ENFORCEMENT FACTSHEET

A Compilation of Regulatory Actions

2021/2022

Published January 2024

Table of Contents

1. Introduction Pg 3

2. Overview of Enforcement Process Pg 4

3. Overview of the most common breaches identified in 2021 and 2022 Pg 6

4. Purpose and Intended Nature of the Business Relationship Pg7

5. Enhanced Due Diligence Pg 9

6. Ongoing Monitoring – Transaction Monitoring Pg 12

7. Reporting Pg 15

7.1 Internal Reporting Pg 16

7.2 External Reporting Pg 17

8. BO related breaches Pg 21

8.1 Identification and Verification of the Identity of the BO Pg 23

8.2 The ownership and control structure Pg 24

8.3 Reporting Pg 26

9. Concluding Remarks Pg 29

Introduction

The Financial Intelligence Analysis Unit (FIAU) has been continuously working towards ensuring that the fight against money laundering and funding of terrorism (ML/FT) is effective by ensuring that subject persons (SPs) are compliant with their anti-money laundering and counter financing of terrorism (AML/CFT) obligations. In doing so, the FIAU through the Compliance Monitoring Committee (CMC) imposes administrative measures which are effective, proportionate, and dissuasive, as per the Financial Action Task Force (FATF) standards. Article 59 of the European Union Directive 2015/849 of 20 May 2015, i.e., the 4th AML Directive, also requires the imposition of administrative sanctions and measures in case of breaches that are serious, repeated, systematic, or which are a combination of these.

This paper focuses on the most serious and material breaches identified by the CMC between the years 2021 and 2022[1]. These are in relation to purpose and intended nature of the business relationship, enhanced due diligence (EDD), transaction monitoring, reporting, and breaches relating to beneficial ownership (including identification and verification and reporting). It aims to guide SPs in the performance of their AML/CFT obligations, whilst ensuring that their ML/FT risks are effectively mitigated. It should be noted that other breaches were also identified during the years 2021 and 2022, however, these are not included in this Factsheet. For further details on breaches identified, please refer to the publications and key takeaways issued on the FIAU website.

The years 2021 and 2022 were characterised by the FATF's decision to place Malta on the list of jurisdictions under increased monitoring (or as commonly known the "grey list"). The basis for this decision was that three recommended actions out of a total of fifty-eight set out in Malta's Mutual Evaluation Report were not fully addressed.

These related to the identification of accurate beneficial ownership (BO) information; the imposition of effective, proportionate, and dissuasive sanctions in cases of non-compliance with beneficial ownership obligations; and the need for increased focus of FIAU intelligence analysis on serious tax offences and related ML together with the enhanced use of FIAU intelligence in support of the detection and investigation of these offences.

In line with the action plan submitted by Malta to the FATF, apart from its regular supervisory cycle, the FIAU also performed targeted and thematic examinations to assess SPs adherence to BO obligations. While the FIAU has and will always follow due process in its supervisory and enforcement function, there was an increase in the administrative measures taken for BO breaches as a result of such focused examinations. However, the enforcement actions taken on SPs for breaches of BO obligations are not synonymous to any material risks in the level of adherence to BO obligations by SPs at large and in the absolute majority of cases these were single events of non-compliance. In this regard, reference is also being made to the 'Compliance with Beneficial Ownership Obligations by Company Service Providers' paper issued by the FIAU on 31 March 2022 which confirms the good level of compliance in BO obligations.

This Factsheet is to be read in conjunction with other guidance notes issued by the FIAU, including the guidance note on Transaction Monitoring ('A Look Through the Obligation of Transaction Monitoring') issued in April 2023 which highlights the SPs' obligation to carry out effective ongoing monitoring and to scrutinise unusual, anomalous, and suspicious transactions. Additionally, the Paper should be read in conjunction with any sectoral risk assessments or risk assessments at both national and supranational level and the European Banking Authority's fourth opinion on the ML/FT risks affecting the EU's financial sector, amongst other papers and opinions.

1 Although the breaches were identified between 2021 and 2022, the respective compliance examinations and the occurrence of the breach may have taken place before.

Overview of the Enforcement process

Examinations to monitor compliance with AML/CFT obligations are carried out by the FIAU's Supervision Section and/or any of its agents (these being the Malta Financial Services Authority or the Malta Gaming Authority, depending on the sector of the SP under review). Upon the conclusion of an examination, the case at hand is categorised depending on its level of seriousness and materiality, taking into consideration the potential breaches identified, the regard which the SP had to its AML/CFT obligations at the time of the examination, the cooperation shown by the SP, its size and sector. The most serious cases with identified potential breaches of AML/CFT obligations are escalated to the Enforcement Section. Officials within the Enforcement Section present the case before the CMC, which in turn decides on whether any potential breach is a contravention of one's AML/CFT obligations and, where this is the case, on the administrative measure to be imposed. The following procedure is followed:

1. The case is escalated to the Enforcement Section depending on its seriousness and materiality.

2. The case is allocated to an Enforcement Officer who assesses the findings report (Report), containing the potential breaches identified by the Supervision Section, and the representations sent by the SP together with all the evidence available.

3. For examinations carried out on or after January 2022, the SP is also being formally notified of the opportunity to substantiate its written representations orally through a meeting with the members of the CMC.

4. The CMC meeting is held where the case is presented by the Enforcement Section.

5. The CMC decides whether each finding constitutes a breach or otherwise of the SP's AML/CFT obligations. In the case where the CMC determines that the finding constitutes a breach, it also decides on the administrative measure to be imposed in line with the FIAU's Sanctions Policy.

6. The level of seriousness, the impact and the systematic nature or otherwise of each breach are taken into consideration to determine the administrative measure to impose.

7. An administrative measures letter is issued to the SP containing the deliberations and decision of the CMC.

8. A publication with a description of the case and of the administrative measures imposed in terms of Article 13C of the Prevention of Money Laundering Act (PMLA) as well as the FIAU's policies and procedures is made available on the FIAU's website. Administrative measures which do not include any penalties or where the penalties do not exceed EUR50,000 are published anonymously.

9. Where the SP feels aggrieved by the administrative measure imposed, it may appeal the decision before the Court of Appeal (Inferior Jurisdiction). Appeal Notices, and Appeal Decisions will also be explained in the publication.

Fig. 1 – The Enforcement Process

The administrative measures which may be imposed by the CMC include the following:

- Written Reprimand – this is a written warning and is imposed for breaches identified which are of a minor nature.

- Remediation Directive – when this measure is imposed, the SP is expected to bring its operations in line with its AML/CFT obligations. The SP is generally requested to update policies and procedures, as well as to ensure the implementation of the same. Customer profiles may also need to be updated in line with the updating of the policies and procedures. Remediation Directives are generally imposed for less material breaches whilst follow up directives for more material ones.

- Follow-Up Directive – SPs are required to draw up and implement an action plan containing action points and target dates for the completion of each point. The SP is expected to ensure that the remedial measures indicated in the action plan are implemented. Meetings are held with the SP on a periodic basis, depending on the extent of the directive and the seriousness of the failures determined. System walkthroughs, employee interviews and a sample of customer profiles for review are usually the means employed by the Enforcement Section to attest the implementation of the action plan.

- Administrative penalty – The FIAU may also impose administrative penalties for breaches of AML/CFT obligations. Any penalty must be commensurate to the seriousness of the case, as well as the nature of the SP.

    (a) Minor breaches can result in an administrative penalty of €250 up to €1,000. The FIAU may alternatively issue a reprimand in writing.

    (b) On the other hand, a breach that is neither minor nor serious, repeated, or systematic can result in an administrative penalty per breach of not less than €1,000 but not more than €46,500.

    (c) Serious, repeated or systematic breaches are subject to the highest amounts in terms of administrative penalties. For SPs carrying out relevant financial business, depending on the nature of the breach, its impact and any systemic concerns, administrative penalties per breach may reach as much as €5 million or where this is not considered enough given the nature of the case, 10% of the SP's annual turnover, after considering the latest approved financial statements of the company. In cases of SPs carrying out relevant activity, the administrative penalty may not exceed €1 million or not more than twice the benefit derived from the contravention, where this amount may be quantified.

    (d) The CMC may also impose a penalty on a natural person who at the time of the contravention was a director or officer tasked with the responsibility for the management of the legal person or was purporting to act in this capacity, if such individual is found to have contributed to a breach committed by the SP either wilfully or through gross negligence. The Committee commits itself to ensuring the most rigorous approach in the determination of such acts by any individual and ensures that the necessary evidence is at its disposal before it decides that any individual has contributed to the breaches determined.

