list of interviewee designations



Glossary

AML/CFT	Anti-Money Laundering and Counter Funding of Terrorism
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
CASPAR	Compliance and Supervision Platform for Assessing Risk
CDD	Customer Due Diligence
CRA	Customer Risk Assessment
EDD	Enhanced Due Diligence
FIAU	Financial Intelligence Analysis Unit
IPs Part I	Implementing Procedures Part I
IPs Part II	Implementing Procedures Part II for Remote Gaming Sector
MGA	Malta Gaming Authority
ML/FT	Money Laundering and Funding of Terrorism
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
PMLA	Prevention of Money Laundering Act
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
RBA	Risk-Based Approach
SoF	Source of Funds
SoW	Source of Wealth



1. Executive Summary

During the first quarter of 2023, the Financial Intelligence Analysis Unit (FIAU), in collaboration with the Malta Gaming Authority (MGA), conducted a thematic review on the remote gaming sector. The purpose was to assess the anti-money laundering and combating the funding of terrorism (AML/CFT) regulatory¹ and practical knowledge, awareness of the Company's Policy and Procedures of the Money Laundering and Reporting Officer (MLRO) and any employees involved in the AML/CFT compliance function (hereinafter referred to as "Relevant Employees")² of remote gaming operators licensed under the Gaming Act (Chapter 583 of the Laws of Malta).

In general, interviewees demonstrated sound knowledge regarding the purpose of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) and the Implementing Procedures Part I (IPs Part I), the high-level concepts of the risk-based approach (RBA), the customer identification and verification measures, ongoing monitoring, outsourcing obligations, the timing for submitting suspicious reports and AML/CFT related training obligations.

However, there is room for improvement in relation to the knowledge on the administrative measures applicable under the PMLFTR and the purpose and content of the Implementing Procedures Part II for the Remote Gaming Sector (IPs Part II). Even though interviewees were able to detail the high-level concepts of the RBA, there are gaps in the awareness of the inherent and residual risks their respective remote gaming operators are exposed to.

Other areas requiring improvement include:

- The sources to be used to assess the reputability of a jurisdiction.
- The timing of Customer Risk Assessments (CRAs).
- The expected level of activity that needs to be collected to build a customer's risk profile.
- The Customer Due Diligence (CDD) requirements applicable to the different risk level assigned to customers.
- Situations which require the application of mandatory Enhanced Due Diligence (EDD).
- Politically Exposed Person (PEP) screening obligations.
- The obligations related to the period of retention of records.

For further details on the findings of the thematic review, MLROs and Relevant Employees are encouraged to refer to the applicable chapters of this paper.

¹ That is, of the AML/CFT obligations under the Prevention of Money Laundering Act (PMLA), the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR), the FIAU's Implementing Procedures Part I (the "IPs Part I") and the FIAU's Implementing Procedures Part II for the Remote Gaming Sector (the "IPs Part II"), as further detailed in this guidance paper.

² Vide Annex I for a complete list of interviewees' designations.



2. Scope of the Thematic Review

MLROs and Relevant Employees involved in the AML/CFT compliance function play a crucial role in protecting remote gaming operators from being misused to launder the proceeds of criminal activity. Since they are a pivotal element in the AML/CFT control framework implemented by remote gaming operators, it is imperative that they understand the money laundering and terrorism financing (ML/FT) risks they may encounter. Furthermore, knowledge of the measures, policies, controls, and procedures in place to mitigate these risks is essential. In view of this, a thematic review was carried out to evaluate the understanding by MLROs and Relevant Employees of AML/CFT regulatory principles, and their practical implementation across several topics, including *inter alia*, the RBA, Customer Due Diligence (CDD) measures, reporting obligations and training.



3. Methodology

AML/CFT regulatory obligations are applicable to anyone who is licensed by the MGA to provide a service as detailed further below. These services encompass 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 worth³. These services include the following game types:

Type 1

Games of chance played against the house, the outcome of which is determined by a random generator, and includes casino-type games, including roulette, blackjack, baccarat, poker played against the house, lotteries, secondary lotteries and virtual sports games.

Type 2

Games of chance played against the house, the outcome of which is not generated randomly, but is determined by the result of an event or competition extraneous to a game of chance, and whereby the operator manages his or her own risk by managing the odds offered to the player.

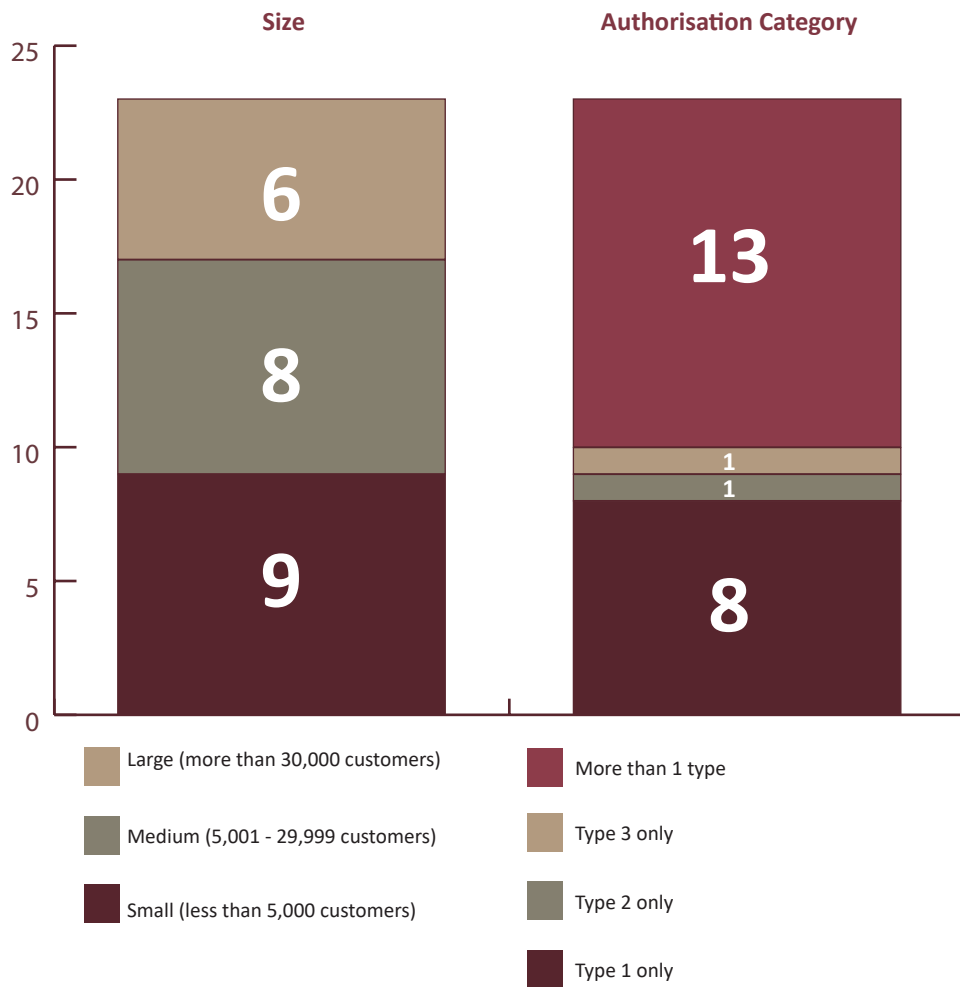
Type 3

Games of chance not played against the house and wherein the operator is not exposed to gaming risk, but generates revenue by taking a commission or other charge based on the stakes or the prize, and includes player versus player games such as poker, bingo, betting exchange, and other commission-based games.

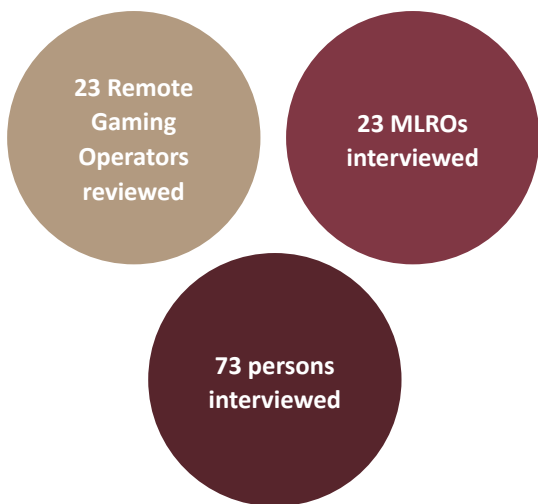
The thematic review consisted of 23 compliance examinations on remote gaming operators. As illustrated in the sample selection chart below, the FIAU aimed to select a representative sample of remote gaming operators across various sizes and authorisation types.

