FIAU

# Enforcement Factsheet:

## Common observations across sectors subject to AML/CFT Supervision

Issued: 04 May 2021

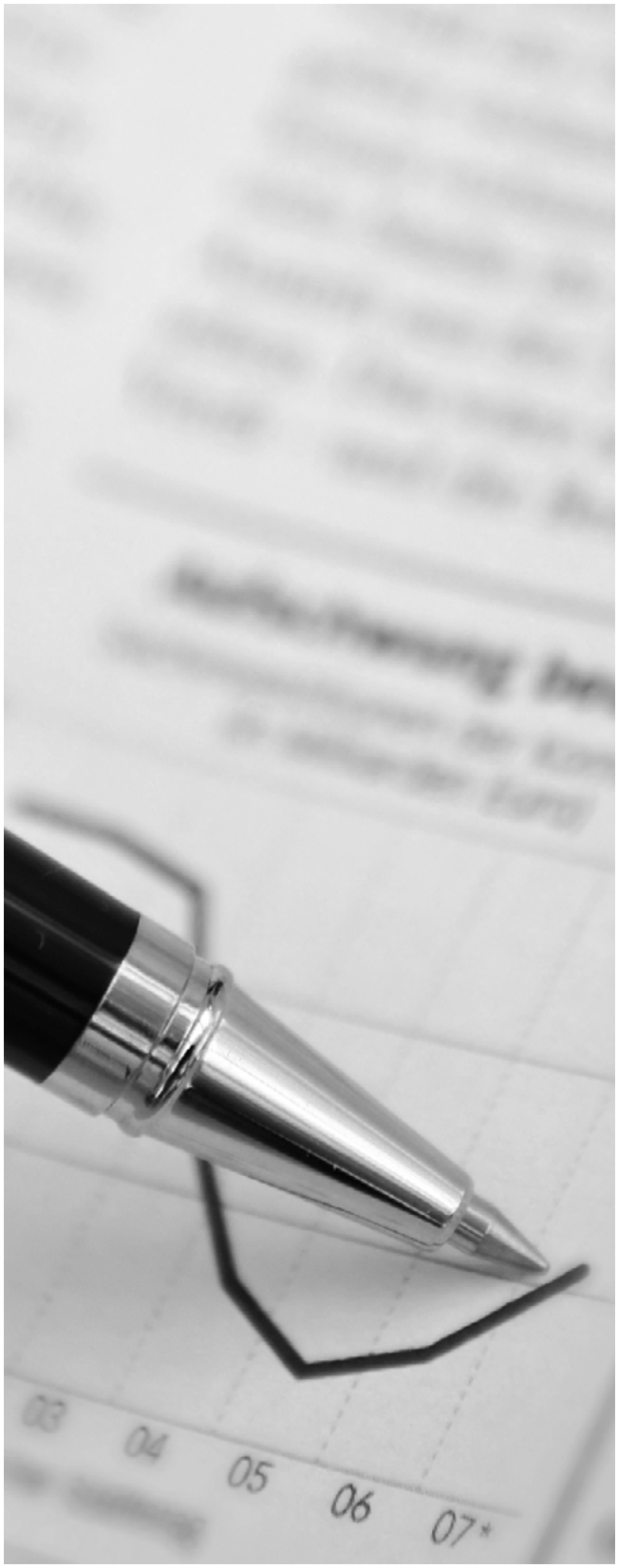
# CONTENTS

# INTRODUCTION

Over the past two years and following the overhaul of its anti money laundering/combatting the funding of terrorism (AML/CFT) Supervisory Strategy, the Financial Intelligence Analysis Unit (FIAU) has stepped up its supervisory and enforcement actions to ensure more effective compliance by subject persons (SPs) with AML/CFT obligations. As a result of this overhaul, the FIAU significantly increased its supervisory coverage[1], and has been taking more meaningful enforcement action including heftier pecuniary sanctions and the imposition of numerous remediation directives. These initiatives coupled with more regular and qualitative guidance, as well as increased investment by subject persons in AML/CFT resources, have notably improved the level of compliance with AML/CFT obligations in Malta.

In a bid to provide more insights on AML/CFT compliance trends, the Enforcement Section of the FIAU has analysed the enforcement actions undertaken by the FIAU in 2019 and 2020 and is publishing this factsheet which presents the conclusions of this analysis. Readers will find a graphical representation of the most common findings included in Annex 1 to 3 of this factsheet.

This factsheet together with the FIAU's paper on the Business Risk Assessment provides SPs operating in the various regulated sectors with insights into the most common observations which emanated from the AML/CFT supervisory visits. These documents are intended to assist SPs to further align their internal AML/CFT controls with the legal obligations and the FIAU's expectations. This is also necessary in order to ensure that the said controls are adequate and robust to protect their services, and ultimately, the Maltese economy from being abused for money laundering/funding of terrorism (ML/FT) purposes.




[1] 167 examinations were carried out under the annual supervisory cycle (July 2019 – June 2020) and 142 examinations have been carried out so far throughout the annual supervisory cycle (July 2020 – June 2021). This denotes a stark increase over the 67 examinations carried out in 2017 and 58 examinations in 2018.

# EXECUTIVE SUMMARY

The most common finding noted across all sectors relates to the appreciation of risk, both at the institutional level and at the customer level. This can be especially seen from the observations on the customer risk assessment included in this factsheet. While understanding risks is essential, the transposition of such understanding into effective methodologies to determine the risk exposure both at the business and customer level is crucial.

Other common findings relate to the requirements to have in place comprehensive customer risk profiles, transaction monitoring procedures and the need to consider occasional transactions within the context of all that is known about the customer, including past activity. The kind and extent of findings at times differ from one sector to another.

Robust AML/CFT controls are a must to protect the reputation of the SP and of the local jurisdiction. Effective measures to monitor customer relationships and transactions that take place through such established relationships are indispensable. Should it happen that these controls are absent, the possibility that the local economy will be abused for ML/FT purposes will increase with all that may entail in terms of financial and economic repercussions for all concerned.

# COMMON FINDINGS AND EFFECTIVE MEASURES FOR PREVENTION

## 1. THE BUSINESS RISK ASSESSMENT

Understanding the ML/FT risks that SPs are exposed to, is the cornerstone for the proper application of AML/CFT obligations. The carrying out of a Business Risk Assessment (BRA) is thus indispensable for SPs to identify and understand the ML/FT risks that they are exposed to and how such risks could possibly impact their business should they materialise. This assessment ultimately aids the SP to devise effective controls to mitigate the identified ML/FT risks.

The obligation to carry out a BRA emanates from Regulation 5(1) of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR) and is explained in further detail under Section 3.3 of the Implementing Procedures Part I. The BRA must, as a minimum take into account ML/FT risks posed by customer types, geographical connections, the type of products or services that are offered and transactions carried out, as well as the delivery channel or interface (i.e. method) through which services or products are offered. Published National and Supranational ML/FT risk assessments that provide information on ML/FT risks to which Malta or the EU is particularly exposed to must also be taken into consideration and included in the assessment.

Further information with regards to the obligation to carry out a BRA and the observations noted during supervisory examinations may be found in a separate paper issued by the FIAU on 9 April 2021 entitled: The Business Risk Assessment.

## 2. THE CUSTOMER RISK ASSESSMENT

The obligation to carry out and document a CRA has been in place since 2011. In terms of Regulation 5(5)(a)(ii) of the PMLFTR, SPs are required to have in place customer risk assessment procedures to carry out a customer risk assessment ("CRA") prior to establishing a business relationship with or carry out an occasional transaction for a customer. This obligation is dealt with in further detail under section 3.5 of the Implementing Procedures Part I.

A good number of SPs reviewed were either found not to have CRA measures in place or else the processes which they had in place were quite basic and did not allow for a sound assessment of the customer risks. Where a CRA was in place, at times it was observed that not all aspects of customer risks were taken into consideration, which would usually result in a risk assessment that is not comprehensive and does not adequately assess the ML/FT risks arising from establishing a business relationship with or carrying out an occasional transaction for a given customer. This in turn impacts the customer's risk profile since if an assessment was not comprehensive enough, the resulting risk rating would not be accurate and hence resulting in inadequate risk mitigating measures.

Some SPs, while having knowledge about their customers and intended use of the business relationship or scope of the carrying out of an occasional transaction (e.g. an understanding of the customers' respective business operations and geographical exposures), and who could have leveraged such knowledge to assess the ML/FT risk posed by that customer, failed to do so. The information they held was not utilised to determine the level of risk and to determine the appropriate level of customer due diligence and control measures that they should have applied considering the overall risk presented by the customer.

In other cases, it was noted that SPs were considering particular clients as low risk on the basis of their familiarity with such clients, allowing themselves to be overly influenced by the familiarity with these customers rather than basing their risk understanding on a sound assessment. Needless to say, this was resulting in a subjective approach which quite often resulted in the considerations being taken to assess the risks posed by customers not being recorded.