Overview of the most common breaches identified in 2021 and 2022

An overview of the administrative penalties imposed during 2021 and 2022 for each particular breach is being delineated hereunder.

Year		2021		2022		Total
High Level Breaches	**No. of cases**	**Penalty**	**No. of cases**	**Penalty**	**No. of cases**	**Penalty**
Ongoing Monitoring / Transaction Monitoring	13	€ 3,669,998	16	€ 911,481	29	€ 4,581,479
Identification and Verification	19	€ 2,699,196	19	€ 23,108	38	€ 2,722,304
Purpose and Intended Nature of the Business Relationship	14	€ 2,002,001	19	€ 612,356	33	€ 2,614,357
Reporting	6	€ 1,304,649	11	€ 279,544	17	€ 1,584,193
Customer Risk Assessment	17	€ 454,222	20	€ 459,586	37	€ 913,808
Enhanced Due Diligence	12	€ 627,995	8	€ 167,926	20	€ 795,921
Business Risk Assessment	17	€ 440,574	15	€ 305,126	32	€ 745,700
Money Laundering Reporting Officer	6	€ 233,514	4	€ 62,857	10	€ 296,371
Record Keeping	5	€ 163,103	2	€ 5,000	7	€ 168,103
Politically Exposed Persons	6	€ 70,184	5	€ 90,232	11	€ 160,416
Policies	8	€ 102,204	6	€ 24,418	14	€ 126,622
Breach of Directive	2	€ 37,525	1	€ 0	3	€ 37,525
Breach of Monitoring Order	1	€ 18,000	0		1	€ 18,000
Ongoing Monitoring / Updating of Docs	0	€ 0	2	€ 2,139	2	€ 2,139
Certification	0	€ 0	1	€ 0	1	€ 0
Jurisdiction Risk Assessment	2	€ 0	1	€ 0	3	€ 0
Outsourcing		€ 0	0	€ 0	1	€ 0
Reliance	0	€ 0	2	€ 0	2	€ 0
Screening	0	€ 0	2	€ 0	2	€ 0
Training	2	€ 0	3	€ 0	5	€ 0
Total	29	€ 11,823,165	33	€ 2,943,773	62	€ 14,766,938

Table 1- Statistical data regarding the most common breaches

Purpose and Intended Nature of the Business Relationship

Regulation 7(1)(c) of the PMLFTR obliges SPs to assess and, as appropriate, obtain information on the purpose and intended nature of the business relationship and establish the business and risk profile of the customer. This involves a clear understanding of the customer's motives behind requesting a product or service, as well as the funding sources used. By gaining insight into the sources of a customer's funds, SPs can effectively construct a thorough business and risk profile. This, in turn, empowers SPs to diligently monitor the business relationship, ensuring that the customer's activities align with the established business and risk profile.

During 2021 and 2022 a total of 33 breaches were identified in regard to this obligation. The primary deficiencies were associated with the failure to establish a comprehensive business and risk profile of the customer. Specifically, it was noted that, at times, inadequate information and/or documentation to understand the customers' source of wealth was gathered. In most cases, whilst information was collected by the SP on its customers' source of wealth (such as the business/industry of the customer and expected source of funds), the information was deemed to be too generic and vague. Therefore, the customer's risk profile was incomplete and the SP's ability to scrutinise transactions effectively was jeopardised.

Another common breach observed was the failure to collect details on the anticipated level and nature of activity that is to be undertaken throughout the business relationship. While understanding that this information may be difficult to obtain at account opening stage for some sectors, such as is the case for investment services and gaming activities, it is important to obtain information that can assist in establishing the extent of the level of activity to expect. At least obtaining information about the employment and investment/gaming prospects will help in determining the possible level of activity to expect, which will aid in monitoring the actual activity being carried out by customers. Equally important is to revise and better calibrate these brackets from time to time considering the overall transactional activity carried out by a SP's customers. Indeed, in some occasions it was observed that the income/transactional activity brackets were considered too wide, thus limiting the SP from having visibility of more precise amounts which the customer would be transacting throughout the business relationship.

Case Study (Collective Investment Schemes)

The information obtained in relation to the purpose and intended nature of the business relationship for the client profiles assessed during the compliance examination was insufficient. This included lack of information on the anticipated level and nature of activity to be undertaken during the business relationship, and lack of information on the source of wealth and expected source of funds of the customers. While comprehending that most often customers would fund their operations through their income, understanding the customer's employment is indispensable. For this reason, reference to "funding through income from employment in engineering" or "funding through self-owned business" cannot be considered as detailed enough to understand from where the customer would fund its operations. Regarding the anticipated level and nature of the activity, the Committee noted that whilst investment prospects may be unavailable at the initial stages of a business relationship, the Company should still seek to understand one's investment appetite. It was also observed that the Company's policies and procedures lacked the necessary detail to ensure that the required information and documentation is obtained from its customers on a risk-sensitive basis. In view of this, the Company could not build a comprehensive business and risk profile on its customers, which would in turn allow the Company to carry out adequate ongoing monitoring.

Case Study (Financial Institution)

During the compliance examination it was noted that no information was collected by the SP on the anticipated level and nature of transactions at onboarding stage for circa 53% of the customers reviewed. While this could be indirectly covered through obtaining details of the customer's employment/ business, this was also found to be deficient. Indeed, an inadequate form was being used by the SP for customers who were natural persons, and this since it did not cover the customer's areas of business activity. In fact, the SP either did not collect any information at all on the nature and details of the customer's occupation or employment or alternatively collected information that was so generic in nature that it held little value to understand the customer's business profile. Furthermore, notwithstanding the fact that the customer onboarding form used for corporate customers included a section covering the customers' area of business, some issues relating to inadequate information were still identified. For example, in respect of one customer reviewed, although the primary business activity was indicated as 'Business Consultancy' and the second business activity as 'IT Consultancy', open-source checks conducted by FIAU officials revealed that the customer in question provided legal advice on passport acquisition through investment. Therefore, the information collected by the Company was too generic and did not describe the nature of the consultancy provided adequately.

Case Study (Credit Institution)

No source of wealth information/documentation was collected by the SP for a number of profiles, whilst no expected source of funds information was obtained for a number of others. Moreover, there were other circumstances where the source of wealth and expected source of funds information was too generic. For example, the source of wealth for two customers was listed as 'salary (savings)' and 'income' respectively, with no further information from where the income and salary originated. The source of funds listed was equally generic. The Committee concluded that the information provided was not sufficient and failed to provide any reassurance that the funds used within the business relationship were indeed understood by the Bank, thus prejudicing effective monitoring of the business relationship.

Enhanced Due Diligence

Regulation 11 of the PMLFTR delineates situations necessitating enhanced customer due diligence. In cases where a heightened risk of ML/FT is identified, corresponding measures may involve the collection of additional documentation, as well as the enhanced scrutiny of transactions. SPs may need to apply these enhanced measures at any point of the business relationship, be it at onboarding or throughout the business relationship. Some EDD measures are prescribed by law such as those relating to the servicing of PEPs or entering into correspondent business relationships, while others are to be applied at the discretion of the SP depending on the risks identified. In all circumstances, understanding the extent of the risk faced by the established business relationship or the occasional transaction carried out is essential to determine the appropriate mitigating measures to implement. Circumstances where the risks emanate from exposures to corruption, adversely known customers or links to high-risk businesses most often will require enhanced customer profiling by obtaining documentation to prove the customer's source of wealth, as well as heightened levels of scrutiny of the relationship and the transactions entertained.

A total of 20 breaches related to EDD were identified between 2021 and 2022. Some shortcomings related to the failure to establish adequate EDD policies and procedures, which subsequently led to no or ineffective EDD measures being carried out. Other shortcomings identified related to the failure to carry out EDD measures despite establishing that there were high-risk elements in the relationship that required the carrying out of EDD. While one single element does not necessarily lead to a high-risk situation that requires EDD, SPs should be careful in considering the risks and level of due diligence carried out when dealing with high-risk jurisdictions, cash intensive businesses, the usage of products or services which facilitate anonymity, activity conducted through a complex structure for which there does not seem to be a legitimate explanation or where the activity is associated with a higher risk of corruption.

