



FIAU

Financial
Intelligence
Analysis Unit
Malta

The Enforcement Guide

An overview of the FIAU's Enforcement Process

First issue: April 2026

Applicable from: 1st July 2026



Table Of Contents

Introduction and Scope	05
Section 1: Legal Empowerment	09
1.1 Powers of the FIAU	10
1.2 The Compliance Monitoring Committee	12
1.2.1 Establishment and involvement of the Compliance Monitoring Committee	12
1.2.2 Meeting requests with the Committee	13
1.2.3 Determination of breaches and administrative measures to Impose	15
Section 2: The Enforcement Process	16
2.1 Supervisory Interventions	17
2.2 Enforcement Notice Letter	18
2.3 Other Interventions	19
2.4 Written Representations and In-Person Meeting	20
2.4.1 Written Representations	20
2.4.2 In-Person meeting	21
2.5 The CMC Process	22
2.5.1 Case Assignment	22
2.5.2 Case Processing	22
2.5.3 Case Presentation and Determination by the CMC	23
2.5.4 Case Determination Notification	24
2.5.5 Applicability of the Process	25
Section 3: The Sanctions Policy and Procedures	26
3.1 Administrative Measures	27
3.1.1 Administrative Penalties	28
3.1.2 Periodic Penalty Payment	31
3.1.3 Method of Payment	32

Table Of Contents

3.2 Directives requiring corrective actions	32
3.3 Written Reprimands	35
3.4 Publication of Administrative Measures	35
3.5 Recommendations or notifications to other regulatory/supervisory authorities or other bodies	36
3.6 Specific recommendations on key persons within the subject person	37
3.7 The termination of business relationships	38
3.8 Any other administrative action the Committee legitimately directs	38
3.9 Interim Measures	38
3.10 Lack of clear-cut breaches	39
Section 4: The Sanctions Calculation Tool	41
4.1 Three Pillar Considerations	43
4.1.1 Pillar 1: Gravity and Impact of the Breach	43
4.1.2 Pillar 2: Regard to AML/CFT obligations	46
4.1.3 Pillar 3: Size of the subject person	47
4.1.4 Final Considerations	48
Section 5: Communication with the subject person	50
Section 6: Cooperation with Prudential Regulator	53
6.1 Decision Letters	54
6.2 Prudential Concerns	54
6.3 Joint Action	55
6.4 Exchange of Information	56
Section 7: Enforcement Lifecycle	57
Section 8: Appeals	61
Conclusion	64

List of Abbreviations

Abbreviation	Full Term
AML/CFT	Anti-Money Laundering/Combatting the Funding of Terrorism
BoG	Board of Governors
CASPAR	Compliance and Supervision Platform for Assessing Risk
CBARR	Centralised Bank Account Register Regulations
CMC	Compliance Monitoring Committee
CO	Compliance Officer
ENL	Enforcement Notice Letter
FIAU	Financial Intelligence Analysis Unit
GPF	Governing Principles and Framework
MFSA	Malta Financial Services Authority
MGA	Malta Gaming Authority
ML/TF	Money Laundering/Terrorism Financing
MLRO	Money Laundering Reporting Officer
PMLA	Prevention of Money Laundering Act
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
RBA	Risk-Based Approach
REQ	Risk Evaluation Questionnaire
RFI	Request for Information
SCT	Sanctions Calculation Tool
SMO	Senior Managing Official
SP	Subject Person
ToR	Terms of Reference

Introduction and Scope

The Financial Intelligence Analysis Unit's (FIAU, Authority, Unit) foremost priority is to safeguard the integrity of the jurisdiction by preventing it from being exploited by money launderers and terrorist financiers. In doing so, it also plays a critical role in protecting the public at large from the broader economic and social harms associated with money laundering and terrorism financing. One key way to achieve this objective is a legal and regulatory framework that requires the subject person (SP) to implement robust AML/CFT controls. These controls should be designed to allow SPs to understand: the risks they face, the customers they service, and be aware of the transactions or activities they are exposed to, with the ultimate aim of identifying and reporting any suspicious behaviour, activity, or transaction.

To ensure these obligations are met, the Authority conducts supervisory interventions to assess compliance and the adequacy and effectiveness of AML/CFT frameworks implemented. Where these assessments reveal material shortcomings, cases are escalated to the FIAU's enforcement section. Enforcement action is then taken based on the nature and materiality of any breaches determined following due process.

Importantly, enforcement extends beyond the mere imposition of penalties. The primary objective of all administrative measures applied by the Authority is to drive compliance and ensure that the SP has in place AML/CFT systems that are not only robust but also effective and sustainable over time.