***Case study***

*During a supervisory visit, the SP who was an accountancy firm provided some information about each of the clients that were reviewed. However, this information was not considered in light of possible risks that the customer could expose the SP to since no CRA measures were in place. Nor were the clients assigned with any risk rating and there was no determination of the appropriate level of due diligence that was required to be carried on these clients. When questioned about the possible risk exposure of these clients, the SP was not knowledgeable of the factors that would contribute to a heightened ML/FT risk .The SP explained that the majority of their clients were friends and family members, and since the SP was also the MLRO, s/he deemed such a close relationship to be a sufficient means of mitigating any possible risks.*

*While knowledge on the customers is important, the proper carrying out of a CRA is indispensable to ensure a coherent and uniform approach to risk assessing customers and to implement adequate risk based controls.*


In other instances, it was noted that although the CRA carried out did take into account all the four main risk factors (i.e. client, geographical, product/service/transaction, and interface risks), the criteria that were being considered to assess the risk within each pillar were too generic and inadequate to derive an appropriate risk understanding.

- By way of example, limitedly assessing the customer risk by dividing customers into "self employed", "in employment" or "other" is not sufficient to understand the customer risk. Another common practice seems to be that the customer's activities or trade have been found to be factored into the products/services risk, which risk factors should feature in the section dedicated on customer risk since these are specific to each customer.

It was also observed how certain CRAs in place consisted of forms, such as tick-box questionnaires which included a number of questions with 'yes' or 'no' answers which at times added little value to understanding the customer risk. These forms were considered to be more of an on-boarding form rather than a CRA.

- For example, questions such as "is the expected source of wealth known?" or "is the customer in employment?", while being important considerations, add little value to understanding the customer risk unless the expected source of wealth, where this is necessary is also identified and corroborated with the information on the nature of the employment of the customer when calculating the risk.

Occasionally, it was also observed that SPs were assigning lower inherent risk scores to business relationships which should have been attributed with a higher inherent risk score. This resulted in the risk categorisation being skewed towards the lower end of the spectrum. Thus, SPs were failing to carry out the adequate level of CDD, especially in situations which in view of their high risk nature, would require the application of Enhanced Due Diligence measures. In addition, it was also noted that at times, SPs were relying on the residual risk to risk categorise customers. It is the inherent risk which provides a true representation of level of risks one is exposed to and that will ultimately dictate the levels of controls necessary. Thus, it is the inherent risk that should be used to risk categorise customers. While inherent risk cannot be altered by the SP, the introduction of increased controls can lower the residual risk.

- For example, a complex corporate customer having a cash intensive business was assigned a 'Medium' inherent risk, while in view of the risks surrounding this customer, a high inherent risk is expected. Appropriate levels of controls can then reduce the residual risk.

***Case study***

*Following a review of a CRA tool of a financial institution, it was noted that despite the fact that there were multiple risk scenarios considered and information included in the tool for an array of questions, the score assigned to the replies for such questions was not in line with the level of risk perceived. For example, one of the possible answers that could be chosen for the question on the occupation of the customer was 'business owner', with the weighting assigned being that of 'medium'. No more detail or information on the kind of business of the customer was being included in the tool, on the basis of which the risk could be determined. Although the SP explained that they would obtain more information from the client on the business activities, and that they would physically update the risk assessment tool when such further information was obtained, there was no record that this was being done in practice. Although the SP could manually update the final risk rating assigned, this situation could be easily avoided if the tool included more detailed questions either on the employment of the individual or on their salary so as to be better informed about the source of wealth.*

In other instances, issues related to the timing of the performance of the CRA were noted, where SPs would have carried out CRAs but well after the business relationship would have been entered into. Therefore, in such cases SPs would have onboarded customers and provided them with services without understanding the risks they posed and without understanding the level of controls that should have been applied to reduce the risks identified.

***Case study***

*During one of the supervisory examinations at a credit institution, it was noted how customers were onboarded and allowed to make use of the Bank's services even though no CRA had been carried out by the SP. As a result, the risks to which the SP was exposed to by providing services to these customers were unknown and all customers were being subjected to the same level of due diligence independently of the risks they posed. The SP acknowledged this systematic deficiency and confirmed that it had a backlog of customers which needed to be risk assessed.*

The FIAU has lately noticed an improvement by SPs in the carrying out of CRAs. SPs are implementing and enhancing their CRA measures and are making sure that customers are risk assessed at on-boarding and as circumstances so require during the business relationship.

## 3. JURISDICTION RISK ASSESSMENTS

An indispensable part of the BRA is an understanding of the geographical risk exposure. This would require not only a consideration as to whether the different jurisdictions the SP is exposed to are reputable or otherwise (i.e. whether such jurisdictions have adequate AML/CFT regimes) but also a consideration of the actual ML/FT risks the said jurisdictions are exposed to and how this may contribute to the risk exposure of the SP. The requirement to assess the jurisdictional risks is explained in detail in Section 8.1 of the FIAU's Implementing Procedures Part I.

Some SPs did not have a defined standardised process or methodology in place to assess the reputability and risks of jurisdictions they are exposed to. Instead, they would randomly refer to websites and articles to determine geographical risk. This resulted in SPs having a subjective approach in assessing the said risk, as the assessment of jurisdictional risk and the sources of information relied upon would differ and be dependent on the respective officer/employee carrying out the same. Officers/employees would end up determining the level of risk without having common guidance or direction as to what aspects to consider, and to what extent one aspect should influence the overall risk associated with a given jurisdiction. Furthermore, they would not be guided as to which control measures would be appropriate to target and mitigate the identified risks linked to specific jurisdictions.

In other instances, SPs failed to appreciate the distinction between the reputability of a jurisdiction and the broader ML/FT risks posed by the same. The determination of reputability is more limited in scope and involves an assessment of how robust the AML/CFT framework of a jurisdiction is. This may be achieved by referring to evaluation reports published by international bodies that are responsible for assessing jurisdictions' adherence to international AML/CFT standards, such as FATF, MONEYVAL and other FATF style regional bodies ("FSRBs"). The assessment of jurisdictional ML/FT risks extends beyond reputability, and involves a broader understanding of risks to which the jurisdiction is exposed. By way of example, one is expected to consider whether the jurisdiction is exposed to elevated rates of particular proceeds generating crimes (e.g. a jurisdiction known to be a hub for drug production or a jurisdiction prone to elevated corruption practices), whether the jurisdiction or region is known to have particular terrorist organisations or organised crime groups operating within, or whether a jurisdiction is known to provide for the setting up of non-transparent legal entities and arrangements that could be misused for tax evasion or to conceal the proceeds of other crimes. All these factors could heighten the risk exposure of the SP through its dealings with that jurisdiction. Such lack of distinction between the notion of reputability and wider jurisdictional risk can be seen especially in relation to customers residing or whose business is located in European Union (EU) Member States, which are at times automatically considered to be low risk jurisdictions in view of the adoption of the same robust AML/CFT legal framework. While EU Member States can be considered as being reputable jurisdictions (unless international bodies such as FATF or MONEYVAL pronounce themselves otherwise), this does not entail that they all present a low risk of ML/FT as some of them have significant levels of criminal activity or presence of large organised crime groups, which in turn might impact the ML/FT risk exposure of the SP. The actual level of risk can only be determined once a proper JRA has been carried out.

***Case study***

*During one of the supervisory examinations carried out, it transpired that the SP did not assess the jurisdictional risks to which it was exposed. Although the SP was quite knowledgeable on the possible risk factors that would emanate from offering their services to clients from high-risk jurisdictions, the SP could not explain the control measures necessary to mitigate such risks. The SP explained that they did not require a JRA since all their clients were EU Nationals, which were deemed to be reputable.*

*Notwithstanding that the SP was only targeting EU jurisdictions, the SP was required to carry out a JRA also on EU countries to understand the risks prevailing in such jurisdictions and to what extent the SP's operations could be exposed to such risks.*

It was also observed that SPs at times see the JRA as a very onerous obligation. This also in view of the international outreach of their customers, which may have connections with multiple different jurisdictions. SPs often consider this as triggering a requirement to carry out a JRA on all such jurisdictions.

However, this would go beyond what is required of SPs as in such circumstances they would need to assess the degree and extent of exposure to a given jurisdiction before carrying out a JRA thereon, taking also into account the nature of the service/product the SP is providing. It is on this basis that SPs should determine on which jurisdictions they need to carry out a JRA and how detailed it should be.

One would still need to monitor customer activity including any business activities and trading in order to determine whether geographical exposure changes over time, whether any change thereto also influences the geographical risk exposure of the SP and whether there is the need to revise and update the JRAs carried out.