Case Study (Financial Institution)

The Company failed to have in place adequate EDD procedures defining the EDD measures to be applied depending on the heightened ML/FT risk exposure identified. The policies and procedures did not provide details for Company officials to understand when to request additional CDD information/ documentation or when to apply enhanced scrutiny but rather only generically referred to the need to apply enhanced measures for high risk situations. The issues identified in the procedures were reflected in the profiles reviewed as part of the sample. In one particular profile, the customer was a national of a country which at the time of the examination was on the FATF list of jurisdictions under increased monitoring. The customer was also sending large values of funds to higher-risk jurisdictions. EDD measures applied by the Bank consisted of calls held with the customer, and copies of a bill pertaining to a credit card utilised by the same. However, these could not be considered as adequate EDD measures and were not sufficient to mitigate the risks of the customer.

Case Study (Financial Institution)

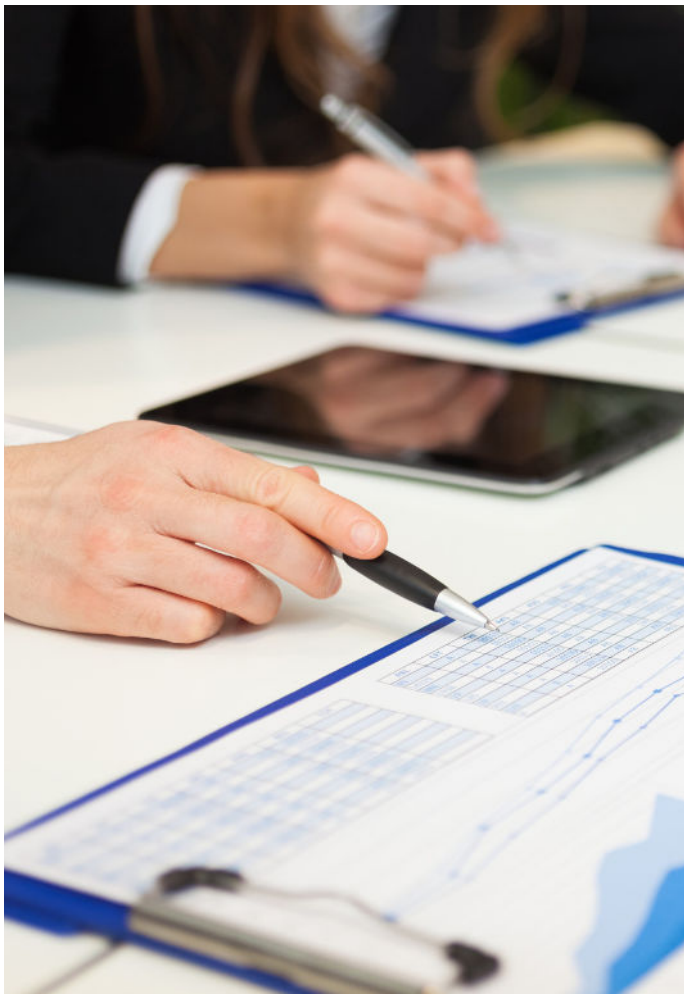
The Company had a comprehensive CRA measure in place that identified instances of heightened risk requiring the application of EDD. However, for some instances the Company failed to act on such identified risks and to apply the necessary controls to manage the same. An example is relayed hereunder:

Case 1 – The customer in question operated in the gaming sector (but had an account for the company's own operations and not to process gaming activity) and had an annual transaction limit of over €250,000 with average transactions being processed indicated as ranging between €5,001 and €50,000. The ownership structure involved a fiduciary company holding shares on behalf of the BO. This kind of structure allows the customer or the BO to remain anonymous and/or facilitates hiding their identity, increasing the risk of ML/FT. The customer was also adversely known in view of adverse information linking it to criminal activity in Italy. All these elements should have prompted the Company to perform EDD, both to obtain a comprehensive understanding of the customer's source of wealth as well as to scrutinise the transactions undertaken through the relationships.

Case Study (Financial Institution)

The Company failed to carry out EDD measures for circa 33% of the customers reviewed during the examination. An example of this failure is found below:

Case 1 – The customer in question was attributed an overall medium-high risk rating because of the high-risk business related to virtual currencies. While the company stated that it had carried out enhanced transaction scrutiny, it was found to be ineffective. Factors such as the values of the transactions, their frequency, and the jurisdictions from which they were originating or to which they were directed, were not being considered. Besides, the transaction scrutiny was always being carried out after the transactions were effected. While not all transactions need to be scrutinised before they take place, high risk and unusual transactions should be scrutinised before they are allowed to pass through the customer's accounts. It was also noted that the customer had indicated in its Application Form that it was operating in the information technology industry, with its source of wealth originating from 'trading income from sale of services/goods' and the expected source of funds being that of 'receiving direct deposits from customers'. The source of wealth and expected source of funds information retained by the Company was lacking in detail and thus insufficient to constitute EDD, especially when considering the high-risk business of the customer. In fact, as per the FATF report entitled 'Virtual Currencies Key Definitions and Potential AML/CFT Risks' issued in June 2014, virtual currencies were deemed to present a high risk of ML/FT. The Company was therefore expected to obtain further information and documentation substantiating the information provided.



Case Study (Credit Institution)

During the compliance examination, it was noted that EDD measures were either not applied or else deemed inadequate. An example may be found below:

Case 1 – The customer was assigned a high-risk score because of his connections with a jurisdiction which the SP considered as high risk. The connection to this jurisdiction warranted the application of appropriate EDD measures due the country's known connection with cash and corruption. Notwithstanding this, the SP failed to obtain additional information on the customer and its nexus to Malta, as well as about the intended nature of the business relationship. Questions should have been asked as to why a customer residing in this jurisdiction was seeking to open a term-deposit account in Malta, therefore additional documentation should have been obtained to assess the customer's source of wealth. Moreover, the Bank also failed to better understand the expected source of funds to be used in the relationship, i.e., family savings and collect related documentation.

Carrying out effective EDD measures aimed at effectively mitigating and managing the enhanced risks perceived in the specific relationship or transaction entertained, is still a recurrent issue that SPs need to consider carefully. While aware that risks are being better understood by SPs, the efficacy of these assessments is subject to the controls being implemented. While envisaging that this is being covered through the introduction of more robust transaction monitoring measures, SPs need to ensure that where warranted, measures are in place to also have an extensive understanding of the customer's profile, as this determines the extent of the effectiveness of the transaction monitoring implemented.

Ongoing Monitoring – Transaction Monitoring

Regulation 7(1)(d) of the PMLFTR explicitly refers to the obligation to conduct ongoing monitoring of a business relationship. Regulation 7(2)(a) of the PMLFTR then proceeds to explain that this ongoing monitoring shall consist in:

(a) The scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions are in line with the customer's business and risk profile. Moreover, the scrutiny of transactions will aid the SP in detecting any anomalous or unusual transactions. When a transaction is deemed to be suspicious, the SP is then obliged to submit a suspicious report to the FIAU; and

(b) Ensuring that the documents, data, or information held by the SP are reviewed and kept up to date.

Reference must here be made to the FIAU's Guidance Note entitled, 'A Look Through the Obligation of Transaction Monitoring' issued in April 2023, wherein SPs can find a detailed overview of how effective and efficient transaction monitoring should be conducted. SPs are to keep in mind that whilst having an automated system in place is not an absolute requirement, this depends on the size of the SP, the complexity of the business model, the risk appetite of the SP, and the number of transactions executed daily. The Guidance Note also delves deeper into this, as well as pre-transaction monitoring. While this Guidance Note mainly targets institutions which process payments and similar transactions for and on behalf of customers, it provides invaluable guidance on the obligation to monitor transactions that is equally beneficial to all SPs.

A total of 29 breaches were identified in relation to transaction monitoring between 2021 and 2022. The main deficiencies identified related to ineffective transaction monitoring being undertaken by SPs which resulted in systemic failures of such obligations. There were also instances where although monitoring was carried out, the transactions were neither effectively scrutinised nor understood, resulting at times in the processing of transactions the source of which could not be explained.

Case Study (Credit Institution)

The Bank failed to scrutinise several transactions or otherwise, the scrutiny performed was inadequate.

One particular customer received funds through a series of transactions for which the Bank did not deem it necessary to obtain further information or documentation to scrutinise the same. There were five total remitters effecting transactions in favour of the customer, which transactions totalled to amounts ranging from circa USD 2million - 3.8 million for each remitter. These transactions were all received by the customer in a span of 18 months.