Whether through corrective measures, sanctions, or preventive actions, the approach taken ensures any enforcement decision is **proportionate, effective, and dissuasive**. The collective approach ensures past misconduct is accounted for and, more importantly, that future conduct improves and effective controls against ML/FT risks are implemented. Through this approach, enforcement helps maintain a fair, transparent, and well-regulated environment.

The Authority applies a risk-based approach in the assessment and handling of supervisory cases. Where shortcomings are identified but do not reveal any material weaknesses overall, such cases are not escalated for enforcement action. Even within the enforcement process, a risk-based approach is maintained to ensure that priority is given to cases presenting the most significant or material weaknesses, thereby focusing resources where they can have the greatest impact.

In November 2022, the FIAU issued its 2023-2026 Strategy, which, in its first pillar, states the need to ensure a more transparent approach to monitoring and enforcing AML/CFT measures, and to promote accountability and build public trust and confidence in the FIAU's compliance monitoring and enforcement functions. This Enforcement Guide (the 'Guide') aims to provide an end-to-end explanation of the FIAU's enforcement process and to assist the SP and the public at large in understanding the process the Unit follows to ensure a just and fair process when applying effective, proportionate and dissuasive enforcement actions. This Guide is comprised of **eight sections**:

1

Within its first section, the Guide sets out the legislative provisions that mandate and empower the FIAU to act in respect of any breach or failure to comply with any rules, regulations or directives. It also lays out and gives a brief explanation of the administrative measures available at law to the FIAU for the purposes of carrying out its enforcement function. Finally, this section explains the composition and governing principles of the Compliance Monitoring Committee, an internal organ set up by the FIAU to support the exercise of its enforcement powers.

2

The Guide then provides an overview of the enforcement process; starting from when a case is escalated to the Enforcement Section following the issue of a Potential Breaches Letter to the SP, to the receipt of representations (including any in person meeting) submitted by the latter, and the subsequent preparation and presentation of the case before the Compliance Monitoring Committee (CMC, Committee). It also explains the process that the SP may be required to follow to implement corrective actions as required by the CMC. Reference is also made to settlement agreements that may be entered into between the FIAU (acting through the CMC) and the SP.

3

This section then expands upon the FIAU's Sanctions Policy and Procedures. This document highlights the considerations taken by the Compliance Monitoring Committee when determining the appropriate measures to take or impose.

- 4** The next section provides a high-level overview of the FIAU's internal sanctions calculation tool, which calculates an appropriate value of an administrative penalty for the CMC to consider in its deliberations. This value, as further explained in the relevant section of this Guide, is based on the type of the obligation breached, the extent to which the breach is serious, systematic and repetitive, the impact of the breach, as well as the SP's conduct both when the breach was committed and after.
- 5** This section explains the typical communication process with the SP undergoing an enforcement process, highlighting what to expect in terms of notifications throughout the process.
- 6** The Guide also explains the cooperation arrangements with other domestic authorities as well as with foreign counterparts and supranational authorities.
- 7** Enforcement Lifecycle is the section that explains the procedure and timelines expected from the moment a potential breaches letter is issued by the FIAU (or its Agents), up to the determination of the administrative measure/s the CMC decided to impose, and the publication of such measures.
- 8** Finally, this Guide provides an insight into the process undertaken should an appeal be lodged against the FIAU by a SP before the Court of Appeal (Inferior Jurisdiction) following the imposition of an administrative penalty exceeding five thousand Euro (€5,000).

This Guide is being published to provide information regarding the processes implemented by the FIAU's enforcement section. It is important to note that this Guide is forward-looking and does not necessarily apply to past cases determined, where enforcement action may or may not have been taken. Therefore, this Guide is not intended to have retroactive application. It is not intended to be legally binding upon the FIAU or exhaustive, and does not address every aspect of the enforcement process in place. It serves to highlight and explain to the SP the most salient and relevant elements of the processes and procedures implemented by the FIAU in the carrying out of its enforcement function.

This Guide explains the typical enforcement process adopted by the FIAU, however, depending on case-specific circumstances, the FIAU may vary its enforcement process as necessary to ensure that any ML/TF risks are appropriately addressed. Users of this Guide are advised to exercise due care and, where appropriate, seek further clarification or independent legal advice in relation to their specific circumstances.

Section 1: Legal Empowerment

Section 1: Legal Empowerment

1.1 Powers of the FIAU

The FIAU is responsible for supervising SPs for compliance with their Anti-Money Laundering and Combating the Funding of Terrorism (AML/CFT) obligations emanating from the Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta (PMLA, the Act), and any regulations made thereunder, principally the Prevention of Money Laundering and Funding of Terrorism Regulations, Subsidiary Legislation 373.01 (PMLFTR, the Regulations), and any other procedures or binding guidance issued by the FIAU in terms of the PMLFTR. The FIAU is also responsible for monitoring compliance with the reporting obligations under the Centralised Bank Account Registry Regulations, Subsidiary Legislation 373.03 (CBARR).