***Case study***

*During one of the reviews carried out, it was noted that the SP did have a measure in place to risk assess jurisdictions, which measure took into consideration multiple sources and included a methodology as to how the global risk was being calculated. However, this JRA was not an integral part of the BRA and the CRA. The BRA did not include detail on the geographical risk exposure of its clients. As a result, there was no effective use of the JRAs as a means to understand the risk exposures and mitigating measures necessary. The SP's CRA included a section on the geographical risk, however it split this into three categories, being clients from EU countries, business carried out in high-risk jurisdictions, and BOs from high-risk jurisdictions, and therefore consideration to the actual assessment of the countries which the customer was involved with was not featuring in the CRA, including the ensuing risk that such jurisdictions would pose to the SP. Although the JRA in place including its methodology were sufficient, these were not being transposed into the BRA and the CRA measures of the SP, and therefore such JRA was not actually being used in practice.*

Moreover, several SPs, although having JRAs, failed to determine and understand from where the risk would derive and how best to mitigate such identified risk. Rather they were applying a one size fits all approach to managing risks from all jurisdictions exposed to.

For example, certain jurisdictions would be considered as high risk in view of links to terrorism, while others could be considered as high risk due to the lack of transparency of legal entities or arrangements that could be setup in such a jurisdiction. The mitigating measures that SPs would need to implement to manage these risks must differ in nature. For example, when scrutinising transactions for customers who have links with countries who pose a higher terrorism financing risk, care should be given even to the lowest value of transactions. On the other hand, when scrutinising transactions for customers who have links with countries which lack transparency, care should be given to voluminous and/or complex transactions and transfers from companies owned by the same beneficial owner.

***Case study (DNFBP)***

*While reviewing the policies and procedures of a SP, it was noted that the control measure to be applied for clients whose geographical risk resulted to be 'high' was to collect a professional reference letter. While the professional letter may be a good measure to mitigate risks of for example identity theft, or forging of documentation, it cannot be used to counter all geographical risks. The SP was expected to understand the type of risk exposure from each jurisdiction and determine what measures would be more appropriate to mitigate such risks, rather than adopting one measure to fit all circumstances. For example, the adoption of pre-transaction monitoring for transactions being carried out throughout business relationships with jurisdictions where the risk of corruption or fraud is especially high would have been a more appropriate measure to mitigate the risks as it would be key in such circumstances to determine the provenance of the funds and the purpose of the transaction.*

***Case study (financial institution)***

*During the review at a financial institution, it was noted that the JRA of the SP included all the countries that its clients had dealings with. However, when carrying out the CRA, the SP did not include all the countries that the client had connections with but limited its consideration only to the country with the highest risk score. However, it was noted how in a number of instances there would be little to no transactions flowing through the highest risk country, while transactions which were flowing to/from the other countries were much more frequent and of higher amounts. This therefore resulted in an inadequate consideration of the risk exposure and thus inappropriate application of controls to address the ML/FT risks arising from those jurisdictions which may not have carried the highest risk score but with which the customer was transacting with.*

## 4. MITIGATING MEASURES, POLICIES, CONTROLS AND PROCEDURES

Regulation 5(5)(a) of the PMLFTR requires all SPs to have AML/CFT measures, policies, controls and procedures in place which are adequate to address the risk identified through the BRA. These must be formalised (i.e. through a document or system), and should then be implemented when providing services/products to clients. These policies and procedures are to be regularly updated in order to reflect any legislative updates (such as amendments to the PMLFTR and the FIAU's Implementing Procedures) and to reflect any changes in the business activities of the subject person, such as the provision of new services or products or new methods and means through which existing products are offered.

It is worth noting that overall improvements have indeed been observed and more detailed and specific procedures manuals are being prepared. In fact, a number of SPs had even updated their AML/CFT policies and procedures and provided copies of such as part of their representations following a supervisory visit. After reviewing these policies and procedures, and during the meetings carried out as part of the remediation, Enforcement officials noted that SPs were not only preparing more robust policies and procedures that are relevant to their business activities, but were also implementing these in practice.

Certain observations which have been noted in recent years include the following. One of the most common observations is that SPs would not have documented AML/CFT policies and procedures in place. Others would utilise policies and procedures manuals that are prepared by representative bodies, AML/CFT consultants or advisors. While the adoption of sectorial models of AML/CFT procedures are permissible and actually the development of such model procedures serve to better guide SPs and provide them with insights as to what type of controls and CDD measures should be set out in such policies and procedures, it is important to treat these sectorial procedures as models and SPs should always ensure that these are tailored to their operational setup, business model and activities.

In other instances, it was noted that SPs took the approach of reproducing the AML/CFT obligations set out under the FIAU's IPs, without modelling the same according to their own business reality and risks identified.

***Case Study***

*The procedures manual of a particular SP did not reflect the specificities of the SP. The SP had engaged a third party to prepare a procedures manual. However, the contents of the document were very generic and included several possible scenarios which were not relevant to the SP. In fact, the manual was not fine-tuned to suit the business of the SP. Additionally, this procedure manual also made reference to a specific risk assessment tool which the SP did not even have in place. As a result, the procedures manual, while in respect of some aspects was adequate, was not entirely relevant to the SP's operations. Moreover, it was observed that even the parts that were relevant were not being implemented, which continued to reinforce the indication that the SP adopted a set of procedures and made them his own simply to fulfil on paper its obligation at law. Having a documented procedures manual is futile unless it is also effectively implemented*

At times, in the case of smaller firms or sole practitioners, it was also observed that while procedures manuals were not formalised, SPs were still implementing a number of AML/CFT measures . As a result, in such cases, SPs were found to be adequately complying with their CDD and other AML/CFT obligations. In these cases, SPs were however deemed not to be compliant with the obligation to have formalised AML/CFT processes and procedures in place, which is an important requirement to ensure uniformity in the application of AML/CFT safeguards.

***Case study***

*During one of the examinations carried on a Notary Public, it was observed that the Notary did not have his/her own formalised policies and procedures in place. However, all the client files that were reviewed had the necessary information and documentation required, and there were varying levels of due diligence implemented by the SP, commensurate to the risks observed. It later transpired that the SP was basing his/her approach to the implementation of AML/CFT obligations by following an FIAU guidance document which was providing information on specific risk factors and commensurate mitigating measures. The FIAU in this case still required the Notary to document the procedures that were otherwise being implemented. However, taking note of the Notary's interest and willingness to comply with his/her obligations and the implementation of established (though not formalised) procedures based on a sound understanding of risk, the FIAU did not consider the breach of not having formalised procedures in place to be a serious one and this did not lead to the imposition of pecuniary fines.*

Other findings at times related to the effective use and implementation of procedures manual. At times it was found that the procedures manual would in itself be appropriate but that it would then not be implemented in practice by SPs. Such findings are considered to be serious, as the point of having AML/CFT procedures in place is that of ultimately ensuring effective compliance with AML/CFT obligations and mitigating effectively any possible risks that one would be exposed to. Hence it is considered futile to have processes and procedures in place simply for the sake of having them without implementing same in practice, and where appropriate, monitoring that they are being adequately implemented.

***Case Study***

*The procedures manual that a remote gaming operator provided to the FIAU prior to the carrying out of a supervisory examination were noted to be quite robust and provided adequate guidance as to how the customers were to be onboarded and how their business relationship was to be monitored throughout. Yet, the onsite compliance review revealed that the procedures manual was not being implemented at all by the SP. Although the procedures manual indicated that all the clients who reach the Euro 2,000 threshold would be subject to a CRA and would be requested to provide due diligence documentation, none of the client files reviewed who had surpassed the said threshold were risk assessed. Furthermore, although customers were repeatedly asked to provide due diligence documents and were informed that their account would be suspended until the requested documentation is provided, customers who failed to provide the necessary information and documentation were still allowed to wager and withdraw funds.*

# 5. CUSTOMER DUE DILIGENCE OBLIGATIONS

The obligation to carry out customer due diligence measures emanates from Regulation 7(1) of the PMLFTR and is explained in further detail under Chapter 4 of the FIAU IPs Part I. In terms of Regulation 7(1), SPs are required to identify their customers and verify their identity by collecting documents and information from reliable and independent sources, and also to identify and verify the identity of beneficial owners (BOs) and the ownership and control structure of clients that are legal entities or arrangements. This same Regulation further requires SPs to obtain information and/or documentation on the purpose and intended nature of business relationships and to establish customer business and risk profiles. In terms of Regulation 7(1)(d) SPs are then required to carry out on-going monitoring of established business relationships, which involves the obligation to keep obtained CDD documentation up to date and the scrutiny of the customer's activity together with the transactions carried out throughout the duration of the business relationship.

### 4.1. Identification and Verification of Clients and Beneficial Owners

The supervisory examinations carried out over the past two years indicate that overall SPs have a sound knowledge of their obligations to know who their customer is and, where applicable, who is/are their customers' Bos. In respect of identification and verification obligations, while shortcomings have been identified, these are usually considered to be minor to moderate across all sectors. With respect to the obligation to identify and verify the identity of BOs, it is not common to come across cases where SPs would not know who the beneficial owners of corporate clients or other legal arrangements are. As is explained hereunder, in most cases the deficiencies noted with respect to this obligation consist of cases where SPs would not have obtained and verified all the identification details that are set out under the IPs Part I, however the SP would still have determined who the BO was in such a case.