The Committee in this regard noted that SPs should be cautious when processing complex and large value transactions and care should be given to understanding their economic and lawful purpose. Nonetheless, for example for the transactions performed by one of the remitters, the only information held by the Bank was that the remitter was in the same line of business as the customer, without understanding the connection of the parties, and the purpose for the inward remittances.

In other files, several internal transfers were noted which at times reached millions of Euros . Whilst the Bank provided inter-company loan agreements, the Committee held its reservations on the same in view of the fact that there was no purpose behind the loan; the repayment terms were very short; and there were no interest fees to be paid. This raised serious questions on the legitimacy of the loans. The mere fact that companies would be related through common ownership or because they form part of the same group is not a justification for allowing funds to process freely between them. There still has to be a valid and justified rationale for the transactions being undertaken. As a minimum, understanding the purpose of the funds being transferred and establishing an economic rationale is crucial to avoid risks of funds being layered through such inter-company transfers.

Case Study (Remote Gaming Operator)

During the examination, Officials identified shortcomings revolving around discrepancies between the deposits made by players and the information held by the Company. Examples of this are being relayed hereunder:

Case 1 – As per documentation collected by the Company, the customer seemed to be earning €2,000 per month. Notwithstanding this, the player deposited a total of €58,000 in the span of eight months. Deposits made in two specific months amounted to over €7,000 and €10,000 respectively. Despite the incongruence in the amounts deposited and income, the Company failed to collect further information explaining the transactions.

Case 2 – The business relationship in question commenced in March 2019. A screenshot of an investment portfolio dated December 2019 was obtained as source of wealth information, showing an amount of approximately €50,000. Notwithstanding this, the player's total deposits amounted to over €120,000 with the withdrawals amounting around €118,000. More specifically, in one particular month, the player deposited circa €19,000 and withdrew approximately €10,000. Although the Company did indeed obtain some form of source of wealth information, this was not sufficient and this since the deposits being transacted exceeded the amount covered by the investment portfolio. Furthermore, upon a closer analysis of this investment portfolio, it was discovered that the balance was not of €50,000, but rather of only €20. Moreover, the Company failed to enquire information pertaining to the player's employment. In view of this information, the Company was expected to collect more information and documentation in order to understand whether the source of wealth and source of funds of the player were originating from legitimate sources.

Case Study (Remote Gaming Operator)

The SP's Procedures Document stated that the Company's MLRO is to continuously monitor any changes in the client's financial status, business activities and type of transactions. No automated system was in place to assist the MLRO. However, this control was being ineffectively implemented in practice particularly since the voluminous transactions being processed, without any automated checks being undertaken, made it humanly impossible for the MLRO and any other staff to be monitoring what transactions which were being processed and which ones should be flagged for review. In fact, in one of a number of examples, the SP failed to detect that there was one player making use of several accounts under different domains. This would be a key control within the remote gaming sector to ensure that the €2,000 threshold is not circumvented and that there is a proper oversight and understanding of a player's activity. Therefore, the system and checks which were conducted manually were deemed ineffective.

Case Study (Land Based Casino)

The Company failed to obtain sufficient level of information when compiling its customers' business and risk profiles. Due to this, the Company was unable to conduct adequate transaction scrutiny. However, even in the absence of the information necessary to build a good customer profile, the gaming history of a customer and the gaming patterns could still shed light of instances that require specific attention. For example, consideration of the level of drops, wins and losses provide useful information which may be used to determine those transactions that diverge from the norm and require a review. The Company would then be expected to proceed to ask for further information and documentation from the customers.

One player dropped circa EUR 101,000 and lost circa EUR 90,000 in a period of twenty days and 3 December 2019 in a period of twenty days. In another twenty-five days, the player dropped around EUR 23,000 and lost circa EUR 19,100. The Committee also noted that in almost two years, the player dropped €988,700 and lost €164,735. The Company submitted that the client is a well-known Maltese businessman who is known to have own various local businesses and dealt extensively in real estate. Moreover, it was additionally noted that the player visited that Casino in excess of 300 times. In spite of this, the Company only asked the player to complete an EDD Form circa two years after the date of registration, notwithstanding the high risk elements which were evidently present. The fact that the customer was a well-known businessman, was not a justification for the failure to query into the customer's source of funds and the transactions processed.

However, even though some deficiencies were noted, it was clear that SPs are committed to enhancing their ability to effectively monitor transactions both on an a-priori and a-posteriori basis, on a risk-sensitive basis. Specifically, when it comes to the banking sector, investment also included the introduction of artificial intelligence, aimed at not only capturing anomalous and unusual transactions but to utilise transaction data to adapt the checks being carried out with a view to increasing the level of effective monitoring being carried out.

Reporting

As per Regulation 15(3) of the PMLFTR, SPs are obliged to report to the FIAU any knowledge or suspicion they may have that either funds are the proceeds of criminal activity or are otherwise to be used to finance terrorism, or that a person was, is or may be involved in ML/FT. This obligation applies also in relation to attempted transactions and any such report has to be filed promptly[2]. The said obligation links with the obligation under Regulation 15(1) of the PMLFTR for SPs to have internal reporting procedures.

The most salient breaches relating to these obligations dealt with the failure to submit a suspicious transaction report (STR) or suspicious activity report (SAR), and/or the inadequate adherence to internal reporting obligations. A total of 17 breaches related to reporting were identified between 2021 and 2022. What follows are some examples of these breaches. It is to be noted that some of these breaches related to the failure to report suspicions arising from the possible concealment of BOs. However, these will be dealt with later in this Factsheet, in the section specifically catering for BO related breaches.

2 This depends on the timeframe of the case in question. As per Legal Notice 214 of 2020, the PMLFTR was amended so that SPs were obliged to report promptly. Prior to this, the Regulation used to state that the report was to be made "as soon as is reasonably practicable, but not later than five working days from when facts are discovered, or information obtained". However, regard should also be had to what is provided in the IPs Part I which provide a clearer indication as to when the reporting obligation to the FIAU is actually triggered.

Internal Reporting

SPs are to have clear policies highlighting the steps that their officers or employees are to take when they become aware of any information that may give rise to knowledge or suspicion that a person or a transaction is linked to ML/FT. Officials of the SP are to treat any suspicion with urgency and report the matter to the MLRO without any delay by the next working day[3].

Case study (Financial Institution)

Two transactions, amounting to €2,000,000 and €1,300,000, supported by two 'Gentleman's Agreements' were processed by the SP. The agreements failed to provide sufficient information justifying why these amounts were being paid. This, together with the adverse media surrounding one of the customers involved, should have been enough for an internal report to be filed. Only once an internal report had been filed could the MLRO review it and decide whether there were enough indications to suspect if there is a link to ML/FT and that an external report had to be submitted to the FIAU.

Case Study (Remote Gaming Operator)

The Company had received correspondence from the Cybercrime Unit of an EU Country about one of the customers the Company was servicing. The customer was depositing funds through stolen credit cards. In view of this, the Cybercrime Unit of the EU Country requested the Company to terminate the business relationship with the customer. While the relationship was terminated, the case was not escalated to the MLRO to consider whether an STR needed to be filed with the FIAU.

3 Once again, this depends on the timeframe of the case in question. Prior to the 2020 IPs, officials of the SP were to report any suspicion to the MLRO without any delay. The 2020 IPs provided more clarity to this and added that officials are expected to escalated matters to the MLRO by the next working day.

External Reporting

Upon considering the contents of an internal report, as well as any documentation attached with the report, if the MLRO concludes that there is knowledge, suspicion, or has reasonable grounds to suspect that:

(a) A transaction may be linked to ML/FT.
(b) A person may have been, is or may be linked with ML/FT.
(c) ML/FT has been, is being, or may be committed or attempted.

The MLRO is to file an STR with the FIAU on the same day when he becomes aware of such knowledge or suspicion of ML/FT.

Case Study (Credit Institution)

The Bank failed to submit a number of STRs to the FIAU, despite evident suspicious behaviour by its customer. An example of this is set out below:

Case 1 – The customer was receiving several low value transactions from different sources. The funds received were then being transferred to two individuals who were nationals of a jurisdiction close to areas where terrorists are active and through which terrorists may transit. These transactions were not flagged or scrutinised, as they did not reach the thresholds put in place by the credit institution for monitoring purposes. No STRs were submitted by the Bank despite the terrorism financing risks which arose, especially due to the pattern of transactions and the fact that the funds were flowing to a jurisdiction in proximity of areas where terrorists are active. It could not be argued that there was no suspicion of FT just on the basis that the funds originated from low-risk jurisdictions or that the individuals to whom the funds were being transferred were nationals of reputable jurisdictions on whom there was no adverse information known. Indeed, FT was not something that was being considered by the Bank as in its representations it only made reference to ML risks.