Breaches of the requirements arising from any of these provisions may result in regulatory action. The FIAU is empowered to enforce the provisions of the PMLA, the PMLFTR and any procedure or guidance issued in terms of Regulation 17 of the PMLFTR and Regulation 5 of the CBARR. The FIAU is empowered to impose administrative measures and penalties for identified breaches of AML/CFT obligations, in terms of Regulation 21 – 23 of the PMLFTR and Regulation 8 and 9 of CBARR and to issue directives to SPs in terms of Article 30D of the PMLA.

The imposition of corrective actions through the issue of directives under Regulation 23 is the main administrative measure intended to address and rectify non-compliance by mitigating risks, preventing reoccurrence, and restoring compliance. Where appropriate, remediation may be required independently of, or instead of, the imposition of a fine. Self-imposed remediations are among several other factors considered when determining enforcement outcomes.

Not all supervisory interventions carried out by the Authority result in escalation to enforcement. In fact, a notable percentage of the FIAU's annual supervisory interventions have no significant shortcomings or reveal issues that are not sufficiently material to warrant escalation to enforcement. In these cases, the FIAU adopts a risk-based proportionate approach by addressing these matters through supervisory remediation, which is less intrusive and not legally imposed, but is carried out by agreement with SPs.

The administrative measures that the FIAU may impose, as well as the criteria considered to determine which one or more of the measures to impose, are explained in Section 3 of this Guide.

Regulation 22 of the PMLFTR and Regulation 9 of CBARR also allow the Authority to settle administrative penalties by entering into settlement agreements with SPs, provided certain criteria are met. These agreements allow for:

- A reduced but effective, proportionate and dissuasive penalty, subject to the waiver of the right to appeal.
- The admission of the breaches.
- The prompt implementation of remedial actions.

Failure to remediate will result in the original penalty becoming payable, and the potential application of other enforcement measures to ensure completion of the remedial actions. The Settlement Policy is available on the FIAU's website: Settlement Agreement Policy.

The FIAU also holds the power, through Regulation 21(5) of the PMLFTR, to impose fines on specific categories of personnel if they are found to have been aware of inadequate AML/CFT controls within their organisations and failed to act with the requisite diligence expected of their positions, or who have otherwise contributed to the ineffective application of the required AML/CFT controls.

Examples include:

- Personnel holding the position of a director or similar functions.
- An officer holding a senior executive management function; or an officer appointed as a reporting officer or to carry out a monitoring function (i.e., the MLRO and CO).

These are all collectively referred to as Senior Managing Officials (SMOs). This responsibility extends to situations where, through an act, omission, or gross negligence, the individual(s) severely impact the SP's control framework. For this Guide, any reference to SPs shall, where applicable, be understood as also referring to SMOs. SPs may wish to refer to the paper: *Common Issues related to the Money Laundering Reporting Officer* for further guidance.

1.2 The Compliance Monitoring Committee

1.2.1 Establishment and involvement of the Compliance Monitoring Committee

The Compliance Monitoring Committee (CMC/Committee) is an internal organ of the FIAU, established by its Board of Governors. The CMC was established in 2011 to ensure a committee consisting of experts and senior staff makes decisions on breaches, rather than vesting this solely in the FIAU's Director. Its purpose is to determine whether AML/CFT breaches were committed by the SP and/or the SMOs, and establish the proportionate, effective and dissuasive administrative measure(s) to impose for the breaches. The FIAU, acting through the CMC, may also enter into settlement agreements with the SP and is responsible for monitoring compliance with directives requiring corrective actions by the SP.

The CMC is established and managed by its Governing Principles and Framework (GPF) as enacted by the FIAU's Board of Governors (BoGs). The CMC's GPF may be accessed on the FIAU's website. In determining the administrative measures to impose, the CMC is also guided by a Sanctions Policy (**Refer to section 3**).

The CMC is convened as and when necessary. Its composition is explained in the CMC's GPF, however, each CMC may be composed of different members. CMC meetings are held only when a quorum is met. A CMC Secretary is responsible for taking minutes of the decision/s. Once a CMC meeting is set, the members receive a notice from the CMC Secretary and, in line with the GPF, each member ensures there is no conflict of interest related to the case to be discussed.