³ "Money and, or money's worth" includes, without limitation, currency accepted as legal tender in the jurisdiction or jurisdictions of its issue, virtual currencies, units of value, tokens of value, goods, services and any form of property which may be traded, sold, converted into, or otherwise exchanged for money, goods or services.

Chart 1
Remote Gaming Operators Sample Selection



During the thematic review, the FIAU and MGA Officials reviewed the AML/CFT policies and procedures of the examined remote gaming operators and interviewed 73 persons.⁴ The questions asked were aimed at assessing the interviewees' AML/CFT regulatory and practical understanding.



Regulatory Understanding

Interviewees' regulatory understanding was assessed through questions relating to local AML/CFT legislation and guidance.

Practical Understanding

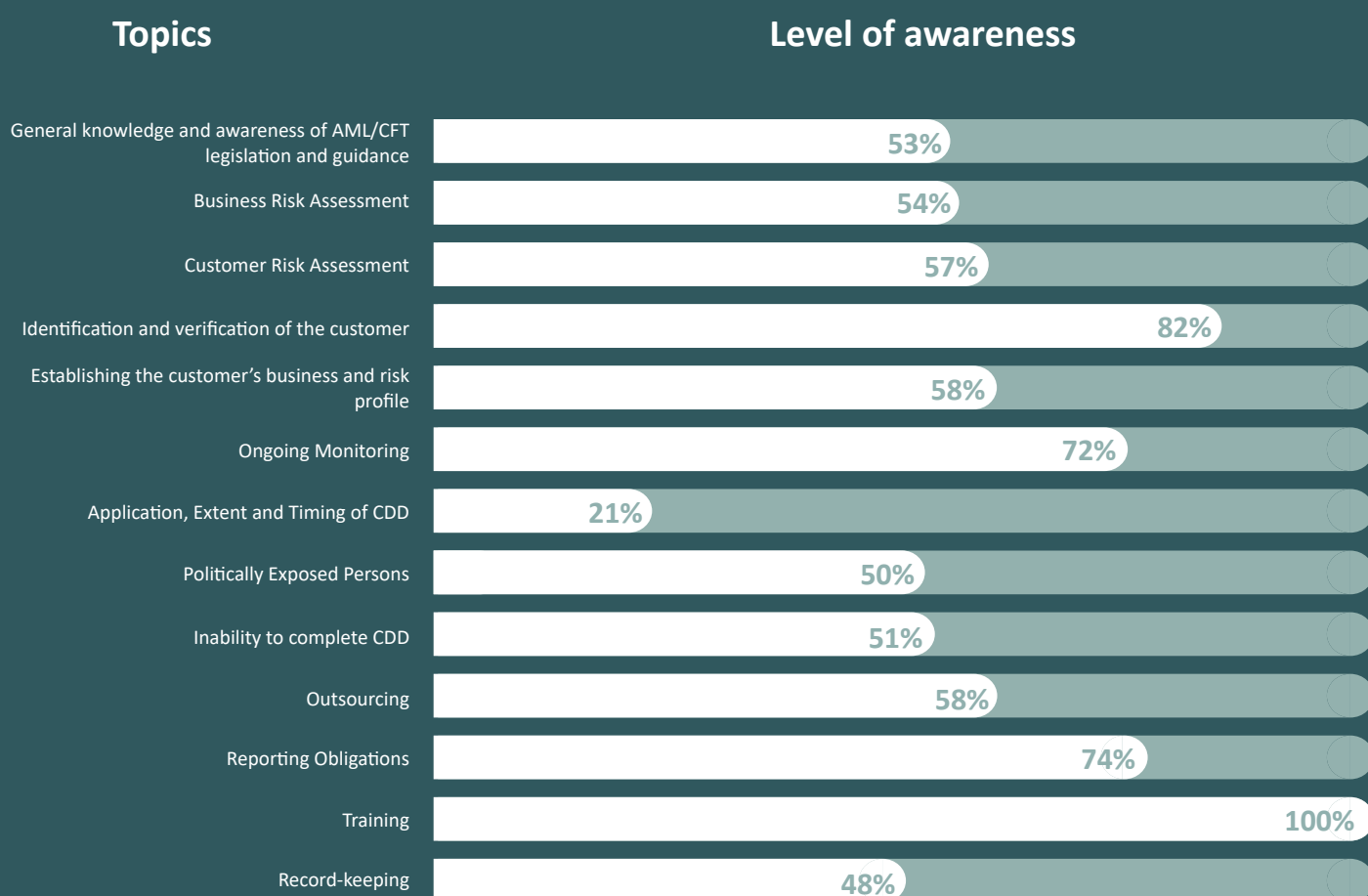
Questions posed to interviewees were aimed at assessing their practical understanding, that is, how AML/CFT obligations were implemented in practice by the respective remote gaming operator.

⁴ Vide Appendix I for a complete list of interviewees' designations.

4. Key Findings from the Thematic Review

Overall analysis

The replies provided by MLROs and Relevant Employees to the questions posed were aggregated and analysed for the purpose of measuring the overall level of awareness across the various AML/CFT topics. The results of this analysis are shown below.



4.1A | MLRO experience

Useful guidance

Regulation 15(1)(a) of the PMLFTR requires remote gaming operators to appoint an officer of sufficient seniority and command as the MLRO. The MLRO is responsible for receiving reports from the remote gaming operator's employees, or through software solutions used to analyse transactions on information or matters that may give rise to knowledge or suspicion of ML/FT. Furthermore, the MLRO is tasked with evaluating these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected to ML/FT. If such knowledge or suspicion of ML/FT is identified, the MLRO must report it to the FIAU and respond to any request for information promptly.

The role of the MLRO is further explained in Chapter 5 of the IPs Part I, Chapter 5.1 of the IPs Part II, and in the Guidance Note on the Common Issues Related to the MLRO issued by the FIAU on 6th April 2022.

Findings



On average, MLROs interviewed had between **3 to 5 years** of AML/CFT related work experience.



61% of MLROs had other roles within the company.

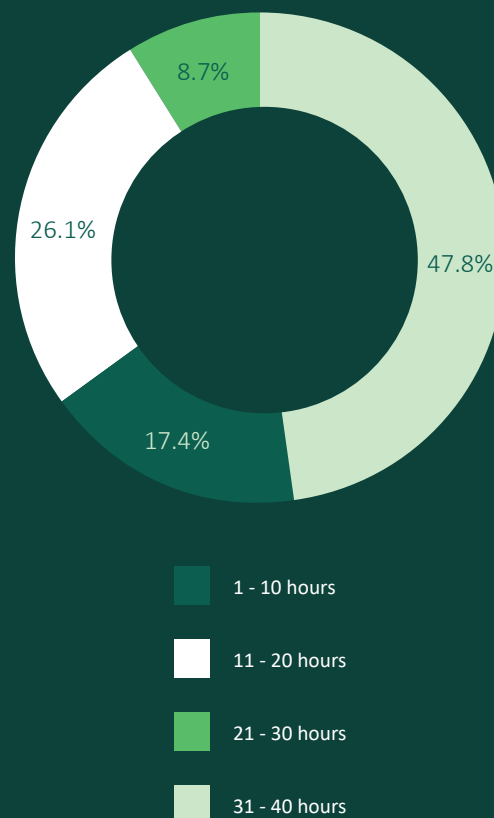


96% of MLROs were employed on a full-time basis within the company, whilst one was employed on a part-time basis (also acting as MLRO of another remote gaming operator on a part-time basis).

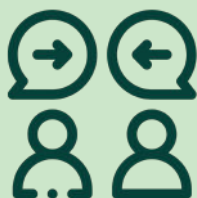


One large remote gaming operator did not appoint a designated employee.

Chart 2
Total number of hours per week dedicated to the role of MLRO



Key takeaways



**Conflicts
of
Interest**

While having a dedicated MLRO function is ideal, it is recognised that this may not always be possible and situations will arise where a person acting as MLRO will also have additional functions and/or duties within the company. In these circumstances, the remote gaming operator needs to assess whether the arrangement may impact the independence and impartiality required from the MLRO to effectively carry out the duties and responsibilities associated with the role. As outlined in Section 5.1.2 of the IPs Part I, this assessment must be documented.