The predominant shortcoming noted in this regard related to the verification of residential addresses of foreign customers. This was mostly the result of the verification document obtained not including the details of the customer's residential address as would be the case with most passports.

It was observed that in most of the cases, SPs would know who the BOs of corporate customers are as well as understanding the corporate structure. However, it was observed how SPs sometimes would not question the purpose behind complex structures. It was also noted how in circumstances where there would be no one natural person identified as a BO, in rare occasions SPs did not extend such verification requirements to determine Senior Managing Officials.

In occasions where SPs failed to determine who the BO of a corporate customer was, this was usually the result of over reliance on corporate constitutive documents to meet their obligations at law. While corporate constitutive documentation (such as M&As) would indicate who the directors as well as BOs of corporate customers are, one would still need to obtain further information and documentation to comprehensibly identify and verify who the BO is.

***Case study***

*Shortcomings with regard to the identification and verification measures were noted in several files of a real estate agent. Whenever the sale of property involved a legal entity, the SP, while carrying out customer due diligence on the agent (i.e. the person appearing on behalf of the legal entity) and the legal entity, failed to verify the identity of the BOs of the legal entities.*

On very rare occasions it was identified that CSPs would obtain information and organigrams from customers without obtaining independent and reliable information to comprehensibly confirm the corporate structure of customers.

***Case study***

*During a supervisory examination at a CSP, one of the files reviewed involved a corporate customer which formed part of a complex corporate structure that had shares held in a foundation registered in a non-EU jurisdiction. In this case the CSP failed to obtain supporting documentation (such as the Foundation's constitutive document) to confirm who the beneficiary/ies of the foundation and ultimately the BOs of the corporate entity were and relied on a declaration made by the foundation's administrator located in a non-EU jurisdiction. A declaration to determine who the BO was should not have been considered as sufficient for the purposes of establishing the ownership and control structure of the corporate customer in question. Instead, the SP should have resorted to an independent and reliable source and obtained supporting documentation to verify the information being provided by the customer.*

There were also one-off cases where SPs failed to determine who the BO/s were. Such circumstances were at times also of a very serious concern and included situations where the SP did not even carry out any form of due diligence on such customers, including the basic identification and verification requirements.

***Case study***

*In a number of files reviewed at an investment company, the SP failed to establish the identity of the directors and of the BOs of the corporate customers prior to onboarding the same. Although the SP had eventually terminated its relationship with these customers due to the fact that they were not forthcoming with providing the required information and documentation, the SP had still processed a number of transactions for the customer, despite not having all the necessary information on who ultimately owns and controls the corporate structure.*

*In addition, this same SP was also offering payment services to customers, without having first onboarded them as customers, and thus, without carrying out the necessary customer due diligence measures. As a result, the SP failed to identify and verify the identity of both natural and corporate customers and also failed to determine the BOs behind the corporate customers.*

Other shortcomings were observed in circumstances where SPs were servicing charities (created for a charitable purpose with no persons having ownership interest) or companies where, in view of the distribution of shares and/or voting rights, no individual BO could be determined. In such situations, SPs would conclude that there was no BO without considering the individuals in senior management positions or otherwise responsible for the entity's administration as BOs in terms of law and carrying out the appropriate CDD in their regard. While in most cases the identity of these officials would be known, the SP did not proceed to verify their identity.

### 4.2. Assessing and obtaining information on the purpose and intended nature of business relationships and establishing the customer's business and risk profile

Another indispensable part of the CDD process consists in assessing, and where appropriate, obtaining sufficient information and/or documentation to establish the purpose and intended nature of the business relationship and to build a comprehensive customer's business and risk profile. SPs are required to have an understanding of what to expect throughout the course of the business relationship, both in terms of the activity to be carried out and the expected value and volume of the transactions carried out by customers using the SP's services or products.

At times it was observed that SPs did not have the necessary processes and measures in place to ensure the collection of sufficient information to establish the client's profile and the purpose and intended nature of the business relationship.

- For example, SPs used onboarding forms that required the collection of generic client information such as "in employment", "trading/holding company", and expected source of funds marked as "from business operations". Such vague information is not considered sufficient to establish the customer's business and risk profile.

- In other instances, SPs were making use of very wide or vague brackets to collect information on the expected level of activity which do not allow for a proper understanding of what to expect throughout the business relationship, such as indicating that the expected value of transactions or the expected turnover will be "more than Euro 2,000,000".

- The obtainment of generic information was also observed in a number of examinations carried out on remote gaming operators. While remote gaming operators are not expected to gather source of wealth information/documentation from each and every client, where this is necessary in view of the higher risks identified, obtaining details such as "employed", "in business", "entrepreneur" etc add no value in understanding the customer's profile and determining his source of wealth. Instead, the SP would be required to collect information either directly from the player on the employment or otherwise use information from statistical models. In the case of 'high' risk clients, this information would need to be supplemented with documentation which actually substantiates the information collected.

Subject Persons should ensure that they obtain the details necessary to understand the customer's activity, the intended use of the products and/or services offered by the SP and where appropriate how the customer intends to fund their operations. The details and extent of information and documentation to be obtained is dependent on the level of risks perceived.

### 4.3 On-going monitoring of business relationships

The obligation to carry out ongoing monitoring of business relationships is set out under Regulation 7(1)(d) of the PMLFTR and is composed of two aspects:

a) the scrutiny of transactions or activities being undertaken throughout business relationships to ensure that these are in line with the subject person's knowledge of the customer, and the customer's business and risk profile; and

b) ensuring that the data, documents and information obtained as part of the CDD process are reviewed and kept up to date.

Scrutiny of Transactions

The scrutiny of transactions, which is envisaged under Regulation 7(2)(a) of the PMLFTR is one of the most important obligations at law. Transaction scrutiny enables SPs to detect anomalous, unusual, complex and large transactions and to question whether there exists a justifiable reason for such transactions. A suspicious report would need to be filed with the FIAU when such reasonable justification for these transactions cannot be established and there is a suspicion that the transactions may be linked to ML/FT.

It is worth noting that throughout the past couple of years the FIAU has noticed several improvements with regards to adhering to this obligation particularly within the Credit and Financial Institutions and the Gaming Industry, whereby these institutions and industries are investing in transaction monitoring tools. These tools are assisting SPs by generating alerts which need to be acted upon, particularly in relation to suspicious activity which falls outside the customer's level of activity. Significant improvement was also noted within the Notarial sector when it comes to the scrutiny of individual transactions undertaken.

Credit and Financial Institutions are at the forefront of any effort to combat ML/FT in view of the volume of transactions passing through the accounts held by customers with such institutions. While post transaction scrutiny is in most instances being carried out quite effectively, various deficiencies are being identified in so far as pre-transaction monitoring is concerned.

There were instances where pre-transaction monitoring was found to be limited only to screening against sanction lists and reviewing for particular details included in the payment message, such as reference to particular invoices or agreements or messages indicating the purpose of the transaction (for ex. “loan repayment”, “donation” etc). This limits the effectiveness of any pre-transaction monitoring carried out by the said institutions which would also necessitate the obtaining of documentary evidence, especially with respect to complex and large transactions. SPs are also required to refer to Regulation 11(9) of the PMLFTR which delves into the requirement to apply EDD in cases of complex or large transactions.

In other cases, it was found that transaction monitoring systems had limited pre-set parameters used for pre-transaction monitoring which were not sufficiently exhaustive to detect anomalous and suspicious transactions.

- For example, transfers between multiple accounts which do not have any economic or commercial sense in lieu of the customer’s established activity and profile were not being captured by the systems in place.

- Similarly, transactions not in line with the customer profile were not being detected since customer information was being used only when a transaction is being reviewed a-posteriori.

***Case studies***

*(1) One of the Banks subject to a compliance review was clearing off transactions between customers as 'internal transfers' and as a result these were not at all being scrutinised. The Bank was allowing for money to flow from one account to another, at times within the same day, without understanding the rationale for such a transfer and the relationship between the customers. The basis for such clearance was that these transactions were taking place within accounts held with the Bank, thus considered as internal transfers.*

*(2) A credit institution, in its BRA, had declared that it adopts a robust transaction monitoring procedure, whereby all transactions which exceed the Euro 20,000 threshold, were being tightly scrutinised and supporting documentation collected prior to approving the transaction. It was further noted how as per the BRA, the SP had procedures in place to ensure that all of its clients provide supporting documentation relevant to transactions either prior to the transaction or on the same day that the transaction goes through. The SP had assessed this control, amongst others, as being 'Very Strong' to mitigate the inherent risk. However, while reviewing a sample of transactions throughout the supervisory examination, it transpired that in actual fact, the SP was not collecting any supporting documentation prior to approving the transactions, despite the fact that all of the transactions reviewed during the supervisory examination exceeded the Euro 20,000 threshold. Additionally, with regard to the documentation that was collected after the approval of the transactions, this was not always being vetted since in a number of instances, the documentation collected did not corroborate with the transactions.*

Moreover, cases of larger institutions processing significant volumes of transactions without having ongoing monitoring tools or otherwise having ineffective tools are still being encountered.