Case Study (Credit Institution)

One of the customers (Customer A) of the credit institution received a total amount of circa EUR 4.9million from two other customers of the Bank (Customer B and Customer C) on the same date. Four days after the receipt of this money, Customer A lent a total of EUR 4.9million to another Bank customer (Customer D).

An additional AED 43million were transferred from Customer A to Customer D on the same day when these amounts were received from Customers B and C. All Customers had the same BO.

A loan agreement was obtained by the SP between Customer A and Customer D. This was obtained more than two years after the outward transfers occurred. The loan agreement provided for the granting of a loan of EUR 20 million was intended to facilitate the acquisition of a property. Whilst there was an indication for interest to be paid, there was no evidence to suggest that these payments were being made. The money received from this loan by Customer D was eventually used as collateral for another loan granted by the Bank itself of over EUR15million for the purchase of this same property.

Despite the large amounts processed by the Bank and the granting of this loan, no supporting documentation was ever requested by the Bank to demonstrate that this property had actually been bought in practice.

When taking into consideration the facts pertaining to all these customers, the flow of funds and the velocity of the same, the lack of evidence of interest being paid, and the transfer of amounts for the payment of a loan when the Bank was eventually requested to grant a loan to finance the same acquisition, should have led the Bank to submit an STR.

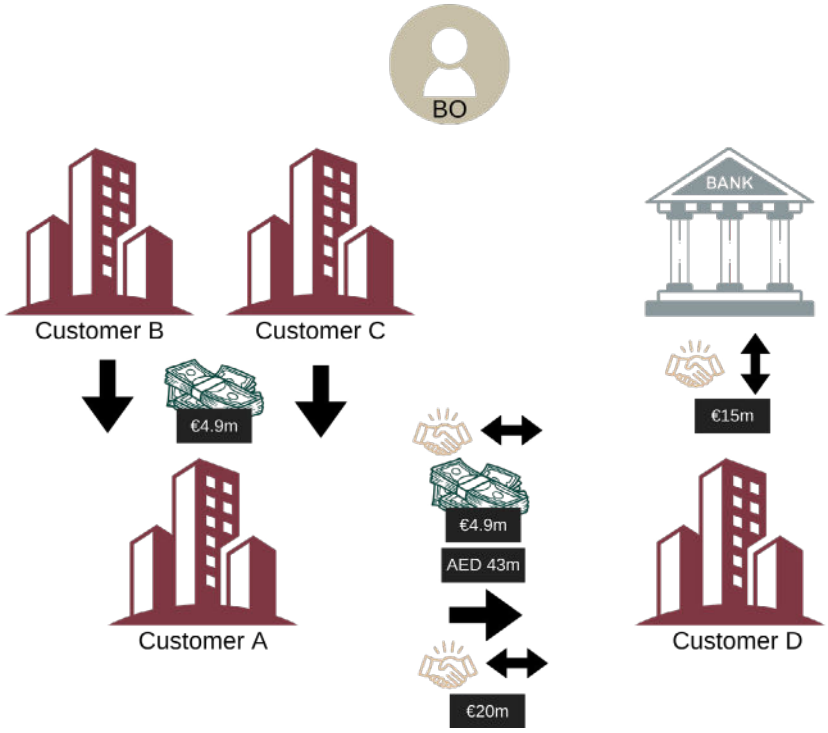


Fig. 2 – Summary of the above case study

Case Study (Company Service Provider)

In 2012, Company Y (BVI company), through a Swiss intermediary, requested the SP to provide directorship services to a newly established company (Company X, a Maltese company). Up to 2020, shares of Company X (the Maltese company) were held in fiduciary capacity by another SP on behalf of Company Y (the BVI company) who was in turn owned by a Russian BO. At this stage, the SP should have questioned why a Swiss intermediary was used by a BVI company (Company Y) to incorporate a Maltese company as a holding company. Moreover, Company X (the Maltese company) then instructed a Dutch entity to incorporate a Dutch company (Company S). Company X wanted to use Company S (the Dutch company) to invest its assets in it.

It was noted that loans were being taken and assigned between Companies Y (BVI company), X (Malta company), S (Dutch Company) and another Cypriot company (Company N), all belonging to the same Russian BO with no evidence as to the purpose of the loans and with no clear rationale as to the assignment of such loans.

Red Flags in relation to these transactions which should have led the SP to report:

- The SP failed to understand the reason as to why Company S (Dutch company), after only 6 months of being incorporated required such a significant loan of $5million from Company N (Cypriot company) to settle the amount owed to its suppliers and for other expenses incurred throughout its business operations.

- The SP held insufficient information on its customer to justify the subsidiary's (Company S) (being the only investment of the customer company) $5million in expenses in such a relatively short period of time. Hence, the SP was required to clearly understand the operations undertaken by the Dutch company.

- The SP was aware that in December 2014, Company X (Malta company) agreed to take on the entire debt due by Company S (Dutch company) to Company N (Cypriot company). Yet, the SP failed to scrutinise the rationale behind the assignment of the loan and the rationale behind its transfer to different interrelated entities. The only notable connection was that of common ownership, however this is not a justification for creating loans, re-assigning them, and transferring same without a justifiable rationale.

- The SP failed to obtain explanations/documentation required to ascertain that such an exponential investment on Company S (Dutch company) made economic sense. In this scenario, the SP was expected to have sufficient reassurance that this

investment was in line with the valued business prospects of Company S. Yet, the SP merely relied on the vague statement that the activity of the Dutch subsidiary was to 'incorporate, manage and supervise businesses'. Furthermore, the SP failed to acquire further details on the services to be undertaken by it, without scrutinising whether it would make economic sense for Company X's involvement.

- In 2018, Company X (Malta company) assigned the debt it took over from Company S (Dutch company) (thus the amount owed by Company X to Company N), to Company Y (BVI company). Here again, the SP failed to query why the debt was once again transferred onto another company owned by the same Russian BO. Yet another red flag in this case study related to a loan between Company Y and Company S. The SP failed to look into this despite being directors of Company X (the Maltese company), they only became involved once the loan became directly relevant to Company X. Since Company X, as a holding company, had direct links with the rest of the companies, the purpose of the transactions being undertaken should have been of crucial importance to the SP. Furthermore, issues surrounding the collection of CDD documents of the Russian BO were noted.

- The SP also did not obtain any detail or explanations as to why Company Y owed funds to Company S in December 2019.

- The SP failed to determine the purpose as to why Company S was owed money by Company Y and whether this was due to any services offered by Company S to Company Y.

- FIAU official's concerns were further exacerbated in view of the significance of the amount due which was over €5million. The SP had no idea which services could have been provided by Company S to Company Y and whether these were in line with the significant amount due.

All this information was important due to Company X (the SP's customer) being the holding company for company S. Any activity done by Company S would therefore impact Company X. Understanding the activities of Company S, especially given the amounts involved, was indispensable.