In situations where the MLRO has a conflict of interest with any other functions carried out for the remote gaming operator, it is important that regular independent checks and reviews are carried out to ensure that the AML/CFT policies, controls, procedures, and measures are effectively being adhered to.



**Time
commitment**

Having the MLRO carrying out additional functions will also give rise to questions as to whether they are able to dedicate sufficient time to their role. It is, therefore, crucial that the MLRO is provided with sufficient human resources and technological means to mitigate the time they must dedicate to the other roles or functions to be carried out as remote gaming operator.

Likewise, when an employee is acting as the MLRO for two or more subject persons, it must be ensured that these multiple appointments allow the MLRO to fulfil their functions in an effective manner, by ensuring that there is sufficient time commitment and that situations giving rise to conflicts of interest are avoided. MLROs should bear in mind that the more appointments one holds and the more complex or voluminous the activities of the subject person concerned, the more difficult it is for the MLRO to meet their obligations at law in a satisfactory manner.



**Designated
Employee**

Based on the nature and size of activities (e.g., when there is a large volume of transactions or where there is a large volume of internal reports to be considered), remote gaming operators should consider whether there is a need to appoint one or more designated employees to assist and, whenever necessary, temporarily replace the MLRO when absent. The designated employee can in their own right determine that a suspicious report is to be filed when the MLRO is absent.

The appointment of the designated employee must receive the approval of the MLRO, and therefore following registration of the designated employee on CASPAR, the MLRO should approve them on the portal.

4.1B | Knowledge & awareness of AML/CFT legislation & guidance

Useful guidance

In line with Section 7.3 of the IPs Part I, MLROs and Relevant Employees are to be aware of the following legislative instruments and other binding guidance:

- a. the provisions of the Prevention of Money Laundering Act (PMLA)
- b. the provisions of the PMLFTR
- c. the provisions of the Criminal Code concerning the funding of terrorism
- d. relevant data protection laws, rules and guidance
- e. the FIAU IPs, other guidance and/or interpretative notes issued by the FIAU
- f. the applicable offences and penalties resulting from breaches of all the above.

The first part of the PMLA provides a definition of money laundering and criminalises the act of money laundering.⁵ The PMLA also lays out the procedure for the prosecution of money laundering and establishes the FIAU and its functions.

The PMLFTR set out the obligations and procedures that remote gaming operators are required to fulfil and to implement, and without which an AML/CFT regime cannot be effective.

Section 1.4 of the IPs Part I summarises the purpose of the PMLA and PMLFTR, whereas Section 1.2 of the IPs Part I details the relevant terrorism financing provision of the Criminal Code.

Sections 2.2 and 2.3 of the IPs Part I detail the purpose, status and application of the IPs respectively. The IPs Part I and the IPs Part II are issued in terms of Regulation 17 of the PMLFTR, which empowers the FIAU to issue these procedures and guidance to bring into effect the provisions of the PMLFTR. In accordance with this regulation, the IPs Part I and the IPs Part II (as applicable) are legally binding on all remote gaming operators (excluding B2B and Type 4 remote gaming operators). The tables below outline some of the administrative sanctions and criminal offences for breaches of AML/CFT obligations.

Table 1
Administrative penalties under Regulation 21 of the PMLFTR applicable to remote gaming operators carrying out relevant activity.

	Minimum	Maximum
Penalty for each contravention	€1,000	€46,500
Minor contraventions	€250	€1,000
Serious, repeated, or systematic breaches	€1,000	€1,000,000 or not more than two times the amount of the benefit derived

⁵ Article 3(1) of the PMLA.

Table 2
Criminal offences under the PMLFTR

Regulation 7(10) of the PMLFTR	False declaration, false representation, or the production of false documentation by a customer or person purporting to act on the customer’s behalf	A fine not exceeding €50,000, or imprisonment for a period not exceeding two years, or both the fine and imprisonment.
Regulation 16(1) of the PMLFTR	Prohibited disclosures (tipping off)	A fine not exceeding €115,000, or imprisonment for a period not exceeding two years, or both the fine and imprisonment.

Findings

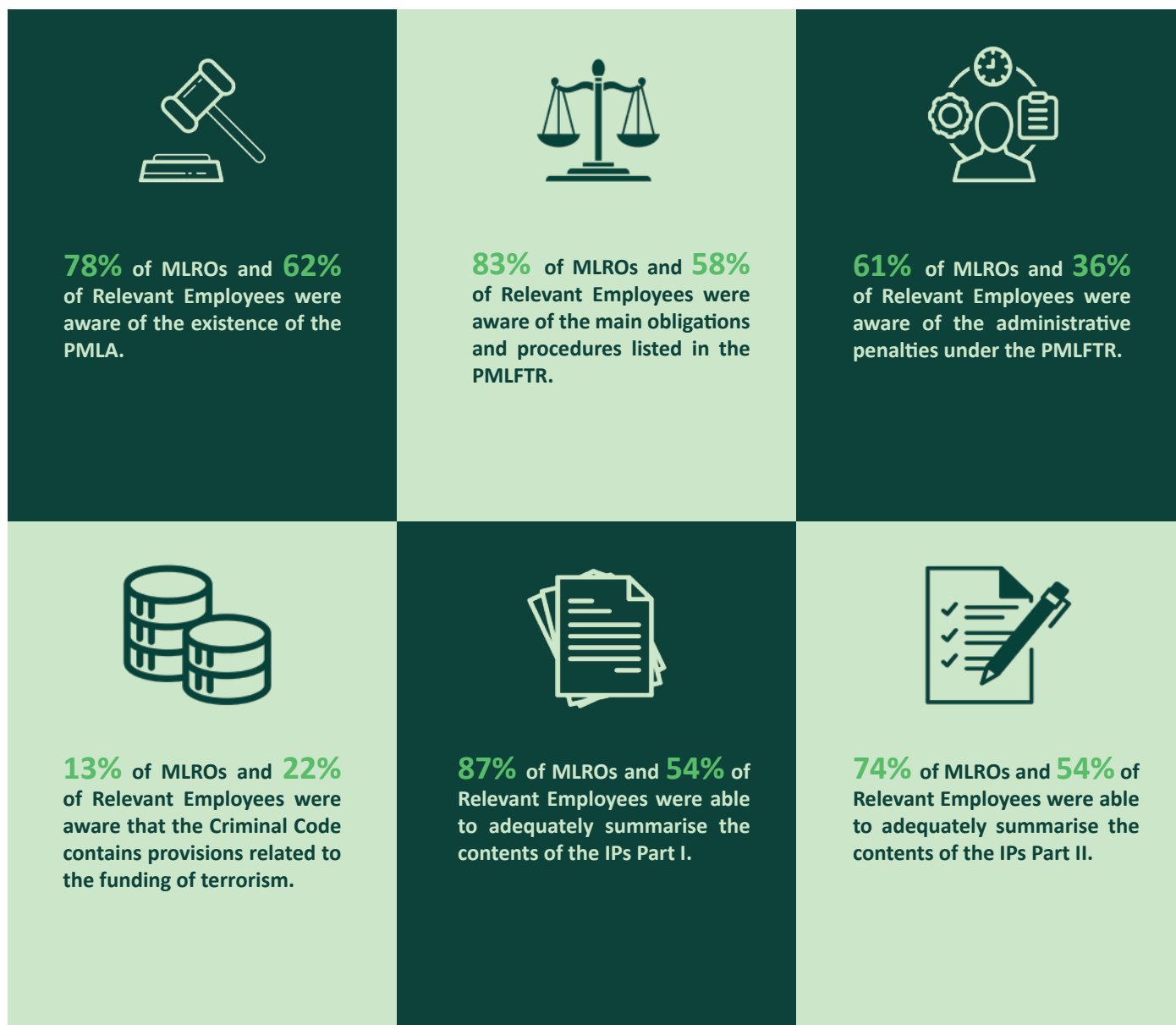
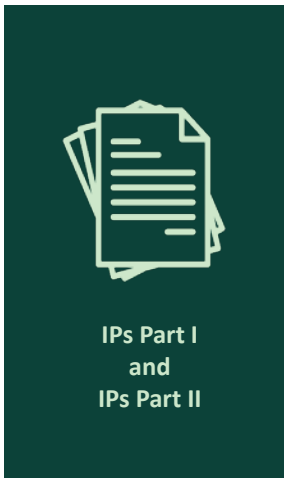


Chart 3
Awareness of Relevant Employees in identifying their AML/CFT key personnel



Key takeaway



The purpose of the IPs Part I is to assist remote gaming operators to understand and fulfil their obligations under the PMLFTR, thus ensuring effective implementation of the provisions of the PMLFTR. In addition, the purpose of the IPs Part II for the Remote Gaming Sector is to focus on certain aspects of the PMLFTR and their application, which warrants elaboration at an industry-specific level to highlight specific aspects of relevance and ensures that they are understood and interpreted consistently by remote gaming operators.