- For example, the tool would be ineffective because the scenarios inbuilt in it would not be tailored to the modus operandi and risk appetite of the SP, including for different transactions that the SP would be processing. Value thresholds utilised were also at times set too high when considering the amounts customers usually transacted and the risks involved, since the tool failed to flag large transactions.

A number of SPs were also at times limiting their review to incoming transactions, without scrutinising outgoing transactions.

- By way of example, layering of funds through accounts owned by the same customer or through a group of customers is a money laundering typology that is best detected when outgoing transactions are also analysed and in these instances, post transaction monitoring proves useful since a holistic review of both incoming and outgoing transactions can be carried out.
- Terrorist Financing or Terrorist Activities are also usually identified from a review of the flow of outgoing funds. This would therefore necessitate the taking into consideration the destination of where funds would be transferred to. Mostly incoming funds would not be suspicious in such circumstances and suspicion would usually be determined from analysing outgoing transactions.

Terrorist financing can be monitored through various methods, such as for example:

(i) monitoring transaction, particularly those which are linked to jurisdictions that are located on the border with or close to other jurisdictions known for their funding of terrorism risks or terrorism;

(ii) monitoring transactions of donations, crowdfunding or transactions going to voluntary and/or religious organisations, particularly foreign ones;

(iii) collecting sufficient information on the trading activities of the client, particularly where the client exports dual use goods to countries known to present risks related to terrorism;

(iv) monitoring the accounts of clients for any incoming funds especially in small amounts from multiple jurisdictions, and which are then immediately either withdrawn or else used to purchase flights to countries or territories which are linked with or close to countries known for their terrorism financing risk.

For more information on how to identify typologies and red flags with regards to FT, SPs are invited to refer to the FIAU guidance document on the funding of terrorism entitled: **Guidance Document on The Funding of Terrorism**, which was published by the FIAU on 7 February 2018 and its revision dated 17 July 2020.

While post transaction monitoring is more commonly and effectively implemented by SPs (in comparison to pre transaction monitoring), certain shortcomings were also observed. Transaction structuring was at times not considered for monitoring purposes and therefore customers transacting below the established threshold would slip through the net without any monitoring being carried out. A review to understand patterns of transactions and determine any incongruencies that would raise doubt also in line with previous patterns or with the available information on the customer was also at times required.

***Case study***

*One of the files reviewed at a credit institution related to a corporate customer who had obtained a loan to finance the purchase of an item. It transpired that the item was not purchased by the corporate customer of the bank himself, but by a connected third party (first sale). The item was then sold to another company (second sale). Although the Bank's corporate customer that took out the loan for the first sale was not part of this sale agreement, and it was the connected third party which was appearing as the seller of the item, the proceeds of the second sale were remitted to this Bank's corporate customer's account.*

*A review of these transactions was carried out by the Bank after the transactions had taken place. When the SP was asked during the supervisory examination to explain the rationale behind all this, and why the third party did not take the loan itself to acquire the property, the SP indicated that the third party who was also a legal person formed part of the same group of companies of its customer and that this was a normal way of carrying out transactions between intra group companies. However, this cannot be considered as a justification for allowing funds to flow freely between group companies without understanding and obtaining the necessary documentary evidence to substantiate the rationale behind such transactions.*

With regards to Notaries and Real Estate Agents, while it is not customary for such sectors to establish business relationships, they still have obligations to detect anomalous, unusual or suspicious transactions or transactions presenting higher risks, such as payments in cash or from customer's own funds. However, it was noted that payments in cash would not always be queried by SPs within these sectors. While not frequent, there were isolated cases where the SP failed to question the purchase of immovable property involving substantial amounts of lump sums paid from own funds.

Nevertheless, it has to be remarked that improvements have been observed in these sectors, with Notaries and Real Estate Agents becoming more conscious of the need to scrutinise high value and/or risky transactions, such as those carried out in cash or through own funds (i.e. not via a bank loan). Other ML typologies linked to property transactions, such as overvaluation of the property or undervaluation of the property are also being identified and scrutinised more regularly by the Notaries and Real Estate Agents.

***Case study***

*Following a review of 10 client files during a supervisory examination carried out on a Notary, it was observed how the transactions of immovable properties in six of the files reviewed were funded from the customer's own funds, without such files containing any information on the source of wealth or source of funds of these customers. The Notary could not explain from where these funds were derived (whether they were from the customer's savings or employment, donations or succession etc) since the forms found on file did not include such detail.*

Transaction scrutiny can at times have close affinity with the application of EDD measure, either as an EDD measure in itself due to the risk presented by the customer thus resulting in closer examination of transactions and activities carried out by the customer, or in view of the fact that the result of transaction scrutiny may lead to an increase in the customer risk and the application of corresponding EDD measures. Of interest in this regard are situations which the FIAU has encountered when supervising CSPs. There were instances where CSPs who provided directorship services also acted as signatories on bank accounts for corporate customers. At times acting as signatory on bank accounts for corporate customers was considered by CSPs as an EDD measure as it allows them to have more control over and insight into the activities of their corporate customers. However, acting as a bank signatory without having the measures in place to actually monitor the transactions and activities of customers may not always be sufficient and may put CSPs in breach of their on-going monitoring obligations. The mere acting as a bank account signatory for corporate customers without the review of customer activity and transactions is thus futile.

***Case study***

*While reviewing the transactions of one corporate customer of a CSP, the officials were told that the Directors were signatories on the bank account and thus they were approving and reviewing transactions. It was noted that the transactions were all making reference to a loan agreement between the customer and another company. However, when this loan agreement was provided to the FIAU officials during the visit, it was determined that the agreement was rather vague and did not include the necessary details required, such as the purpose of the loan, the duration of the loan, and any possible interest rates that would be applicable. Furthermore, the Directors could neither explain the rationale for the loan nor could they provide any detail as to what the activities of this particular client were. Additionally, although the Directors explained that the funds for the loan were originating from a listed fund, it was noted that no supporting documentation was available to substantiate this claim. Therefore, the CSP's involvement as a signatory on the customer's bank accounts did not result in effective understanding and scrutiny of the transactions taking place.*

Some shortcomings were also noted in supervisory examinations carried out on Accountants and Auditors. While inevitably such professionals would be privy to information on past transactions that a customer would have made in the year under review, some still fall short of questioning transactions that were not in line with the customer's profile and go beyond the customer's expected activity, as well as ensuring that sufficient documentation to justify certain transactions are actually obtained.

***Case study***

*One of the files chosen throughout a supervisory examination on an accountant included an increase in share capital. The increase in share capital, which was of circa Euro 200,000, was fully paid up. Although the accountant in this case indicated that he was taking care of all the accounts of multiple companies of this particular client, and that he was aware that this client was financially capable of affording this share capital increase, the SP did not seek to ascertain the source of these funds and support this with the required documentation, a practice which should have been expected in light of the substantial amount involved.*

Ongoing monitoring of CDD

Regulation 7(2)(b) of the PMLFTR requires SPs to ensure that the customer due diligence information and documentation held on file throughout the course of the business relationship is reviewed and updated as necessary. Although it is customary for SPs to update the customer identification details and documentation in the case of trigger events, such as when a passport expires, this obligation also includes the reviewing and updating of information on the activities of the customer, which is at times overlooked. While most SPs had procedures in place requiring the periodic review of customer relationships (independently of trigger events), the implementation of such procedures were at times not being followed in practice.

It was observed that at times, SPs had considerable delays in the updating of customer information, which is usually the result of lack of resources, ineffective procedures and ineffective follow up on requests made to customers for updating of the customer profile.

- By way of example, while a customer may be asked for updated information necessary to enhance his profile, failure by the customer to provide information would not lead to an escalation in actions by SPs. SPs should therefore ensure that measures are in place to escalate customers' lack of cooperation. Reminders, warnings and gradual restriction of service would be indispensable to ensure that the necessary information and documentation is obtained.

***Case study***

*During a supervisory examination on a credit institution, it was observed that although the onboarding process was sufficiently robust to gather all the necessary information, such information was not being referred to in practice when reviewing the customer activities and transactions. As a result, customers were carrying out activities which were not in line with the established profile, yet no action was carried out by the SP to understand this deviation and update the customer's profile. For example, for one of the customers, although the on-boarding forms which were completed by the client indicated that the client's expected source of funds will be deriving from his employment, in the first couple of months since the client was on-boarded, the value of the transactions that took place exceeded the customer's yearly salary tenfold.*

Moreover, situations were found where SPs would update a customer's profile to reflect a change in the pattern of transactions or activities carried out, with the new transactional pattern becoming the new expected level of activity, without however the SP enquiring and seeking explanations to establish the rationale for such a change in activity. This defeats the purpose of on-going monitoring which should be to detect outlaying transactions and activities falling outside of the customer's established profile and determining whether there is a reasonable explanation for the same.