The same Committee members should be involved from the start of the enforcement process till a determination is reached. Therefore, the same Committee members should be present both during the In-Person Meeting (IPM)¹ with the SP (when requested by the SP), as well as during the Committee meeting that determines the breaches and the administrative measure(s) to impose. At least one Committee member is also present during the settlement process (where settlement would be offered), and all CMC members must agree to the terms of the settlement agreement to be entered into with the SP. Any change in the composition of the Committee shall be duly justified and communicated to the SP.

1

An IPM may be held remotely on a case-by-case basis.

1.2.2 Meeting requests with the Committee

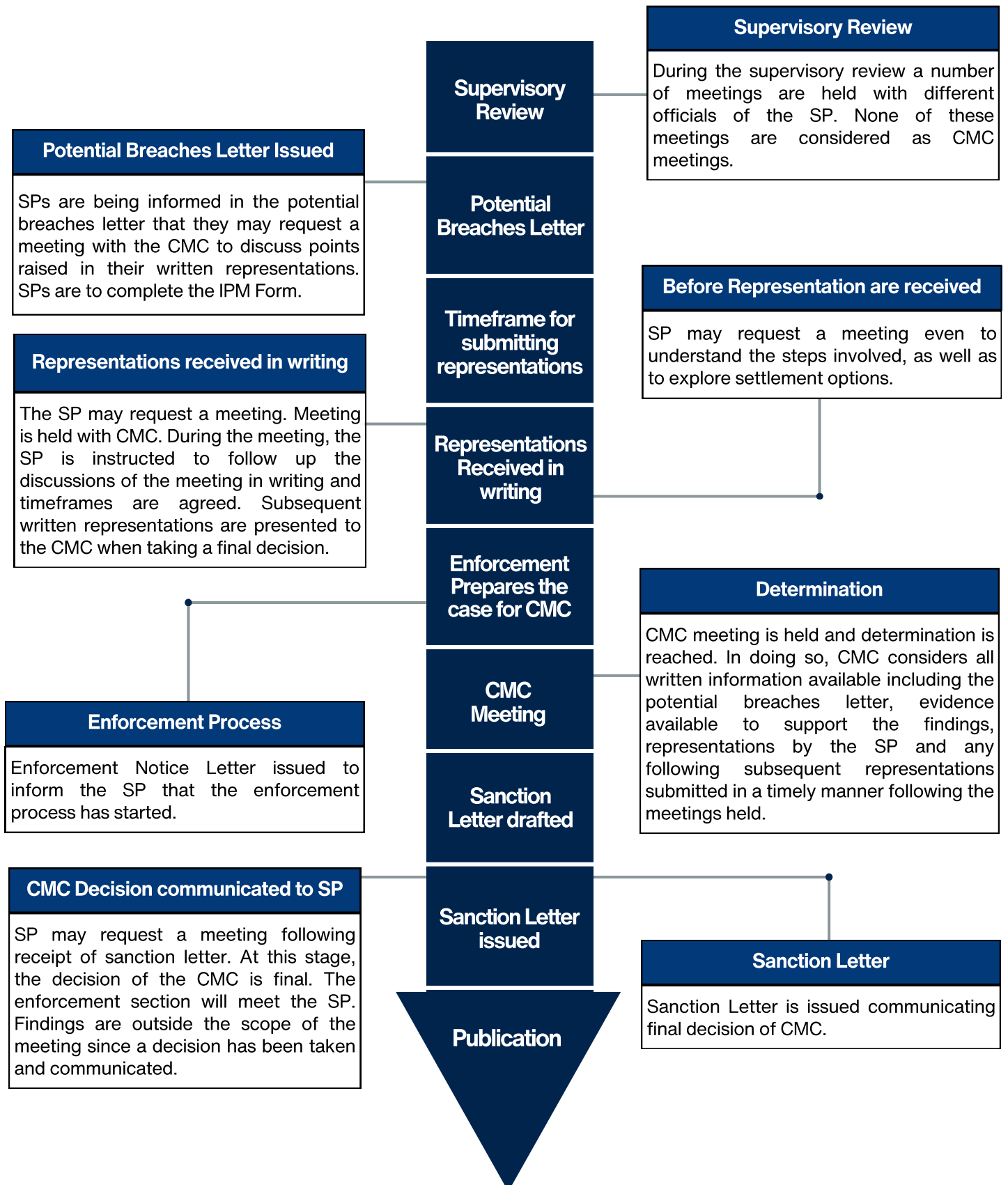
There are various stages where the SP may request a meeting with the FIAU. Depending on when a meeting is requested, this may also be with the CMC. A meeting requested with the FIAU to discuss general compliance matters may involve various members from different sections within the FIAU. This may include members of the enforcement section, but such a meeting would not be considered to be held with the CMC, even if CMC members are present. A SP must specifically request a meeting with the CMC; this typically is during an enforcement process.