Whilst the FIAU recognises that Relevant Employees carrying out AML/CFT related duties may not be fully knowledgeable of all the provisions in the PMLA and PMLFTR, especially if not all the provisions fall within their area of responsibility, it expects them to be aware of the main content of the IPs Part I and the IPs Part II.

4.2 | The Risk-Based Approach

Useful guidance

To ensure that the AML/CFT measures, policies, controls and procedures adopted are effective, Regulation 5 of the PMLFTR requires remote gaming operators to implement these on a risk-sensitive basis through the adoption of a RBA.

As detailed in Chapter 3 of the IPs Part I and Chapter 2 of the IPs Part II, the RBA hinges on two aspects:

- i. An understanding of the risks one is facing.
- ii. The variation of controls, policies, measures, and procedures set in place, based on the risks identified, to achieve the strongest mitigating effect possible.

This calls not only for an understanding and assessment of risk that one's business is in general exposed to, i.e., business risk assessments (BRAs), but also for a more specific assessment of the risk to which a remote gaming operator will be exposing themselves to when establishing individual business relationships or carrying out occasional transactions, i.e., CRAs.

Once a CRA has been carried out, remote gaming operators must then apply the AML/CFT measures, policies, controls, and procedures adopted, in a manner that they address the specific ML/FT risks arising from the business relationship or occasional transaction. How these measures, policies, controls, and procedures are to be applied to specific risk scenarios has to result from the remote gaming operator's Customer Acceptance Policy (CAP). In this regard, remote gaming operators are to refer to Section 3.4.1 of the IPs Part I which sets out the requirements for the CAP.

MLROs and Relevant Employees are also encouraged to review and consult the following sections:

- i. Section 3.2 of the IPs Part I and Section 2.2.2 of the IPs Part II which delineates the risk factors which should be considered in the BRA and CRA.
- ii. Section 8.1 of the IPs Part I, which provides further detail on the jurisdiction risk factor and how to determine the reputability of a jurisdiction.
- iii. The FIAU's Guidance Paper on the Business Risk Assessment dated 9th April 2021.

Findings – Business Risk Assessment and Jurisdictional Risk Assessment



All MLROs and **88%** of Relevant Employees were aware of how often the BRA should be reviewed i.e., upon trigger events or on an annual basis in the absence of any trigger events.



87% of MLROs and **68%** of Relevant Employees were aware of the four main risk pillars (i.e., customer risk, geographical risk, interface risk and product/service/transaction risks) that should be considered in the BRA.



59% of MLROs and **42%** of Relevant Employees were aware of any additional risk pillars in the company's BRA.



91% of MLROs and **74%** of Relevant Employees were able to identify the most prevalent ML/FT risks as per the company's BRA.



65% of MLROs and **36%** of Relevant Employees were aware of the company's inherent risk rating as established through the BRA.



70% of MLROs and **36%** of Relevant Employees were aware of the company's residual risk rating as established through the BRA.



78% of MLROs and **50%** of Relevant Employees were able to provide an explanation of the Jurisdictional Risk Assessment.



17% of MLROs and **10%** of Relevant Employees were aware of the three sources which should be referred to when determining whether a jurisdiction is deemed to be reputable or otherwise as listed in Section 8.1.1 of the IPs Part I.



43% of MLROs and **30%** of Relevant Employees were able to differentiate between a non-reputable jurisdiction and a high-risk jurisdiction.

Findings – Customer Risk Assessment and Customer Acceptance Policy



74% of MLROs and **67%** of Relevant Employees were able to provide examples of risk factors that the remote gaming operator considers within the four main pillars of a CRA.



35% of MLROs and **22%** of Relevant Employees were aware that the customer's reputation, nature, and behaviour should be considered in the CRA.



39% of MLROs and **34%** of Relevant Employees were aware of the 30-day timeframe to carry out a CRA after meeting the €2,000 deposit threshold.



All MLROs and **98%** of Relevant Employees were aware of the customers who are not accepted as per the company's CAP.

Key takeaways




Awareness of Risk Assessment

MLROs and Relevant Employees exhibited a limited understanding of their remote gaming operator’s inherent risk rating as concluded and determined in the BRA. Furthermore, their lack of awareness extended to the remote gaming operator’s overall residual risk rating. It is crucial that they are knowledgeable about the content of the company’s BRA. The BRA should not be viewed solely as a mandatory exercise to fulfil obligations outlined in the PMLFTR and IPs. It should be regarded as a valuable tool that empowers MLROs and Relevant Employees to comprehend the company’s risk exposure, identify ways to mitigate risks to an acceptable level, and determine priority areas for AML/CFT efforts. To gain better understanding of the risk factors specific to the remote gaming sector, MLROs and Relevant Employees are encouraged to review Section 2.2.2 of the IPs Part II.



Non-reputable and high-risk jurisdictions

Remote gaming operators are required to assess whether the jurisdictions they engage with are considered non-reputable jurisdictions or high-risk jurisdictions. Regulation 2(1) of the PMLFTR and Section 8.1.1 of the IPs Part II detail the sources which should be referred to in determining whether a jurisdiction is reputable or not. Even if the interplay between the two concepts of non-reputable jurisdictions and high-risk jurisdictions is significant, MLROs are to note that it is only in the case of business relationships involving non-reputable jurisdictions that remote gaming operators are required to carry out mandatory EDD measures in terms of Regulation 11(10) of the PMLFTR. On the other hand, high-risk jurisdictions have an impact on a customer’s risk rating as per the CRA, potentially leading, although not necessarily, to a high-risk business relationship.



Customer’s reputation, nature, and behaviour

When evaluating the risks associated with a customer, it is essential to consider all known risk factors. Some risk factors, considered in the context of the BRA, need to be reconsidered based on the specific circumstances presented by the customer. This becomes particularly significant in the case of the CRA, where the customer’s reputation, nature, and behaviour must also be considered, as specified in Section 3.5.1(a) of the IPs Part I.



Timing of CRA

The CRA is to be carried out either prior to the carrying out of an occasional transaction or, in the case of a business relationship, no later than thirty (30) days from when the €2,000 deposit threshold is met. When the CRA is carried out at registration stage it is important for the remote gaming operator to ensure that the initial assessment is still valid. In this respect, it is important that MLROs and Relevant Employees are aware of this requirement so that the CRA is carried out within the stipulated timeframes, as this will guide the extent and type of CDD measures to be applied.

It is possible that the initial CRA may need to be reviewed at a later point in the business relationship, potentially leading to a corresponding adjustment in the CDD mitigating measures, due to a change in the CRA rating.

4.3 | Customer Due Diligence

Useful guidance

CDD measures, which are detailed in Chapter 4 of the IPs Part I and Chapter 3 of the IPs Part II consist of the following four main measures:

- i. Identification and verification of the customer – remote gaming operators should also refer to Section 3.2(i) of the IPs Part II for detailed requirements in this respect.
- ii. Identification and verification of the beneficial owner – remote gaming operators should also refer to Section 3.2(ii) of the IPs Part II for detailed requirements in this respect.⁶
- iii. Establishing the business and risk profile of the customer – remote gaming operators should also refer to Section 3.2(iii) of the IPs Part II for detailed requirements in this respect.
- iv. Ongoing monitoring of the business relationship – remote gaming operators should also refer to Section 3.2(iv) of the IPs Part II for detailed requirements in this respect.

Findings – Identification and verification of the customer



91% of MLROs and **92%** of Relevant Employees were aware that the customer's name, surname, permanent residential address, and date of birth details must be collected for all customers, irrespective of their risk rating.⁷



83% of MLROs and **44%** of Relevant Employees were aware that the IPs Part II allow the use of documentary and/or electronic sources to verify a customer's identity.