***Case study***

*A SP who was carrying out recurring accounting services to a number of companies, failed to keep updated the information and documentation held on the customer. The due diligence on the client had been expired for several years, and the organigram held on these clients were all outdated and were not reflecting the current ownership structure of these companies.*

*Furthermore, throughout the course of the business relationship, several adverse media became available on some of the SPs customers, yet no recent adverse media checks, PEP checks and sanction screening were found to have been carried out. While it is at times comprehensible that SPs do not immediately update customer information, through trigger events or otherwise through the ongoing review of the relationship, information and documentation must be accurately updated.*

## 6. ENHANCED DUE DILIGENCE

Regulation 11 of the PMLFTR provides for the obligation to conduct Enhanced Due Diligence measures in situations which represent a higher risk of ML/FT. Enhanced Due Diligence measures are various, ranging from collecting additional documentation from the client, to carrying out more regular monitoring on the clients and more scrutiny on the transactions or activities of such clients.

The need to apply Enhanced Due Diligence (EDD) measures can arise at different points throughout the relationship, being either at onboarding stage, or throughout the duration of the relationship. It was observed that while it is customary for SPs to have measures in place to identify PEPs and to carry out the necessary EDD measures, other circumstances giving rise to a higher ML/FT risks were more difficult to determine, which at times owed to inadequate CRAs. This would result in the EDD measures required to manage the heightened risk not being implemented.

- By way of example, customers considered to pose a higher risk of ML/FT or whose expected source of funds or source of wealth would be questionable, should be required to provide documentary evidence to substantiate the SOW/SOF information available. These could, for example, be sources such as inheritance, shareholder's loan for a corporate customer, income generated from various business etc. While the information obtained would be a good indication, in higher risk situations, supporting documentation such as a will, loan agreements, share valuations, contract of employment, payslips etc have to be obtained and scrutinised to corroborate the information provided by the customer.

***Case study:***
*A remote gaming operator had not implemented any form of EDD measures despite having players who are residents of high-risk countries and players engaging in higher risk game types. In fact, one of the players reviewed had engaged in low odds sports betting – which is a betting method that usually ensures a higher chance of winning – and wagered substantial amounts of funds through such games. The risk would be that ill-intentioned individuals would make use of these bets to launder proceeds of crime without the risk of losing too much of the funds wagered. No measures were implemented by the SP to monitor the relationship more closely and to monitor the activity to determine whether such activity gives rise to suspicions.*

Enhanced ongoing monitoring may also at times be necessary in view of the higher risks which may materialise throughout the course of the relationship. The purpose of such enhanced monitoring is to be more vigilant on the customer's activities and transactions taking place to ensure that any anomalous behaviour is identified.

## 7. INTERNAL AND EXTERNAL REPORTING

Regulation 15(3) of the PMLFTR obliges SPs to report to the FIAU any suspicions of proceeds of crime, ML or FT that subject persons encounter when dealing with their customers, regardless of the amounts involved in any such suspicious transactions.

It is positive to note that the number of Suspicious Transaction Reports (STRs) submitted to the FIAU has been increasing steadily over the past years. In fact, the number of suspicious reports submitted to the FIAU has gone up from 1,668 in 2018 to 5,090 in 2020, and the prospects are that in 2021 the number of suspicious reports received will significantly exceed the 2020 figure. Moreover, increases in suspicious reports submissions are being noted across all the material sectors in Malta, although the main contributors remain the Banking and Remote Gaming Sector.

Nonetheless, the FIAU believes that Investment Service Providers, Trusts and Corporate Service Providers, Notaries, Auditors and Accountants should be submitting more suspicious reports than they are currently doing, and this in view of the fact that these are some of the most material gatekeepers which are considered to be exposed to heightened risks of ML/FT according to Malta's National Risk Assessment. This section identifies some of the shortcomings that are being encountered throughout supervisory examinations in connection with the identification and reporting of suspicious transactions and activities.

It was noted that at times SPs failed to have the necessary measures in place to efficiently analyse internal suspicion alerts that are generated through their on-going monitoring systems. On other occasions, SPs were clearing off alerts generated without having in hand the necessary information to justify such clearing off.

- By way of example, alerts would be cleared as non-suspicious since they were similar to past transactions, even though those transactions were never in line with the established customer profile in the first place. While there may be justifiable reasons for flagged transactions, these alerts generated should be reviewed and be cleared off only if information or documentation obtained satisfactorily indicates that such transactions are not suspicious. Subject persons should also consider updating the customer's business and risk profile with any new information and material that is obtained when scrutinising such alerts or activities.

- Other alerts would be cleared off because these would be considered as internal transfers, being either transfers between own accounts or otherwise transfers between corporate customers owned by the same beneficial owner. Such alerts would thus have been cleared without a proper analysis of the flow of funds which is crucial to determine the suspicion or otherwise of such transactions.

- Other circumstances related to adverse media linking customers to financial crime. Although adverse media would not necessarily lead to the submission of a suspicious report, at times such adverse media was not being considered by SPs to understand the implications of such adverse information on the transactions and activities being carried out throughout the business relationship. Such considerations would be necessary to determine whether there would be any links to the activity of the customer carried out through the relationship with the SP that would merit the submission of a suspicious report.

***Case study (financial institution)***

*While reviewing a sample of transactions at a financial institution, it was noted how the internal transfers that were taking place were not undergoing the same scrutiny as external transfers. In fact, the tool used by the SP was not calibrated in a way to flag internal transfers unless these exceed substantial amounts. This allowed for funds to flow through multiple accounts belonging to the same client (natural person) or through accounts held by corporate clients owned by the same natural person, without any form of scrutiny being carried out. It was also observed that cash withdrawals were all taking place either on the same day that the funds were being received within the above-mentioned accounts or on the following day, with these withdrawals all taking place from the same ATM machine or from ATM machines which were in a close proximity to the others. These withdrawals were taking place in a country known for the presence of organised crime and terrorist groups, which further increased the risks of the transactions. In two years, a total of Euro 7,000,000 in cash withdrawals took place without the SP being alerted by its transaction monitoring tools, and without the SP raising any internal reports to determine whether there was suspicion of ML/FT that had to be reported to the FIAU.*

***Case study (DNFBP)***

*During a supervisory examination on an accountant, it transpired that one of the clients featured in several adverse media both locally and abroad. Yet the SP was satisfied with collecting a declaration from the client himself confirming that the adverse media being reported was not true. The SP did not factor in this risk factor when assessing the customer's risk and in turn, did not increase the frequency of the monitoring of the business relationship and the scrutiny of the customer's activities. Had this been done, the suspicion that the client was involved in illicit activities would have been identified. No suspicious reports were ever raised by the SP. While SPs should not take adverse media as an outright determination to submit a suspicious report, adverse media from independent and reputable sources should be considered as a red flag, raising the need to review the customer's profile and enhance monitoring of their activity as necessary. Should suspicion of ML/FT arise on the basis of such considerations, SPs are then required to report the suspicion to the FIAU.*

It was also observed that while in general SPs proceed to terminate a business relationship in circumstances where the customer becomes unresponsive or would not be willing to provide the necessary customer due diligence information and documentation, at times SPs fail to assess whether such a behaviour is indicative of suspicions of ML/FT to warrant the submission of a suspicious report to the FIAU.

***Case study (DNFBP)***

*In a particular instance, a corporate client of a CSP had its business relationship terminated due to the fact that the client was not forthcoming with the required documentation on its ownership structure, which included a trust, and on the beneficiaries of this trust. Despite being concerned and growing suspicious on the fact that the client was extremely reluctant to provide the required information and documentation, the SP proceeded with terminating the business relationship however did not consider whether it was necessary to file a suspicious report with the FIAU.*

SPs are required to submit suspicious reports to the FIAU in a prompt manner. The FIAU would like to highlight that recent legislative changes to Regulation 15(3) of the PMLFTR, which came into force in May 2020, have stressed even further the importance of submitting suspicious reports promptly, by removing the five working day timeframe for reporting suspicions of ML/FT. The FIAU understands that there are SPs, who in view of the implementation of AML/CFT remediation plans, are carrying out *a posteriori* reviews of business relationships and submitting suspicious reports, albeit late. While the FIAU commends such SPs for taking remediation actions which are leading to the identification and submission of suspicious reports, the FIAU hereby reminds SPs about the importance of ensuring that on-going remediation plans do not hamper their ability to attentively review and monitor current transactions. It is to be ensured that any identified suspicions be reported promptly.

Occasionally, it was observed that the assessment of customer files during supervisory examinations led SPs to review their relationship with such customers and submit suspicious reports. Thus, FIAU officials would have triggered the SP to carry out a review of the case and to subsequently submit suspicious reports to the FIAU, although the SP should have reported said suspicions without any external influence.