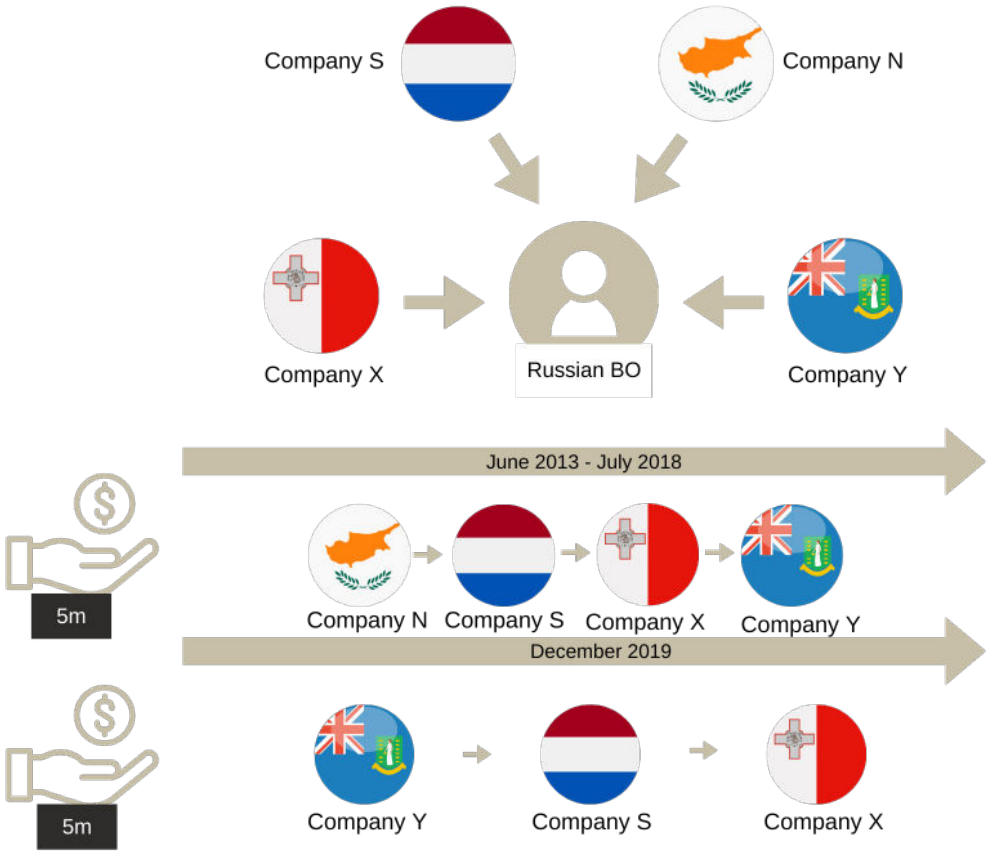


Fig. 3 – Summary of the above case study

Case Study (Trustees and Fiduciaries)

The customer in question was a company which was initially owned by a trust at onboarding. In 2017, a share transfer took place, and individual 1 become its BO. Various adverse media reports were noted in relation to individual 1. These indicated that he was avoiding paying millions of dollars in taxes on art works he had. Moreover, individual 1 was aided by individual 2 to obtain false tax exemption certificates portraying himself to be an art dealer rather than a collector. This helped individual 1 avoid paying sales taxes amounting to over $27 million worth of artwork bought for personal use in the span of five years. In view of this adverse media, which was found through a google search, the Company was obliged to submit a suspicious report to the FIAU, as there was enough reason to suspect that ML or tax evasion could have taken place. Notwithstanding, the Company failed to do so, and was found to be in breach of its reporting obligations.

Reporting is considered as one of the most fundamental AML/CFT obligations. Over the years an increase in reporting by SPs has been noted across different sectors. However, the FIAU always urges SPs to remain vigilant for any suspicious transactions or suspicious behaviour, and to report the same as soon as they are noted or suspected. SPs should ensure that the reports submitted are of good quality and that defensive reporting is, as much as possible, avoided. All lines of defence should always be aware of any emerging risks, trends, and typologies of ML/FT so that reporting of STRs or SARs is performed promptly and effectively.

BO related breaches

Legal persons and arrangements such as companies, trusts, foundations, and partnerships have a myriad of legitimate legal purposes. However, they may also be used in certain complex schemes with the aims of concealing the true owner, the reason behind a transaction undertaken or the assets held by the same legal person or arrangement.

Collecting sufficient information on the BO, the source of the assets of a legal person or legal arrangement and on their respective activities, are all measures which can help in the reduction of the misuse of these vehicles. The lack of adequate and up to date BO information may end up facilitating ML/FT by disguising:

(a) The identity of any known or suspected criminals,
(b) The purpose behind the transactions being undertaken, and/or
(c) The source of the funds being used.

BO information may be concealed through any number of means including the following:

(a) shell companies
(b) complex ownership and control structures
(c) unrestricted use of legal persons as directors
(d) formal nominee shareholders and directors where the nominator is not disclosed
(e) informal nominee shareholders and directors, such as close associates and family.

As per the PMLFTR, the definition of BO is based on a three-tiered test:

1. **Tier 1** – Ownership through direct or indirect means, by holding 25% plus one of the shares, or more than 25% of the voting rights or of the ownership interest in the customer.

2. **Tier 2** – Control through other means. This test is to be applied independently of whether an individual under Tier 1 was identified and may result in the identification of additional BOs where the SP has reason to believe that another person(s) is/are exercising ultimate control over the running of the body corporate or its management through means other than ownership.

3. **Tier 3** – Senior managing officials. If, after having exhausted all possible means, no BO as defined under points (1) and (2) above is identified, the senior managing officials are to be considered as BOs.

It must be clear that even though the above is presented as a 3-tier test, Tier 1 and Tier 2 are not mutually exclusive and it is possible to have situations where one or more BOs is identified under both tiers for the same body corporate. Thus, SPs should consider whether there is anyone otherwise exercising control over the body corporate even where they have already identified one or more BOs under the Tier 1 test.

For senior management officials to be considered as BOs, two cumulative conditions have to be met, i.e. (i) all possible means to identify a BO must have been exhausted; and (ii) there must be no grounds to suspect ML/FT. This since, issues may arise when senior management officials are considered as being BOs. To begin with, SPs are to be vigilant as these situations may have been created to facilitate BO concealment, wherein the person who is actually exercising control over the company may be different to the senior management official and may be hiding behind them in order to conceal his/her identity. This may be done for the purpose of committing ML or any other predicate offence. Furthermore, there may be someone else influencing the senior official's decisions, thus hinting that the senior management official is only the BO on paper and that someone else is actually controlling the company.

To limit the risk of servicing customers with concealed BOs or who are using the SP's services to conceal the true BO(s) of a legal entity, SPs are to look out for a number of scenarios including the following:

i. The absence of or a limited local footprint.
ii. The creation of inexplicably complex structures.
iii. Known BO lacks key knowledge of the company's operations.
iv. Frequent changes to the company name.
v. Simplistic documentation held for shareholder loans.

For more red flags relating to concealment of BO, reference may be made to the FIAU's Intelligence Factsheet issued on 31 December 2021, entitled 'The misuse of corporate vehicles registered in Malta - Focus on Beneficial Ownership concealment - Red flags and Case Studies'. Reference here must also be made to the paper issued by the FIAU on 31 March 2022 entitled 'Compliance with Beneficial Ownership Obligations by Company Service Providers', which covers the thematic reviews conducted in 2021 to assess the level of compliance with BO obligations by company service providers (CSPs).

Between 2021 and 2022, a total of 63 BO related breaches were identified. Amongst these, the most common BO related breaches related to:

(a) The identification and verification of the BO, which at times was considered a serious breach, especially when the identity of the BO was unknown.
(b) The ownership and control structure of the customer, which at times was considered a serious breach, particularly when complex structures were not adequately verified to determine who is the BO.
(c) The failure to report or consider reporting an STR where the suspicion of ML/FT is due to concealment or disguise of the BO. This was always determined a serious breach in view of the ML/FT risk exposure linked with providing services to customers whose true BO(s) is/are concealed. This also gives rise to the possibility that predicate offences also surround the business relationship, including tax evasion and ML.

Identification and Verification of the Identity of the BO

Regulation 7(1)(b) of the PMLFTR explicitly states that customer due diligence measures shall consist in the identification, where applicable, of BOs, and the taking of reasonable measures to verify their identity.

Between 2021 and 2022, a total of 34 breaches relating to the identification and verification of the BO were identified. The failure to identify the BO for a corporate customer means that the SP is unaware and has no knowledge of the individual(s) to whom it is ultimately providing its services or products. This exposes the SP to high ML/FT risks. The identification and verification of a BO should be considered as a foundation for adequate customer due diligence. Without the identification of the BO, a SP would not possess information on the individuals benefiting from the transactions being effected to and from a corporate customer, and cannot monitor them effectively for suspicious behaviour. Therefore, the SP will not be able to conduct an adequate customer risk assessment of its customer.

When dealing with corporate customers, understanding who the BO is, is essential for various reasons including:

- Understanding who owns the customer and carrying out the necessary checks to understand any risk implications with such a relationship.
- Understanding who may potentially fund the activities of the customer.
- Corroborating the information available on the BO with the purpose of the customer and ensure a rationale for any divergences which may arise between the two.

However, the majority of the breaches identified were in relation to obtaining/ keeping a copy of the identity verification document of the BO. Therefore, there is an overall very good level of compliance by SPs to identify who the BO of a corporate customer is. While this is of utmost importance, SPs should also verify the identity of the BO through reliable documentation and ensure that a copy of such document is kept.