96% of MLROs and **98%** of Relevant Employees were aware of other documents which may be used to verify a customer's residential address when the main documentary source does not include the residential address.⁸

⁶ It is acknowledged that in most cases, remote gaming operators will not encounter situations involving beneficial owners. However, these situations cannot be excluded completely as remote gaming operators may be entertaining business relationships with one or more players funded by a syndicate. In these 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 remote gaming operators would therefore have to identify them and verify their identity. Given its limited applicability in the gaming sector, the obligation to identify and verify the beneficial owner was not tested during the thematic examinations.

⁷ Similarly, when opening an account, remote gaming operators are to identify but are not obliged to verify the identity of the customer.

⁸ As detailed in Section 3.2(i)(a) of the IPs Part II.

Findings – Establishing the customer’s business and risk profile



30% of MLROs and **26%** of Relevant Employees were aware that to build a customer’s risk profile, the expected level of activity needs to be collected.



83% of MLROs and **64%** of Relevant Employees were aware of the source of wealth (SoW) expectations for medium-risk players.



74% of MLROs and **56%** of Relevant Employees were aware of the SoW expectations for high-risk players.



78% of MLROs and **54%** of Relevant Employees were aware of the statistical data sources which may be used to obtain SoW information.



64% of MLROs and **74%** of Relevant Employees were aware that statistical data to obtain SoW information cannot be used in respect of high-risk players.

Findings – Ongoing monitoring



61% of MLROs and **40%** of Relevant Employees were aware of both components of ongoing monitoring, that is, ensuring that documents, data and information are kept up to date and transaction monitoring.



83% of MLROs and **64%** of Relevant Employees were aware of the SoW expectations for medium-risk players.



74% of MLROs and **56%** of Relevant Employees were aware of the SoW expectations for high-risk players.

Key takeaways



Customer's identity verification

Customer identity verification must be conducted using data, documents, or information obtained from independent and reliable sources. These include documentary sources and/or electronic sources such as E-IDs (or Bank-IDs) and electronic commercial databases. These sources should allow a remote gaming operator to conclude, to its satisfaction that the customer is who they declare themselves to be. To decide the personal information to be collected and the extent of its verification, one should also bear in mind the ML/FT risk to which the remote gaming operator is exposed, via the business relationship or occasional transaction. Section 4.3 of the IPs Part I and Section 3.2 of the IPs Part II specify the documentary and electronic sources that remote gaming operators should consider for identity verification purposes.



Establishing the SoW

Fulfilling the CDD measures to establish the customer's business and risk profile requires obtaining information and, where necessary documentation to establish the customer's SoW as well as the expected level of activity. The approach to build this profile is risk-based and therefore depends on the results of the CRA, particularly the risk factors which contributed to the assessment and resulting risk rating. When establishing the SoW, remote gaming operators are therefore expected to note the following:

1. That understanding the SoW consists of identifying the activities which generate the customer's net worth and whether this justifies the projected and actual level of account activity. Thus, it is not and should not be considered as a forensic accounting exercise.
2. Self-declarations and open-source checks can be used where the risk is not high, but remote gaming operators should supplement these with independent and reliable information and documentation if there are doubts as to the veracity of the information collected.
3. Where the risk is not high, remote gaming operators can also opt to use statistical data collected from the sources mentioned in points (a) or (b) of Section 3.2(iii) of the IPs Part II to develop behavioural models to gauge a customer's activity. When opting for point (a) of Section 3.2(iii) of the IPs Part II, it is imperative that open sources are using official economic indicators issued by national public bodies or reputable financial institutions. The use of statistical data in this case can be an alternative to the collection of SoW information.
4. In high-risk scenarios, operators must collect independent and reliable SoW information and documentation. It is crucial to acknowledge that statistical data is not suitable for high-risk situations, as the transactional patterns in these cases may differ significantly from average behavioural models. In these instances, gathering SoW information, as delineated in Section 3.2(iii) of the IPs Part II, becomes crucial.



As part of the CDD measures to be implemented, remote gaming operators are expected to have information about the customer's anticipated gaming account activity, specifying the expected value and frequency of transactions to be conducted throughout the course of the business relationship.



Ongoing Monitoring

It is crucial that remote gaming operators adhere to the specified requirements for effective ongoing monitoring of a business relationship due to the following reasons:

i) Maintaining up-to-date information

- **Fresh identification documents:** Obtaining updated identification documents when the existing one expires is essential. This process can be carried out on a risk-sensitive basis or linked to specific trigger events. Keeping the identification documents up-to-date is vital for accurate and reliable customer information.
- **Addressing inconsistencies:** Questioning and addressing any inconsistencies in the data or information already in possession is necessary. Timely identification and correction of inconsistencies contributes to the integrity of the information held.
- **Regular review of documents:** Even in the absence of document expiry or inconsistencies, conducting periodic reviews and updates of data and information on a risk-sensitive basis is important. This ensures that the customer profile remains relevant and reflective of any changes in risk factors.

ii) Transaction scrutiny: The scrutiny of transactions is vital to verify their alignment with the remote gaming operator's understanding of the customer, as well as the customer's business and risk profile. This helps in identifying and addressing any unusual or suspicious activities. Unlike SoW, Source of Funds (SoF) relates to how the funds used for a particular transaction were obtained by the customer. If a transaction falls within their profile and regular or expected activity is carried out through their account, there is no need for the MLRO to obtain specific information and documentation. If a transaction presents a departure from the known or expected behaviour of a customer, then the MLRO is required to question the same.

These two components of ongoing monitoring are further detailed in Section 4.5 of the IPs Part I and Section 3.2 of the IPs Part II. MLROs are reminded that adhering to these components is essential to meet regulatory standards and ensure the integrity of the business relationship monitoring process.

4.4 | Application, Extent and Timing of Customer Due Diligence

Useful guidance

Regulation 9(1) of the PMLFTR provides that CDD measures are to be applied by remote gaming operators when carrying out transactions amounting to €2,000 or more, whether carried out within the context of a business relationship or otherwise.

The obligations in respect of application, extent, and timing of CDD are further detailed in Chapter 4 of the IPs Part I and 3.3.2 of the IPs Part II.

As per the IPs Part II, the €2,000 deposit threshold is applicable when the customer opens an account with a remote gaming operator, leading to the establishment of a business relationship. Thus, CDD measures are not in principle applicable until this threshold is reached. However, to ensure the proper functioning of AML/CFT controls, remote gaming operators are required to apply a minimum level of CDD measures prior to the threshold being reached.

Likewise, when opening an account, remote gaming operators 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) of the IPs Part II are set as the minimum applicable in case of low-risk business relationships.

Once the €2,000 deposit threshold is met, remote gaming operators have to carry out a CRA in terms of Section 2.2.1 of the IPs Part II and meet their remaining CDD obligations, within 30 days from when the threshold is reached, the extent of these varies depending on the customer's risk rating. It should be noted that high-risk situations (as detailed in 3.3.2 of the IPs Part II) require the application of EDD measures.

The €2,000 deposit threshold can be calculated either:

- a. Daily by considering all deposits effected by a customer since the establishment of the business relationship;⁹ or
- b. Over a rolling period of one hundred and eighty (180) days.¹⁰

All accounts held by a customer with the remote gaming operator must be linked, irrespective of the platform used (as long as it falls under same licensee) or the brand under which the customer makes use of the remote gaming operator's services.

⁹ As detailed in Figure 1 of Section 3.3.2 of the IPs Part II.

¹⁰ As detailed in Figure 2 of Section 3.3.2 of the IPs Part II.

Findings



13% of MLROs and **20%** of Relevant Employees were aware of all the CDD measures required for low-risk customers when the €2,000 deposit threshold is met and the CRA and PEP screening have been carried out.



13% of MLROs and **10%** of Relevant Employees were aware of all the CDD measures required for medium-risk customers when the €2,000 deposit threshold is met and the CRA and PEP screening have been carried out.



4% of MLROs and **6%** of Relevant Employees were aware of all the EDD measures required for high-risk customers when the €2,000 deposit threshold is met and the CRA and PEP screening have been carried out.



4% of both MLROs and Relevant Employees were aware of all the situations which require mandatory EDD measures.



65% of MLROs and **68%** of Relevant Employees were aware of how the €2,000 determination is to be applied across all accounts held by a customer.