The SP may request a meeting with the Committee at the onset of the enforcement process; the meeting is held only after the Enforcement Notice Letter (**as further explained in Section 2 below**) has been notified to the SP and written representations have been submitted. A meeting with the Committee is held only to substantiate the SP's written representations. Should a SP wish to hold a meeting with the CMC, the IPM Request Form (annexed to a potential breaches letter) is completed and returned with the SP's representations as a formal request for a meeting with the Committee. Following an IPM, the SP is provided with another opportunity to provide further written representations.

The SP is not present during the Committee meeting where decisions on potential breaches and any administrative measure(s) are determined. The Committee may request to meet with the supervisory officials (or agents) involved during the supervisory intervention, but these officials are not present when the Committee makes its final decisions.

The below diagram explains when meetings may be held:

Process Flow



1.3 Determination of breaches and administrative measures to impose

During the CMC meeting, the Committee establishes whether the SP has breached any of its legal obligations. If so, it then proceeds to establish/assess severity and materiality. The basis to determine a breach is always the legal obligations² in force at the time when the breach took place (or the current legal obligation in case of a continued breach). The SP's written representations, including the additional written representations provided by the SP following the in-person meeting, are an integral part of the Committee's discussion, as is the documentation that the Supervision Section (or the FIAU's Agents) would have collected during the compliance examination. The Committee has direct and unfettered access to all this documentation and always considers it when deliberating on the breaches and the administrative measure(s) to impose.

The SP is encouraged to submit comprehensive, robust representations and attach any additional documentation that may provide further clarity and substantiate them. The SP is also guided to read the FIAU's publication: *Optimising SPs' Representations* to understand the best practices SPs should adopt when submitting representations.

It is important that the SP clearly links each representation to the relevant section and/or paragraph of the potential breaches letter, by using the same reference. If this link is not made, the Committee may decide not to consider the representations.

When determining the administrative measure(s) to impose for the determined breaches, the Committee follows the principles and considerations of the FIAU's Sanctions Policy and uses the Sanctions Calculation Tool to be guided as to the quantum to impose when an administrative penalty is necessary. The Sanction Calculation Tool serves as a guide to the CMC. However, the final determination of the quantum to be imposed is solely at the CMC's discretion. The CMC shall always ensure that the penalty imposed is **effective, proportionate and dissuasive**. Refer to **Sections 3 and 4** for an explanation of the considerations enshrined in the Sanctions Policy and the Sanctions Calculation Tool.

²

As enshrined in the PMLFTR or the CBARR and other binding guidance issued by the FIAU

Section 2: The Enforcement Process

Section 2: The Enforcement Process

The CMC may determine breaches and take administrative measures in the following circumstances:

- i) following a supervisory intervention
- ii) following receipt of material information that evidences potential material failures
- iii) following the assessment of operational breaches
- iv) for not abiding by a lawful order or directive issued by the FIAU in terms of Article 30C and 30D of the PMLA.

This Section aims to explain the Enforcement Process³ followed by the FIAU and the CMC and guide the SP through it.

2.1 Supervisory Interventions

Supervisory interventions are carried out by the FIAU's Supervision Section or by the Malta Financial Services Authority or the Malta Gaming Authority acting as the FIAU's Agents (collectively referred to as the Supervisor) for each of the respective sectors they regulate, or by other Agents of the FIAU as may be appointed by the FIAU in terms of the Law.

Supervisory Interventions may identify no or minor shortcomings or more material weaknesses that would warrant an enforcement process. In the latter case, the SP would receive a potential breaches letter from the Supervisor. The letter details all the findings observed during the compliance examination as well as explain any potential breaches identified following a supervisory intervention. The letter also explains the next steps in the enforcement process, including the right to provide written representations and the right to request an in-person meeting with the CMC. This letter contains instructions for accessing the case documentation folder, which is available to the SP until the time written representations may be submitted. At this stage, the case documentation folder contains all documentation obtained by the Supervision Section. The case documentation folder is also available to the CMC to determine the respective case. The right of access to the documentation folder does not extend to confidential information or internal preparatory documents of the FIAU or its Agents.

³ The enforcement process excludes any corrective actions necessary, which form part of the broader enforcement lifecycle.

2.2 Enforcement Notice Letter

The SP needs to submit written representations within the timeframes stipulated in the potential breaches letter. However, the SP can submit a written request for an extension, which, in justified circumstances, is upheld. The case documentation folder, the potential breaches letter, and the representations, together with any documentation submitted with the representations, will be received by the FIAU's Enforcement Section, in preparation for the initiation of the Enforcement Process.