Case Study (Credit Institution) – BOs not known

The SP in question failed to abide to BO related obligations in various ways as per below examples:

- A number of corporate customers for which no BO information was held.
- A number of corporate customers for which the Bank failed to determine additional BOs.
- A number of corporate customers for which the Bank failed to establish a link between the corporate customer and its BO.

In view of this, the Bank failed to understand who the owners or controllers of the corporate customers were, thus failing to abide to one of the most basic and intrinsic elements of the customer due diligence process.

Case Study (Investment Services) – Verification of identity not carried out

The Company failed to collect verification documents in relation to the identity of the customer. The Company claimed that it had failed to do this because electronic verification (the method of verification used by the Company) was not yet permitted by the IPs. However, this was not the case because, as per the 2011 IPs, SPs could verify the identification details of the applicant for business through recognised commercial electronic data providers if the applicant is not present for verification purposes. Moreover, further amendments to the IPs were adopted to enhance and harmonise them with amendments to the legislation and other material developments originating from changes in international standards. Therefore, the Company's arguments regarding its non-compliance were not founded, because this method of verification was in reality allowed. Moreover, if electronic verification was not catered for in the IPs at the time of onboarding but was included in the IPs later, the Company would have been expected to update its customer profile to reflect these amendments.

The ownership and control structure

In the case of a customer being a body corporate, foundation, trust or similar legal arrangement, SPs are to take reasonable measures to understand their customer's ownership and control structure. This emanates from Regulation 7(1)(b) of the PMLFTR. Whilst some structures may be clear and easy to understand, others may be complex, involving several tiers, legal vehicles, and individuals. When SPs are dealing with complex structures, they are to proceed with caution as this could expose them to an increased risk. Understanding the corporate structure, the BO behind the structure and the legitimate purpose behind it are therefore especially important aspects.

To ensure that this risk is minimised, SPs are to obtain an explanation of the ownership and control structure of the customer. Both the explanation, as well as the structure chart (where this is considered necessary) are to include enough detail for the SP to understand how the BO is linked to the customer.

The ownership and control structure is to be then verified by the SP, by making use of commercial databases, company registries, relevant audited accounts or by obtaining a certified copy of the said structure.

Between 2021 and 2022, a total of 22 breaches relating to the ownership and control structure were identified.

In most serious cases, the SPs failed to maintain information on the ownership and control structure of their customers. This meant that SPs were unaware as to whether the customer they were servicing was complex or otherwise, thus being unable to adequately assess the customer risk. Additionally, and most importantly, the SPs were not able to sufficiently understand the structure of the customers they were servicing, therefore, potentially giving rise to the possibility of BO concealment. However, most of the breaches linked to the verification of ownership and structure of an entity, were related to the structure charts drawn up not being comprehensively verified.

Case Study (Notary)

The SP had failed to document an explanation of the company's ownership and control structure for circa 27% of the customers reviewed, where a complex structure was identified. In this scenario an ownership and control structure was necessary to ensure that there was sufficient information to determine who the BO was, as well as the risks surrounding the customer. Moreover, the ownership and control structure of circa 9% of the customers reviewed was not comprehensive enough to establish who the BOs were. This due to the fact that the percentage written down on the structure indicated the percentage of control rather than the percentage of ownership.

Case Study (Corporate Service Provider)

Shortcomings in relation to the verification of the customers' ownership and control structures were identified for 10% of the customers reviewed.

Case 1 – An ownership and control structure chart was provided in relation to the corporate customer where the ownership was held as to 80% through a trust, whilst the remaining 20% was held through a shareholding entity, which in turn was owned by a foundation. The structure chart and letter explaining the ownership and control structure of the corporate customer were not considered adequate for the purposes of independently verifying the ownership and control structure as it was certified by the trustee of the trust holding shares in the corporate customer. Certification is required from someone independent from the structure so that there is a degree of objectivity in the verification exercise itself. In addition, even if one were to consider the trustee as a possible certifier, the trustee may only be aware of the part of the structure which from the trust leads down to the corporate customer. It cannot be said with certainty that it also had visibility of the part extending from the foundation downwards or with what degree of certainty was it aware of who the beneficiaries of the foundation were.

Case Study (Advocate - Firm)

Issues with the ownership and control structure were noted for approximately 12% of the customers reviewed. Examples of this are being given hereunder:

Case 1 – The Firm in question failed to ensure that the information in the memorandum and articles of association was still valid at the time of onboarding. In fact, these were dated before the onboarding. Moreover, the Firm failed to document the relevant changes that took place in relation to the structure of the customer, following its onboarding.

Case 2 – The customer was described by the Firm as fully owned by corporate shareholder 1, which was in turn owned by corporate shareholder 2. The latter was fully owned by the BO. Although identity verification documentation on the BO was collected by the Firm, it failed to provide documentation confirming the link between corporate shareholder 1 and the customer. Furthermore, when requested to provide documents verifying the ownership and control structure, the Firm provided further documentation relating to corporate shareholder 2, thus evidently failing to provide any in relation to the connection between corporate shareholder 1 and the customer.

Reporting

As mentioned earlier, the obligation to report any suspicion of ML/FT to the FIAU emanates from Regulation 15(3) of the PMLFTR.

Between 2021 and 2022, a total of 11 breaches were identified for the failure to report situations involving the possible concealment of BO.

As part of the BO thematic and targeted examinations carried out by the FIAU, reporting breaches were identified in regard to the failure of SPs to submit STRs or SARs where a company was effectively being controlled by a person other than the individual claimed by the customer to be the BO. In certain instances, the SP identified an individual as a new BO, even though they had sufficient evidence to confirm that the previous BO would still be controlling, managing, and giving the day-to-day instructions for the running of the company.

Other red flags indicative of BO concealment and which should have led SPs to submit an SAR in these cases included:

- Transactions flowing to/from the corporate customer to/from individual/s who were no longer reported by the company to be the BO/s.
- Dividends paid to persons no longer having ownership of the company or otherwise being beneficiaries of shareholding loans.
- Change in shareholders resulting in a change in BO, followed by a change in director/legal representative, with the newly appointed director/ representative being related to the previous BO.
- Several changes in shareholdings without obtaining the necessary rationale and explanations.

Case Study (Corporate Service Provider)

The Company was expected to submit a STR or SAR in relation to reasonable grounds for suspicion that the customer might be owned by another individual who was not listed as the BO. In addition, there were grounds to suspect that tax evasion was taking place. Notwithstanding, the Company failed to report.

Numerous red flags were presented in the activities of this corporate customer:

Corporate Customer	Company 1	Company 2
Original BO- Individual 1	Owned by Individual 3 (Italian National)	Owned by Individual 1
BO then become Individual 2 (Swiss National)	Registered in the BVI	

Table 2- Overview of Companies

- The customer's BO (individual 1) at first was the contact person of a corporate service provider in a foreign jurisdiction but was subsequently replaced by another individual (individual 2).
- The SP was not receiving any payment for its services to the corporate customer, because it was renting office space from individual 2's partner (individual 3). Neither was it paying any rent for the office space let to it.
- The Corporate customer was involved in a number of loan and vessel transfer agreements, as will be further explained below. The way the transfers were structured, as well as the purpose of the structure, posed questions as to the legitimacy of the funds being used. This since a loan facility of €3,200,000 was granted by company 1 to company 2. The former company was owned by individual 3 and registered in the BVI whilst the latter was owned by individual 1 (the original BO of the corporate customer). Company 2 then granted a loan facility of the same amount to the corporate customer on the same day as the initial transfer. A couple of days later, the corporate customer then purchased a vessel from company 1 for the same value, with the purchase price of €1 and other considerations. Therefore, it can be deduced that the funds for the corporate customer to purchase the vessel from company 1 (owned by individual 3), originated from company 1 itself which had also owned the vessel.
- Moreover, the Company identified the source of wealth of its customer as being derived from individual 3 and that this individual could be considered as the BO.

In view of the above information, the Company was presented with a situation where it had reasonable grounds to suspect that individual 3 was a BO of the corporate customer. Moreover, there were enough irregularities for the Company to have had reasonable grounds to suspect that the transactions were connected to ML and tax evasion, thus meriting the filing of a suspicious report with the FIAU.

Case Study (Corporate and Fiduciary Service Provider)

An ownership transfer took place where 99% of the shareholding was transferred from the previous BO of the corporate customer to its present BO. The only explanation behind this transfer was that the previous and present BOs had a close and personal relationship. On that same day, a letter was issued wherein the present BO authorised the SP's Director to accept instructions, for the day-to-day running of the corporate customer, from a company owned, controlled, and managed by the previous BO. Therefore, the previous BO retained control of the corporate customer. Moreover, it was evident that the new BO had no experience or knowledge of the main business area of the corporate customer. In fact, the corporate customer was a holding company investing in subsidiaries involved in the shipping and maritime industry; an industry which the present BO lacked any knowledge of.