Key takeaways



CDD obligations

When a customer/player reaches a deposit threshold of €2,000, MLROs are reminded to fulfil the CDD obligations after assessing the customer's risk level as detailed in Sections 3.2 and 3.3.2 of the IPs Part II.



Enhanced Due Diligence

Section 4.9.2 of the IPs Part I details the situations where EDD is prescribed by law, and these are further detailed in Section 3.3.2 of the IPs Part II in relation to the remote gaming sector. MLROs are reminded that EDD measures are to be implemented when they engage with PEPs, conduct transactions that are complex and unusually large, when business relationships involve non-reputable jurisdictions or when the risk assessment carried out determines a business relationship as posing a high risk of ML/FT (for example when multiple payments methods are used). Another instance where EDD measures are warranted is when there are questions on the funding method being used by the customer or when multiple payment methods are being used by the same customer. Effective EDD measures do not require the application of extensive measures but the application of additional measures that mitigate the high risks identified.



Systems in place to continuously monitor the player's activity

Remote gaming operators are required to establish a system that enables them to continuously monitor player activity before reaching the €2,000 deposit threshold. This system should prevent players from avoiding the application of CDD measures by circumventing the €2,000 deposit threshold. This may be done by depositing funds on multiple accounts to avoid reaching the threshold in one system, regardless of the platform used or the brand under which the customer accesses the remote gaming operator's services, as long as they fall under the same remote gaming operator.

It is essential for the remote gaming operators to establish one customer profile so that all the CDD obligations are assessed under one profile.

4.5 | Politically Exposed Persons

Useful guidance

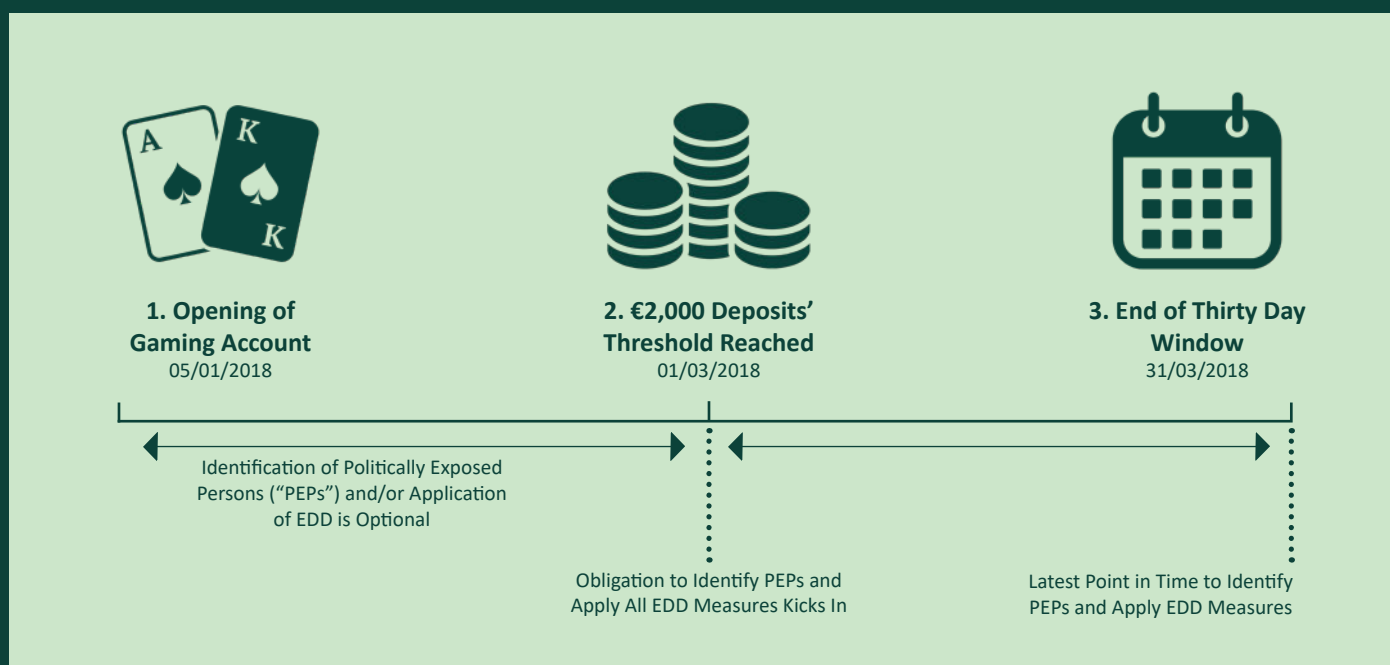
PEPs pose a high risk of ML/FT due to the position they occupy and the influence they exercise. PEPs may abuse their prominent public functions for private gain, such as by being involved in corrupt practices, accepting bribes, or abusing, or misappropriating public funds.

Regulation 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs Part I require remote gaming operators to have appropriate AML/CFT risk management procedures in place that enable them to determine whether a customer or a beneficial owner (current or prospective) is a PEP and, subsequently, to carry out EDD measures, both when establishing or continuing business relationships with or undertaking occasional transactions for a PEP.

Section 4.9.2.2 of the IPs Part I and Section 3.4 of the IPs Part II highlight the methods that remote gaming operators should consider in determining a customer's PEP status. These methods consist of:

- i. Relying on publicly available information, including internet and media searches; or
- ii. Obtaining the information directly from the customer or beneficial owner; or
- iii. Utilising commercial databases.

Figure 1
Politically Exposed Persons – Screening Timeline



Findings



65% of MLROs and **38%** of Relevant Employees were aware that collecting information directly from the customer or utilising reliable electronic databases, internet and media searches are considered acceptable methods for deciding whether a customer qualifies as a PEP.



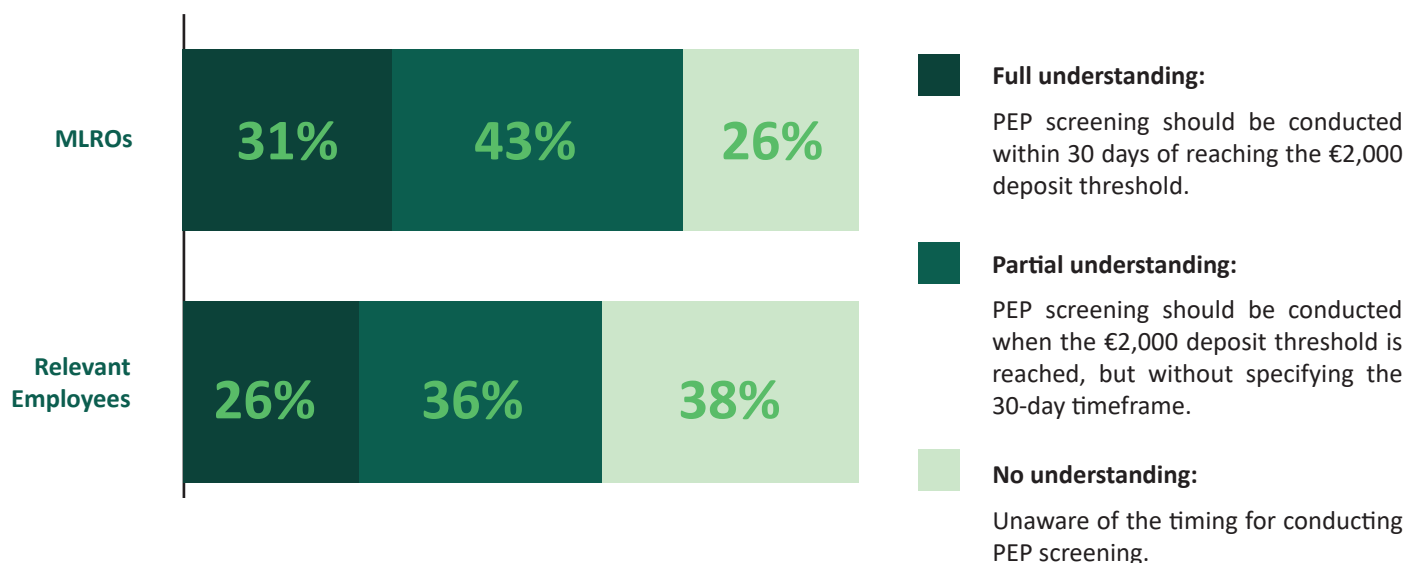
43% of MLROs and **24%** of Relevant Employees had knowledge regarding the necessary actions to be taken once a person has been identified as a PEP, i.e.,

- i. Obtaining senior management approval to service the PEP.
- ii. Establishing the SoW, and where applicable, the SoF.
- iii. Conducting enhanced ongoing monitoring of the customer’s activity.