The SP receives an Enforcement Notice Letter (ENL) once the CMC has been notified of the case, and therefore, a CMC is constituted. The ENL contains details including: the estimated timeframes for the enforcement process to be concluded, the name and designation of the members composing the respective CMC, the date for the in-person meeting (if requested by the SP with its written representations) and a link to the case documentation folder that the CMC will use to determine the case. The ENL also informs the SP of its right to be assisted by a legal representative throughout the Enforcement Process.

The link to the case documentation folder remains accessible until:

- A decision by the CMC is notified to the SP, and the SP pays the administrative penalty.
or
- If not in agreement or in case the SP fails to pay the administrative penalty, until the lapse of the term afforded by law to appeal the decision before the Court of Appeal (Inferior Jurisdiction).
or
- In case of settlement, until a settlement agreement is reached between the parties.

Should a SP decide to appeal the CMC's decision, the case documentation folder is no longer accessible.

The Enforcement Process is concluded once the CMC's decision has been communicated to the SP, or a settlement agreement has been concluded between the parties. The CMC will endeavour to conclude the enforcement process within 18 months of the potential breaches letter. However, this may vary depending on the complexity and circumstances of each case presented to it. Refer to **Section 7** for an explanation of the Enforcement Lifecycle.

2.3 Other Interventions

The CMC may also take enforcement action for breaches that are more operational or case-specific. These refer to:

- a. Late, no replies or submission of incorrect replies to FIAU requests for information (RFIs) issued in terms of Regulation 15(8) of the PMLFTR.
- b. Late, non-submission, or submission of incorrect information of periodic reports required by the FIAU to perform its functions, such as the REQ and/or SP Profile, in terms of Regulation 19 of the PMLFTR.
- c. Late, non-submission or submission of incomplete reports in terms of Regulation 4(2) of the CBAR Regulations.
- d. Failure to adhere to a monitoring order issued by the FIAU in terms of Article 30C of the PMLA.
- e. Failure to adhere to the terms of a Directive imposed by the FIAU in terms of Regulation 23(1)(c) of the PMLFTR and Article 30D of the PMLA.
- f. Any other circumstances that arise from information or evidence provided by Authorities (including other sections within the FIAU), that may indicate potential AML/CFT breaches in the SP's operations, not explicitly covered by the foregoing situations.

In relation to a. to c. above, the Enforcement Section carries out a bulk, yearly exercise following the receipt of information highlighting a potential breach in relation to each respective obligation. In these cases, ENLs are not issued. However, the SP still has the right of representation in circumstances where the findings could lead to the imposition of an administrative measure.

In the cases described under a. to c. above, case documentation folders are not shared with the SP unless requested. The SP may also request an in-person meeting with the CMC if the SP believes it is necessary for better representation.

As to points d. to f. above, these refer to situations where the Enforcement Section is informed and would have received information and/or documentation that a lawful order or directive issued by the FIAU has been potentially breached, or that the SP has potentially breached its AML/CFT obligations either for case-specific relationships or else through systematic issues in its processes. In all such cases, the above-described enforcement process is to be followed.

2.4 Written Representations and In-Person Meeting

Any SP that receives a Potential Breaches Letter has the right to submit written representations, supported by any documentation necessary to clarify their position. The SP may also request an IPM with the CMC to elaborate on any aspect of those representations. Although no minutes are taken during the meeting, the SP may submit additional written representations afterwards to formally record and expand upon the points raised during the discussion. Any documentation referenced during the IPM must also be provided to the CMC.

2.4.1 Written Representations

The FIAU issues a Potential Breaches Letter to the SP detailing potential failures. The SP is then invited to submit representations that may provide for further clarifications, information, or documentation to explain the circumstances of the case. Submitting representations is particularly important as these can significantly impact the CMC's final decisions. However, where no representations are received, the CMC carefully considers whether the potential breaches described in the **Potential Breaches Letter** **subsist**, based on the information and evidence available to it, and, if necessary, decide which administrative measure(s) should be imposed.

When submitting representations, the SP should address all shortcomings it wishes to challenge as outlined in the Potential Breaches Letter issued by the FIAU, clearly explaining and evidencing where the SP is in disagreement with the identified potential breaches, as well as detailing the measures taken or planned to be taken to ensure compliance with the relevant AML/CFT regulations⁴, where applicable. These representations must be supported by documentation. When in disagreement with a finding, rather than solely stating disagreement, the SP is advised to put forward comprehensive arguments, detailed information, and tangible documentation to support its arguments.