The above information should have been enough for the Company to submit a suspicious report to the FIAU.

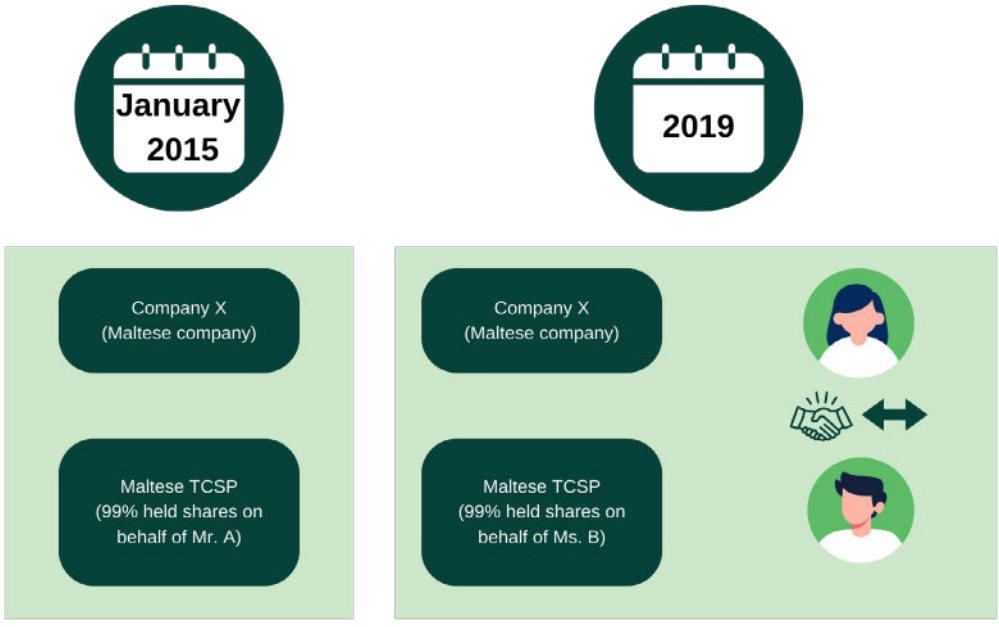


Fig. 4 – Summary of the above case study

Case Study (Trustees and Fiduciaries)

The customers reviewed were two companies within the same structure. Company Y was the shareholder of company X, owning 99% of the shares. These companies were originally owned via a declaration of trust dated 2007, enabling the SP in question to act as trustee and nominee of the BO (Mr A). Approximately 11 years after the relationship was established and shortly prior to the introduction of the obligation to record beneficial owners in the BO Register held by the Malta Business Registry, the BO requested a change in structure. The SP, acting on behalf of the BO Mr A, transferred 75% of the shares of company X onto the SP, however this time these were to be held in trust for three individuals who were the wife and the children of Mr A. Mr A, i.e., the original BO, retained the remaining 25% of the shares. Therefore, each shareholder had no more than 25% of the shares and an official of the SP had to appear as the Senior Managing Official (SMO) on the MBR's BO register for both corporate customers. Nonetheless, decisions regarding the corporate customers were taken by Mr A as he was the only person present during meetings. This clearly indicated that the individual retained control of the two companies and was therefore their BO despite the change in the structure which conveniently coincided with the introduction of the obligation to record BOs on the MBR.

In view of this information, the Company should have questioned whether this arrangement was facilitating ML/FT and should have consequently proceeded to submit a suspicious report to the FIAU.

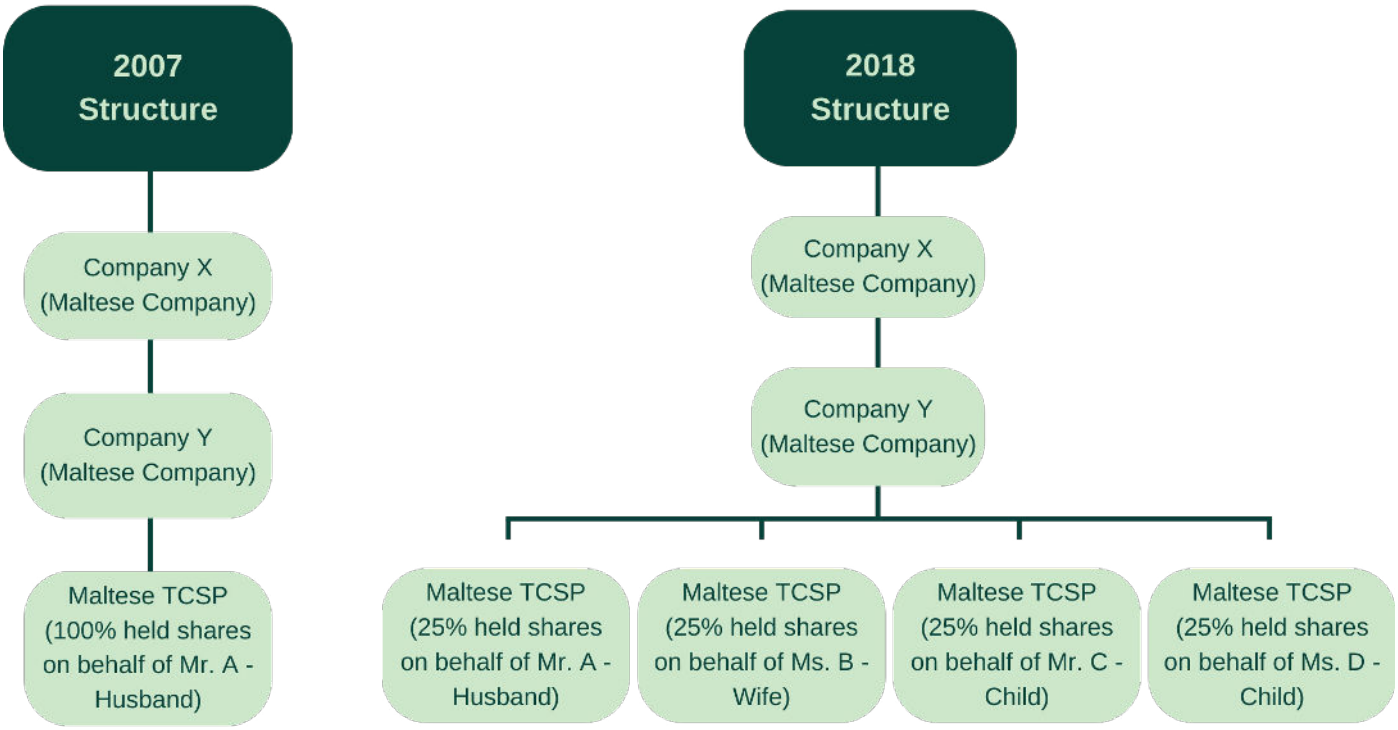


Fig. 5 – Summary of the above case study

Concluding Remarks

The FIAU remains committed to combat ML/FT. Yet effectiveness can only be achieved through the joint efforts of all concerned stakeholders, including SPs. The significant investment in the AML/CFT control framework by SPs is proof of the increased level of commitment to fight ML/TF at large. This paper aims to provide additional guidance to SPs as to the areas that should be given priority to ascertain that their services are safeguarded from illicit intent and abuse. The paper provides guidance on red flags that should be looked out for and control frameworks that should be in place. The commitment by SPs to remain vigilant to the risks they are exposed to as a result of the customers they service, as well as their ongoing investment in AML/CFT controls is crucial to safeguarding the integrity and reputation of the jurisdiction.

AML/CFT is an ongoing and complex endeavour that requires collaboration, technological innovation, and regulatory diligence. The FIAU is intent on providing SPs with the necessary tools to allow them to calibrate their AML/CFT controls in the best possible way to be effective mitigating instruments. Sharing experiences, including through the sharing of cases where controls did not achieve their intended aim or were absent, is one way in which this can be done. A failure may result in sanctioning but ultimately a failure is also a chance to further learn and strengthen one's AML/CFT controls. It is only in this manner that all relevant stakeholders, including the FIAU and SPs, can successfully meet their legal and moral obligations towards the country and the global financial system as a whole.

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

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq l-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