96% of MLROs and **94%** of Relevant Employees were aware of whether their respective gaming operator accepted PEP customers or otherwise.

Chart 4
Politically Exposed Persons – Screening Obligation



Key takeaways



EDD on
PEPs

The rationale behind requiring EDD measures in respect of PEPs, is that they present a heightened risk of ML/FT due to the prominent positions they hold and the influence they exercise. Therefore, MLROs should ensure that remote gaming operators have robust risk management procedures in place to identify PEPs and conduct thorough due diligence to mitigate the potential risks associated with ML/FT that PEPs may pose. It is therefore important that MLROs and Relevant Employees are aware of the steps to be taken once a customer has been identified as a PEP.



Timing
of PEP
screening

Screening for PEP status must be carried out regularly but it is important that this is done within 30 days of the €2,000 deposit threshold being met. This is required even if the remote gaming operator has already screened customers to determine if they were PEPs at registration or earlier on in the course of the business relationship .

4.6 | Inability to complete CDD

Useful guidance

Customers may occasionally not be willing to provide remote gaming operators with the necessary CDD information or documentation, even though the remote gaming operator may have repeatedly requested these. In this case, remote gaming operators should follow the steps detailed in Section 3.6 of the IPs Part II.

Findings



78% of MLROs and **80%** of Relevant Employees were aware of the withdrawal limitations that should be placed on a customer's account from when the €2,000 deposit threshold is met until the completion of CDD measures.



52% of MLROs and **20%** of Relevant Employees were aware of the steps which should be taken when more than 30 days have passed since meeting the €2,000 deposit threshold and CDD measures remains incomplete.



13% of MLROs and **6%** of Relevant Employees were aware of what should be done with the balance on account when the account is suspended and blocked and there is no AML/CFT related reason to justify the retention of the funds.



96% of MLROs and **82%** of Relevant Employees were aware that one should consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

Key takeaway



Customer unwilling to provide the necessary information or documentation

In situations where a customer is unwilling to provide the necessary information or documentation, MLROs are required to terminate the business relationship. They may choose to either close the customer's account or to keep it blocked and suspended entirely.

MLROs should assess whether there are any reasons to suspect ML/FT and if so, they should report to the FIAU at the earliest possible moment as per the PMLFTR. It is important to note that a customer's reluctance to provide CDD documents does not automatically imply suspicion of ML/FT. MLROs should consider all available information, including the payment methods used, the games played, the customer's gaming habits, any existing data on the customer, and information accessible through sources like the internet.

When there are no grounds to suspect ML/FT, remote gaming operators should return the funds to the customer. This should be done in consideration of any legal restrictions on the fund remittance. The funds should be returned to the same source utilising the same channels used to receive them. If it proves difficult to remit the funds to the same source and through the same channels, remote gaming operators must request fresh instructions and assess whether these instructions give rise to suspicion, in which case, a suspicious report shall be filed and remittance shall be suspended pending the FIAU expressing its opposition, or otherwise, to the said transaction.

4.7 | Outsourcing

Useful guidance

Although remote gaming operators may outsource certain AML/CFT obligations as per Section 6 of the IPs Part I, it remains their responsibility to ensure that they always abide with the obligations set out in the PMLFTR. The FIAU ultimately holds the remote gaming operator as responsible for compliance with its AML/CFT obligations.

Remote gaming operators need to be aware of the conditions with regards to outsourcing as per Section 6.4 of the IPs Part I and Section 4.3 of the IPs Part II.

Findings



39% of remote gaming operators outsourced the implementation of their AML/CFT obligations.



6% of MLROs, Deputy MLROs and Designated Employees were aware of the obligations that cannot be outsourced in line with the IPs Part I.¹¹



94% of MLROs, Deputy MLROs and Designated Employees were aware that the outsourcing relationship should be monitored.



94% of MLROs, Deputy MLROs and Designated Employees were aware that the remote gaming operator is ultimately responsible for compliance with AML/CFT obligations.

¹¹ When interviewees were specifically asked regarding tasks that cannot be outsourced, 74% of MLROs, deputy MLROs and designated employees were aware that the MLRO function cannot be outsourced. 13% were aware that the acceptance or otherwise of a customer and the termination of a business relationship cannot be outsourced, but only 6% were aware of both.

Key takeaway



When a decision is taken to outsource AML/CFT obligations, it is imperative to be mindful of the fact that remote gaming operators will always remain responsible for compliance with AML/CFT obligations. MLROs must be aware that they are always responsible for fulfilling all obligations outlined in the PMLFTR and the IPs Part I and Part II. Some AML/CFT aspects cannot be outsourced, including decisions regarding customer acceptance or termination of business relationships.

It is important for MLROs to understand that outsourcing does not extend to the appointment of the MLRO and the individual in charge of monitoring functions. Therefore, these two roles cannot be delegated to third parties, as they must be consistently carried out by an officer or an employee of the remote gaming operator.

Outsourcing does not encompass the decision of whether to file a suspicious report with the FIAU. This remains at the discretion of the MLRO. The remote gaming operator must ensure, through its internal reporting procedures, that even if specific functions are outsourced to a third party, internal reports should be submitted to the MLRO for them to decide whether a suspicious report should be filed with the FIAU.

4.8 | Reporting Obligations

Useful guidance

It is the responsibility of the MLRO to consider any internal reports of unusual or suspicious transactions and, where necessary, follow them up by filing a suspicious report with the FIAU. Section 5.5 of the IPs Part I explains that if after considering the internal report and all the necessary documentation, the MLRO or the designated employee determines that there is knowledge, suspicion or reasonable grounds to suspect that a transaction may be related to ML/FT, or a person may have been, is or may be connected with ML/FT, or ML/FT has been, is being or may be committed, the MLRO must promptly file a suspicious report with the FIAU. This means that a suspicious report is submitted the day when knowledge or suspicion of ML/FT is considered to subsist by the MLRO.

When preparing the submission of a suspicious report, MLROs and designated employees, are to refer to Chapter 5 of the IPs Part I, Section 5 of the IPs Part II and the FIAU's guidance note on submitting transaction reports by Remote Gaming Operators. The guidance note provides sector-specific guidance on the information that gaming operators are to include in the suspicious report.

Findings¹²



24% were aware of the three (non-cumulative) factors which would lead to the filing of an internal report.












All interviewees were aware that an internal report should be made to the MLRO without delay and not later than the next working day.



98% were able to provide examples of red flags which may lead to the filing of an internal report.

¹² The questions associated with the findings relate to other Relevant Employees (i.e., all interviewees excluding MLROs, Deputy MLROs and Designated Employees)

Findings¹³

 <p>52% were aware of the main duties associated with the role of the MLRO.</p>	 <p>57% were aware of the three (non-cumulative) factors which would lead to the filing of a suspicious report.</p>	 <p>96% were aware that a suspicious report should be filed promptly.</p>
 <p>All interviewees were aware that if, due to the nature of the transaction, the latter cannot be delayed, and is therefore still executed despite suspicion of ML/FT, the company is required to submit a suspicious report immediately after.</p>	 <p>64% were aware that when there is suspicion that a transaction may be linked to ML/FT and a suspicious report has been submitted, the unprocessed transaction can be delayed by the FIAU by one working day¹⁴ from when the suspicious report was submitted, to allow the FIAU time to review it and inform the company how to proceed.</p>	 <p>83% were aware that the FIAU is the only Maltese Authority to which a suspicious report should be submitted.</p>
 <p>75% were aware that the filing of a suspicious report is not strictly limited to suspicious transactions, but also extends to other suspicious activity.</p>	 <p>56% were aware that guidance from the FIAU should be sought following the submission of a suspicious report prior to blocking or closing the customer's account.</p>	 <p>81% were aware of the records that should be kept if, when following an internal report, a suspicious report is not filed.</p>

¹³ Given the nature of the questions, those associated with the findings were only posed to MLROs, Deputy MLROs and Designated Employees.

¹⁴ The timeframes are explained in further detail in Article 28 of the PMLA and Section 5.8 of the IPs Part I.