The SP should clearly link both the representations and any supporting documentation to the numbered paragraph(s) of the potential breaches letter. Unless clearly referenced, the representations may not be considered by the Committee.

4

Any details of remedial actions undertaken both if these relate to potential breaches or otherwise will not be considered by the CMC as being an admittance of a breach by the SP. Remedial Actions are only considered as a mitigating factor.

2.4.2 In-person meeting

Moreover, in addition to submitting written representations (which must be submitted within the timeframes referred to in the Potential Breaches Letter), the SP can support its case verbally by arranging a meeting with the CMC. An in-person meeting is accepted only where written representations have been submitted. The purpose of the in-person meeting is to provide the SP with an additional forum to represent itself *viva voce* to the Committee. If the SP wishes to exercise this option, the SP must clearly indicate this through the submission of an IPM Form together with its written representations. Failure to complete or attach this Annex may be interpreted as an indication that the SP does not wish to provide any oral clarifications. The SP may be accompanied by its legal counsel or appointed consultant during the meeting.

However, the SP is expected to possess sound knowledge of its AML/CFT control framework and the risks it is exposed to and is therefore invited to participate actively in the IPM.

During the IPM, the SP may present and explain any aspect of the written representations, which it believes will assist the CMC in its decision. At least two weeks before the meeting, the Enforcement Section guides the SP to areas within the potential breaches letter and the written representations that require more attention during the IPM. At least one week before the IPM, the SP must indicate who will be present during the meeting with the CMC.

During this scheduled meeting, the SP may present additional documentation on the potential breaches identified following the compliance review and offer any further explanations it considers necessary. Similarly, enforcement officials in charge of the case and Committee members may ask case-specific questions and request clarifications on any policies or processes implemented by the SP.

2.5 The CMC Process

2.5.1 Case Assignment

Once the Enforcement Section receives the PB letter and written representations (if provided by the SP), a preliminary assessment of the case is carried out, and the case is assigned to an officer within the Enforcement Section.

2.5.2 Case Processing

The enforcement officer in charge of the case assesses the case (case officer), in line with the FIAU's internal enforcement processes and procedures.

In their assessment, the case officer, as a minimum:

- i)** Ensure that for each finding outlined within the potential breaches letter, the correct and complete provisions of the law have been quoted, and that the identified shortcomings were regulatory requirements at the time of the supervisory intervention.
- ii)** Verify that the findings of the case are clearly explained, free from inconsistencies or contradictions, and contain sufficient detail to permit the SP to submit comprehensive and well-founded representations.
- iii)** Once points i) and ii) are confirmed, cross-reference and corroborate the potential breaches letter with the supporting documentation obtained by or available to the FIAU.
- iv)** Review the representations provided by the SP to understand whether there are any challenges or rebuttals to the findings delineated in the potential breaches letter, and understand any remedial actions taken by the SP.

The case officer does not decide any breaches nor the administrative measure(s), if any. This decision rests solely with the Committee. Once the case processing is finalised and the assessment is discussed with a superior, the case proceeds for presentation to the CMC.

2.5.3 Case Presentation and Determination by the CMC

The case officer is tasked with presenting the case to the Committee, to facilitate the CMC's discussions of the findings and representations submitted and to assist it in making an informed decision whether there is a breach of the legal obligations and which administrative measure(s) to impose for determined breaches, if any. The CMC has access to the same case documentation folder that the SP received before submitting the representations, together with all the representations submitted by the SP.

The case presentation meeting with the Committee is attended by: at least the CMC quorum as per the CMC ToR, the CMC Secretary, and the case officer. Other members of the Enforcement Section, or other Sections⁵, may be present as observers.

During this meeting, the case officer begins by providing the Committee with a background and overview of the following key points:

- Details of the SP involved, the sector in which it operates, its authorisations/licences, a description of the products and services offered, its annual turnover and customer base (and, if necessary any other metric which helps the CMC understand the SP's size) at the time of the supervisory intervention, as well as other relevant information related to the SP; and
- Details of the supervisory intervention performed, or details of the information/documentation received by the Enforcement Section that initiated the case presented.

The case officer then presents the facts of the case to the Committee, providing a detailed description of each individual finding explained in the potential breaches letter, along with the representations submitted by the SP in response, and the documentation available at the FIAU. The Officer's role throughout this process is to provide the Committee with the information needed to make informed decisions, facilitate ensuing discussions and offer clarifications when needed. This process ensures that the Committee can reach an informed conclusion on the case presented.

5

Any member of the Supervision Section (or its Agents) may attend a CMC meeting as an observer provided that they have not been actively involved in the supervisory intervention being discussed during the meeting.