***Case study (DNFBP)***

*While reviewing a sample of files during a supervisory examination, it was observed that one of the files did not have the required customer due diligence information in place. When asked to provide this, the SP conceded to the fact that they did not collect all the required information on this client, and that they were not aware of what the actual activities of their corporate customer were. Although the corporate client had a multi-tier shareholding structure which included trusts and nominees set up in offshore jurisdictions (known for lax transparency obligations), the SP could not explain the rationale behind the setting up of such a structure and assumed that this was a tax structuring setup without questioning and seeking to obtain further information from the customer. Shortly after the supervisory examination, the SP proceeded to file a suspicious report on this client and terminated its business relationship shortly after the submission.*

***Case study (financial institution):***

*A supervisory examination on a bank revealed how a total of USD 2,600,000 were transferred to a corporate customer of the bank. A loan agreement between the parties was held on file at the bank, however this was obtained a year after the transfers took place. The agreement referred to the reason for the loan which was intended to finance the acquisition of an immovable property. According to the bank's records, the customer (the company obtaining the loan) was incorporated to invest and hold assets in the real estate market in a particular jurisdiction. However, this was a different jurisdiction to the one where the immovable property subject of the loan was located. Moreover, once the funds were received by the corporate customer, these were transferred out from the customer's account to another company seemingly within its own group for the purpose of equity contribution and loan from shareholder. Therefore, the funds were not used for the purposes they were actually granted for ie: to purchase the immovable property. Moreover, while according to the loan agreement, interests were due on the loaned amount, no interest payments were actually made or demanded.*

*The loan agreement was thus created to give legitimacy to the movement of money from one account to the other, this particularly since the purpose of the funds being loaned and the actual use of such funds were not corroborated. However no suspicious report was raised by the bank in relation to this operation, and no records of any internal analysis were identified by FIAU officials.*

## 8. THE MONEY LAUNDERING REPORTING OFFICER AND THE COMPLIANCE OFFICER

As per Regulation 15(1) of the PMLFTR, subject persons are required to appoint an officer of sufficient seniority and command as the Money Laundering Reporting Officer (MLRO) and whose main responsibilities are to receive internal reports on any potential ML/FT suspicions, analyse these and submit these to the FIAU where there is knowledge or suspicion of ML/FT. The MLRO is also tasked with ensuring that any requests for information made by the FIAU are responded to in a prompt manner, while SPs are required to ensure that the MLROs are being provided with the necessary training, resources and authority to be able to exercise their functions in an efficient and effective manner.

Furthermore, as per Regulation 5(5)(c) of the PMLFTR, depending on the size and nature of the SPs business, SPs are required to appoint an officer at management level (i.e. compliance officer), whose main responsibilities include the monitoring of the day to day implementation of the SPs AML/CFT measures, policies, controls and procedures. While SPs may decide to allocate the compliance management role and the MLRO role to separate officials, it is still customary (especially in smaller and medium sized firms) to have the MLRO also act as the SP's compliance officer. For this reason, the term 'MLRO' is being used to cover both roles unless otherwise stated.

There have been cases identified through supervisory examinations as well as through authorisation processes when MLROs were found not to have the necessary skills, experience and expertise to carry out such a crucial role. In such scenarios, the SP would be required to take immediate action to ensure that the person appointed as an MLRO is able to carry out the functions entrusted to the same in an effective manner. At times, SPs were requested to remedy this by providing the necessary training to the MLRO.

At times it was also observed that the MLRO's other involvements with the SP created a conflict such as is the case with the individual also being the beneficial owner of the SP or otherwise being involved in servicing customers and extending the customer base of the SP. In such circumstances SPs were required to replace the MLRO and appoint a more qualified person particularly when the current MLRO was found to be substantially lacking in ML/FT knowledge.

***Case study***

*When interviewing the MLRO, it was clear that this individual had accepted the role without clearly understanding the requirements and duties that are expected when occupying such a role. The MLRO did not have knowledge of ML/FT risks surrounding the SP's operations, and on the control measures in place to manage the SP's ML/FT risks. Th MLRO had also never attended any training relevant to the duties of the MLRO and could not answer any questions on the control measures in place and how the SP was addressing its ML/FT risks.*

Occasionally, it was observed that the MLRO was not the ultimate person deciding whether or not to submit a suspicious report to the FIAU. This was either because of the direct involvement of other officials, such as senior management or the board of directors in this decision-taking process, or otherwise due to such company officials indirectly influencing the decision of the MLRO. While such instances are not common, such circumstances raise serious concerns on the SP's ability and willingness to implement effective AML/CFT controls and thereby, to avoid being used as a vehicle of ML/FT.

***Case study***

*During a visit at a credit institution, it was observed how the Board of Directors was intervening in the compliance function of the Bank, undermining the compliance culture that the Compliance Department of the Bank were trying to instill. For instance, although the compliance team presented an audit highlighting the various AML/CFT failures of the Bank and the actions that need to be taken to overcome such failures, these were not acted upon by the Board of Directors. Rather the Board delayed any action necessary by appointing independent external auditors to carry out an independent audit, who in turn reconfirmed the findings presented by the Compliance Department. Yet, even after the findings had been reconfirmed, the Board remained reluctant to provide the necessary resources to enable the Compliance Department to carry out its functions effectively. Moreover, the MLRO's decisions were constantly being overruled by the Board of Directors, who were ultimately controlling the level of adherence by the Bank to AML/CFT obligations, or rather the lack thereof.*

Furthermore, in a limited number of cases, it was observed that the MLRO did not have full and unlimited access to all records, data, documentation and information on the SP's clients to be able to fulfil his scrutiny and reporting responsibilities. This would usually be indicative that the MLRO does not have sufficient seniority and command, and is not operating in an autonomous manner. While the MLRO is not expected to be knowledgeable about all customers and may ask other officials for details about the same, s/he should always have access to information held on the customer, such as customer records, transaction history, and customer risk assessment information, amongst others, to be able to assess any internal reports and potential suspicious activities.

## 9. RECORD KEEPING

Record keeping obligations, which stem from Regulation 13 of the PMLFTR, require SPs to keep records of customer due diligence information, transaction records and other information obtained in fulfilment of the AML/CFT obligations set out under the PMLFTR. Retaining the necessary client records assists SPs in carrying out ongoing monitoring and providing timely information that may be requested by the relevant authorities to assist them in their AML/CFT functions. Records are to be kept for a period of 5 years which in particular circumstances, may be extended by a further 5 years.

While in general SPs have clear and onerous obligations to ensure adequate records are kept on all business relationships and occasional transactions entertained (within the parameters set by law), a number of shortcomings have been identified. Although SPs would at times indicate that they would have collected information and documentation on their clients, and carried out the necessary screening and checks, they would not be able to provide any records of such when requested to do so.

In fact, during supervisory examinations, SPs at times made reference to documentation reviewed in the course of a business relationship or in the review of particular transactions, yet failed to keep a copy of the documentation and a record of the actions taken. Other SPs, when updating the clients' customer due diligence documentation, dispose of previously obtained information or documentation.

SPs should also ensure that documentation and information on customers is readily available and easily retrievable. At times however, SPs did not manage to retrieve the information and/or documentation required by the FIAU, or otherwise required much more time than that provided for under the PMLFTR to reply to FIAU requests for information.

Although a rare occurrence, at times SPs were also not able to provide a comprehensive customer list. This is because the customer lists compiled were either not inclusive of all customers, or not inclusive of customer relationships which were terminated in the previous 5 years.

It should be stressed that inadequate record keeping measures may hinder ongoing analysis particularly because SPs would not be able to provide information and documentation, or to provide it in a timely manner.

***Case study (DNFBP)***

*In preparation to the carrying out of a supervisory examination, a Notary was requested to provide a list of all the customers he had offered his services to in the past five (5) years. Yet this SP did not manage to provide a complete list since he did not have one in place.*

---

***Case study Investment Services Company***

*During a visit at an investment services company, it was noted how the SP's record keeping procedures were rudimentary to the extent that the SP did not even manage to submit a complete list of all its customers. The incomplete customer list was identified on noticing that the total number of clients provided on the list was not tallying with the total number of customers indicated in the most recent REQ, and indeed there was a significant discrepancy.*