Key takeaways



Internal Report

It is important for Relevant Employees to be aware that an internal report should be filed when they become aware of any information or matter that in their opinion gives rise to knowledge or suspicion that a person or a transaction is connected to ML/FT. Relevant Employees are encouraged to refer to Section 5.4 of the IPs Part I for further details.



Submission of suspicious report

Suspicious reports should be filed, when after assessing an internal report and all necessary documentation, knowledge, suspicion, or reasonable grounds to suspect that a person or transaction relates to ML/FT, arises. The filing of a suspicious report is not limited to transactions suspected of money laundering. It extends to any suspicion that the remote gaming operator becomes aware of in the exercise of their 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. Furthermore, a suspicious report must be filed not only in suspected instances of money laundering but also in situations where there is a suspicion of funding of terrorism or that funds are the proceeds of criminal activity.

Reporting must also take place when MLROs 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, based on objective facts, the remote gaming operator ought to have suspected that ML/FT is present.

In line with Section 5.5(iii) of the IPs Part II, MLROs are reminded that guidance from FIAU analysts should be sought following the submission of a suspicious report prior to blocking or closing the customer's account.

4.9 | Training

Useful guidance

In line with Regulation 5(5)(b) and 5(5)(e) of the PMLFTR, Section 7.1 of the IPs Part I stipulates that remote gaming operators are required to take appropriate and proportionate measures from time to time to:

- Ensure that employees are aware of relevant AML/CFT legislation and data protection requirements, as well as of their AML/CFT measures, policies, controls, and procedures.
- Provide training in relation to the recognition and handling of operations and transactions that may be related to proceeds of criminal activity and/or ML/FT.

Section 7.2 of the IPs Part I stresses that awareness-raising initiatives and training should be provided to employees and other company officials whose duties include the handling of either relevant financial business or relevant activity, irrespective of their level of seniority. Thus, this includes directors, senior management, the MLRO and designated employee(s), compliance staff, and all members of staff involved in the activities of the subject person that fall within the definition of 'relevant financial business' and 'relevant activity'.

Findings



ALL MLROs stated that the remote gaming operator provides AML/CFT related induction training to new joiners.¹⁵



ALL MLROs stated that employees were provided with a relevant list of red flags and risk indicators.

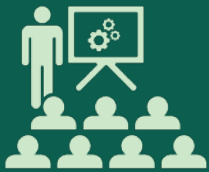


All interviewees stated that they received AML/CFT training since joining the remote gaming operator.¹⁶

¹⁵ 91% of MLROs stated that induction training was provided between 1-3 months after joining the remote gaming operator, whilst 9% stated that it was provided after four months of joining the remote gaming operator.

¹⁶ Induction training was provided at different stages of employment and thus some interviewees may not have yet received the training due to the date of their employment.

Key takeaway



AML/CFT
Training

The thematic review provides evidence that the quality of AML/CFT training may not be sufficient, as indicated by Relevant Employees' lack of awareness on specific AML/CFT obligations. Although many Relevant Employees participate in external training programs, these are not always specialised in Maltese legislation and regulations. Moreover, while acquiring international qualifications is undeniably valuable, there appears to be a need for enhanced training regarding the Maltese regulatory framework and its practical implementation. In essence, there is room for improvement in ensuring that AML/CFT training not only meets international standards, but also adequately addresses the specific requirements of Maltese laws and regulations, while addressing the remote gaming operator's specific AML/CFT procedures, red flags, and the risks to which they are exposed to.

In all cases, new Relevant Employees should be made aware of their responsibilities and those of the remote gaming operator upon being employed or engaged in their relevant position. It is therefore important that they are provided with relevant AML/CFT training as soon as practically possible when joining the company.

4.10 | Record-keeping

Useful guidance

As per Regulation 5(5)(a)(i) of the PMLFTR, remote gaming operators should have record-keeping procedures. Section 9.2 of the IPs Part I details the records which should be kept by remote gaming operators. In this respect, remote gaming operators must maintain the records referred to in Section 9.2 of the IPs Part I, for a period of five years from the date of the termination of the business relationship. However, remote gaming operators are to note that the FIAU, relevant supervisory authorities or law enforcement agencies are entitled to demand that records, including personal data, be retained for longer periods (up to a maximum of 10 years from the date of the termination of the business relationship). This extension may be necessary for the prevention, detection, analysis, and investigation of ML/FT activities by the FIAU, relevant supervisory authorities or law enforcement agencies.

Reference may be made to Chapter 9 of the IPs Part I for information on record-keeping including the timelines applicable to records not listed under Section 9.2 of the IPs Part I, such as records of internal reports, training records etc.

Finding



57% of MLROs and **38%** of Relevant Employees were aware that the official record-keeping period is five years from the termination of the business relationship.

Key takeaway



Record-keeping

AML/CFT related records are not only intended to show that a remote gaming operator complied with its obligations at law but are also essential for them to effectively apply specific aspects of its AML/CFT obligations, like carrying out or revising its BRA and carrying out effective ongoing monitoring. Records maintained by remote gaming operators are also intended to assist the FIAU, relevant supervisory authorities and law enforcement agencies in the prevention, detection, analysis, or investigation of possible ML/FT. Therefore, it is important that MLROs and Relevant Employees are aware of their purpose and the official period of retention to ensure that these records are readily available upon request.

5. Conclusion

Criminals attempt to launder illegally obtained funds through an array of methods designed to conceal the original SoF. Various sectors are prone to misuse for money laundering purposes and the gambling industry is no exception from being used as a money laundering vehicle. It is therefore critical that remote gaming operators design and implement effective AML/CFT control programs to mitigate this risk. The effectiveness of these programs is significantly dependent on the knowledge of the MLRO and AML/CFT compliance officers in relation to how controls are to be applied both for the purpose of mitigating the ML/TF risks, as well as to be compliant with AML/CFT obligations.

During the thematic review, it was observed that the level of knowledge, awareness, and training of MLROs and Relevant Employees in relation to the AML/CFT regulatory framework varied. Some demonstrated a good level of knowledge, awareness, and training, whereas for others it was evident that the level needs to be significantly improved. It is important for remote gaming operators to ensure that MLROs and Relevant Employees are properly trained to enable them to stay updated on developments in AML/CFT obligations, ML/TF risks, and the remote gaming operators' operations, activities, and controls.

The FIAU and the MGA encourage all MLROs and Relevant Employees to read this document and familiarise themselves with the findings and key takeaways. It is also recommended for MLROs and Relevant Employees to take steps to incorporate any necessary enhancements into the remote gaming operators' AML/CFT controls, policies, and procedures to prevent the shortcomings identified in this paper.



Annex I – List of interviewees’ designations

Interviewees’ Designation	Number of interviewees
MLRO	23
Deputy MLRO	4
Deputy MLRO, AML and Compliance Officer	1
Deputy MLRO and Chief Operating Officer	1
Deputy MLRO and Head of AML	1
Designated Employee	2
Designated Employee and AML Coordinator	1
Designated Employee and AML Manager	1
Designated Employee and Operations, Risk and Payments Team Leader	1
Director of KYC and Risk	1
Director of Legal and Compliance	1
Head of Compliance	1
Head of Fraud and AML Operations	1
Head of KYC and AML	1
Head of Risk, Fraud and Payments	1
AML Manager	1
Compliance Manager	3
Fraud and AML Project Manager	1
Fraud Manager	1
KYC and Risk Manager	1
Payment and Risk Manager	1
Payment, Risk and Fraud Manager	2
AML Risk Supervisor	1
AML Team Leader	3
Compliance Operations Team Lead	1
Risk and Fraud Team Leader	1
Risk and AML Shift Leader	1
Senior AML Analyst	1
Responsible Gaming and Payment Analyst	1
AML Analyst	3
Fraud and Payment Analyst	1
Payment Security Analyst	1
Responsible Gaming and Payment Analyst	1
Customer Service Agent	2
KYC and AML Agent	1
Payment and Risk Agent	1
AML and Risk Operations	1
AML Officer	1

© Financial Intelligence Analysis Unit, 2024

Reproduction is permitted provided the source is acknowledged.

Questions on this document may be sent to queries@fiaumalta.org

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq I-Mdina,
Central Business District
Birkirkara, CBD 2010

Telephone: (+356) 21 231 333

Fax: (+356) 21 231 090

E-mail: info@fiaumalta.org

Website: www.fiaumalta.org