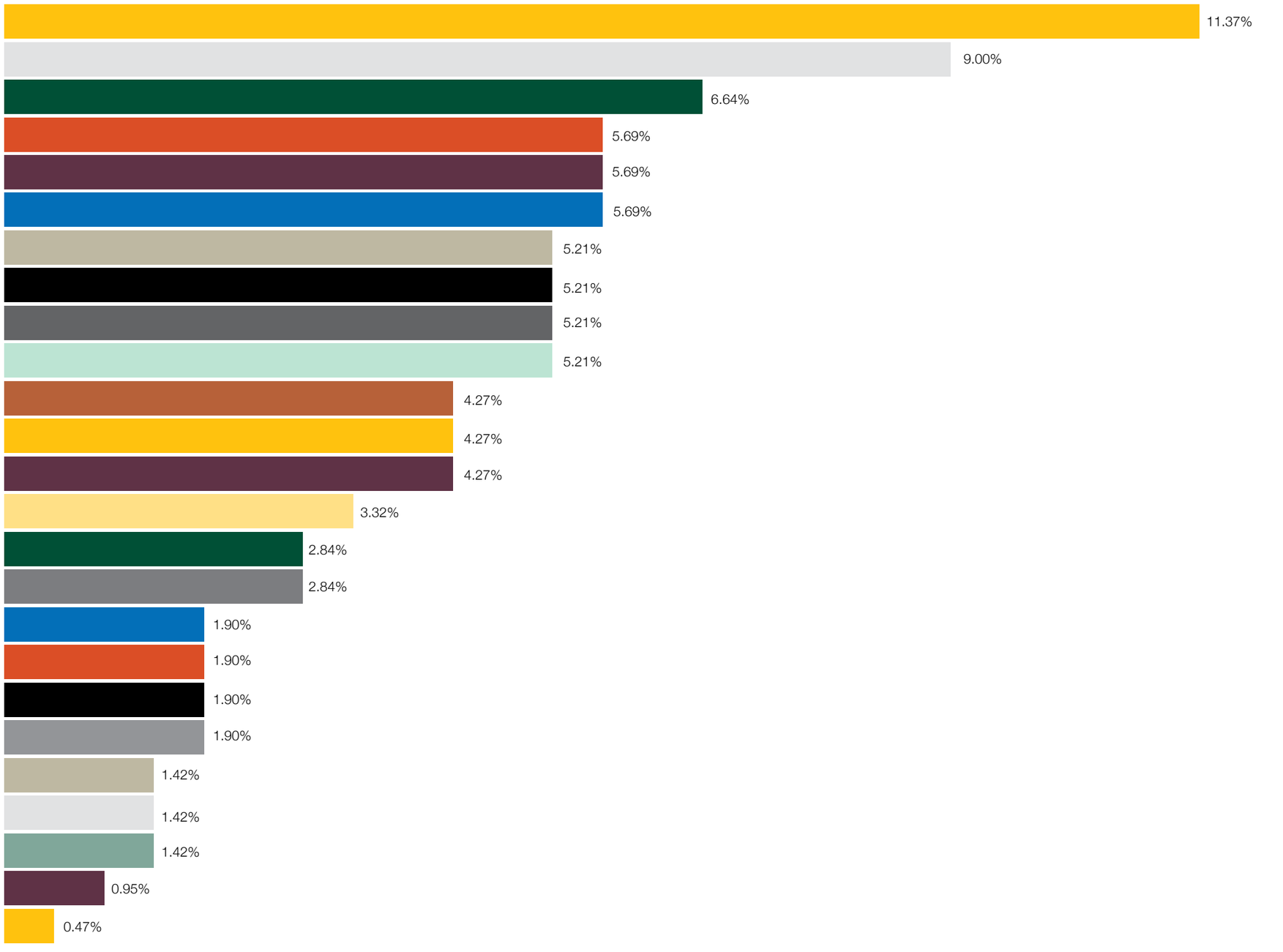
*Furthermore, this same SP also held incomplete transaction data, since copies of such transactional records were not always found on file. It was also noted how the SP did not retain records of any ongoing file reviews.*

# CONCLUDING REMARKS

This paper sheds light on findings and observations that are identified in respect of the more salient AML/CFT obligations outlined in the PMLFTR and the IPs, with the aim of providing insight to subject persons on the types of deficiencies that are being encountered by the FIAU Supervisory Function. Such an exercise is intended to contribute to subject persons' knowledge on the proper implementation of AML/CFT requirements. Indeed, the FIAU is pleased to note that overall it is observing more commitment and investments by subject persons to implement effective AML/CFT procedures. This augurs well in our joint bid to fight money laundering and the financing of terrorism.

# ANNEX 1

Most common findings noted across all sectors in 2020




- Customer Risk Assessment - Inadequate
- CDD - Infringements on obtaining information on the purpose and intended nature of the business relationship
- EDD not carried out/Inadequately performed
- Policies, controls and procedures not in place /not adequate
- CDD - Infringements on the verification of the customer
- Measures to determine whether customer/BO is a PEP not applied
- CDD - Infringements on conducting ongoing monitoring of the business relationship - scrutiny of transactions
- Failure to carry out jurisdiction risk assessment/inadequate
- Business Risk Assessment - Not Performed
- Business Risk Assessment - Inadequate
- Record-keeping infringements
- CDD - Infringements on the verification of the BO
- CDD - Infringements on the identification of the BO
- CDD - Infringement on the identification of the customer
- CDD - Infringements on conducting ongoing monitoring of the business relationship - documents, data and information not up-to-date
- CDD - Performed late
- Failure to carry out adequate certification to verification documentation
- MLRO - related infringements including restricted access to relevant information
- CDD - Infringements on the residential address of the customer/BO
- Customer Risk Assessment - Not Performed
- Failure to submit an STR
- CDD - Infringements on the identification/verification of person acting on behalf of a customer
- Failure to take appropriate and proportionate measures in relation to awareness and training and/or vetting of employees
- CDD - Authorisation in writing from customer for person to act on behalf of customer not available
- Failure to carry out/incomplete assessment carried out on third parties for which reliance is placed on

# ANNEX 2

Most common breaches noted in the financial sector in 2020

**12.12%**

**CDD -** Infringements on obtaining information on the purpose and intended nature of the business relationship

**12.12%**

**CRA Inadequate**

**9.09%**

**CDD** - Infringements on the verification of the customer

**9.09%**

**Business risk assessment not adequate**

**9.09%**

**CDD** - Infringements on conducting ongoing monitoring of the business relationship - scrutiny of transactions

**7.58%**

**CDD** - Infringements on the identification of the customer

**7.58%**

**Failure to carry out appropriate Enhanced Due Diligence measures**

**4.55%**

**CDD** - Infringements on the residential address of the customer/BO

**4.55%**

**CDD** - Infringements relating to certification

**3.03%**

**CDD** - Infringements on conducting ongoing monitoring of the business relationship - documents, data and information not up to date

**3.03%**

**CDD** - Infringements on the identification of the BO

**3.03%**

**CDD** - Infringements on the verification of the BO

**3.03%**

**Failure to carry out jurisdiction risk assessment**

**3.03%**

**CDD** - Performed late

**3.03%**

**Record Keeping Failures**

**1.52%**

**CDD** - Infringements on the identification of person acting on behalf of a customer

**1.52%**

**Failure to carry out/incomplete assessment carried out on third parties for which reliance is placed on**

**1.52%**

**Inadequate adherence to Reporting Obligations**

**1.52%**

**Measures to determine whether customer/BO is a PEP not applied**

# ANNEX 3

Most common breaches noted in the non-financial sector in 2020

**11.36%**

**Customer risk assessment** - Inadequate

**7.58%**

**Business risk assessment** - Not Performed

**7.58%**

**Measures to determine whether customer/BO is a PEP not applied**

**6.82%**

**Failure to carry out jurisdiction risk assessment/inadequate**

**6.06%**

**CDD** - Infringements on obtaining information on the purpose and intended nature of the business relationship

**6.06%**

**Policies, controls and procedures not in place/not adequate**

**6.06%**

**EDD not carried out in relation to customers determined by the SP as presenting high ML/FT risks/Inadequate EDD applied**

**5.30%**

**CDD** - Infringements on the identification of the BO

**5.30%**

**CDD** - Infringements on the verification of the BO

**4.55%**

**CDD** - Infringement on the verification of the customer

**3.03%**

**Customer risk assessment** - Not performed

**3.03%**

**Business risk assessment -** Inadequate

**3.03%**

**CDD** - Performed late

**3.03%**

**Record-keeping infringements**

**3.03%**

**CDD** - Infringements on conducting ongoing monitoring of the business relationship - scrutiny of transactions

**3.03%**

**CDD** - Infringements on conducting ongoing monitoring of the business relationship - documents, data and information not up-to-date

**2.27%**

**MLRO - related infringements including restricted access to relevant information**

**2.27%**

**Failure to take appropriate and proportionate measures in relation to awareness and training and/or vetting of employees**

**1.52%**

**CDD** - Infringements on the identification of the customer

**1.52%**

**CDD** - Authorisation in writing from customer for person to act on behalf of customer not available

**1.52%**

**CDD** - Infringements on the identification/verification of person acting on behalf of a customer

**1.52%**

**Failure to submit an STR**

**1.52%**

**CDD** - Infringements on establishing the business and risk profile of the customer

**1.52%**

**Record-keeping Failures**

**0.76%**

**CDD** - Infringement on the residential address of the customer/BO

**0.76%**

Failure to carry out adequate certification to verification documentation

65C, Tower Street,
Birkirkara BKR 4012,
Malta



Questions on this document or on the application of AML/CFT measures may be sent to **queries@fiaumalta.org**

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

**Telephone:** (+356) 21 231 333
**Fax:** (+356) 21 231 090
**E-mail:** info@fiaumalta.org
**Website:** www.fiaumalta.org