For each reported potential breach, the Committee determines whether it constitutes an actual breach of the SP's AML/CFT obligations and establishes the most appropriate administrative measure(s) to be imposed, if applicable. It then considers all the breaches identified, together with cross-cutting aggravating and mitigating factors, to arrive at an administrative measure(s) that is proportionate, effective and dissuasive.

In its determinations, the Committee also determine whether the FIAU should propose and offer the possibility to the SP to enter into a settlement agreement, as governed by the FIAU's Settlement Policy available on the FIAU's website: [Settlement Agreement Policy](#)

Formal minutes are taken during Committee meetings, ensuring that the Committee's deliberations is formally documented.

2.5.4 Case Determination Notification

Once the CMC decides on the case, the case officer, under the supervision of their superior/s, is responsible for carrying out the tasks needed to implement the CMC's decision. If the CMC decides to offer a settlement, the case officer then follows the steps in the FIAU's Settlement Policy.

When a settlement is proposed, the FIAU ensures that a high-level overview of the breaches, as decided by the Committee, is communicated. In addition, the quantum of the administrative penalty that would have been originally imposed by the CMC outside the settlement is communicated, as is the final administrative penalty imposed if a settlement agreement is reached, together with the remedial actions expected to be undertaken.

Where, in line with the Settlement policy, the CMC decides not to offer a settlement, or the SP does not agree to a settlement agreement, or if the settlement process was not satisfactorily concluded, the case officer follows the normal enforcement process and ensure that:

- i) A Sanction Letter is communicated to the SP informing them of the right to appeal the decision before the Courts of Appeal (Inferior Jurisdiction).
- ii) A publication notice (which is distinct from the Sanction Letter) of the administrative measure(s) imposed is issued in line with the FIAU's Publication Policy (**Publication of AML/CFT Administrative Penalties and Measures Policies and Procedures**).

For each potential breach, the Sanction Letter explains whether the Committee determined a breach of the law, the rationale for the decision, and how the representations and any documentation were considered. It also outlines the administrative measure(s) being imposed.

Where an administrative measure includes a penalty, the sanction letter must provide a breakdown of the penalty attributed to each breach, together with an explanation of the aggravating and mitigating factors considered, and a clear reference to the final amount being imposed. The Sanction Letter must also clearly set out the SP's right of appeal before the Courts of Appeal (inferior jurisdiction), and state that the penalty will be published on the FIAU's website.

2.5.5 Applicability of the Process

Actions on SMOs follow the same procedure as that following a supervisory intervention.

Section 3: The Sanctions Policy and Procedures

Section 3: The Sanctions Policy and Procedures

The Sanctions Policy and Procedures (SPP) explain the administrative measures that may be taken or imposed by the Committee, in line with its powers under law. The SPP provides the Committee with guidance to assist it in determining the appropriate measure(s) to take or impose in view of identified breaches related to the application of AML/CFT obligations.

3.1 Administrative Measures

Administrative Measures are all those actions that the Committee may take or impose on the SP for breaches of AML/CFT obligations or where the Committee has concerns about the implementation of AML/CFT obligations by the SP. The collective actions taken by the CMC must be proportionate, effective and dissuasive, as explained in the table below⁶.

Proportionate	A range of enforceable measures which can be applied in accordance with the severity of the breach, to ensure that the enforcement measure imposed is commensurate with: the seriousness, impact and frequency of the breach committed by the SP, the regard and extent to which a breach was deliberate or caused by recklessness, and the size and materiality of the SP.
Effective	The enforcement measure(s) applied are sufficient, so as not to be seen as a cost of doing business, that they promote compliance by the SP against which the measure has been imposed and deter the SP from repeating the breach.
Dissuasive	The extent to which an administrative measure can deter non-compliance by other SPs. This is achieved through official publication notices, fact sheets, guidance papers and outreach mechanisms to share case studies and ML typologies and provide guidance on the control framework necessary to manage them.

⁶ These definitions are included solely for guidance and clarity in the interpretation and application of this document. These definitions are not to be construed as exhaustive, nor as limiting the ordinary legal or contextual meaning of the terms where such interpretation may reasonably apply.

3.1.1 Administrative Penalties

Regulation 21 of the PMLFTR establishes the penalties the CMC may impose. The Committee uses the Sanctions Calculation Tool (SCT) to be guided as to the administrative penalty to impose the penalty; the resulting amount is merely indicative. It is at the CMC's discretion to determine the actual amount to be imposed. Refer to Section 4 for more details about the SCT.

The Committee may decide to impose a periodic pecuniary penalty, in addition to or instead of a one-time penalty. Daily pecuniary penalties should not be imposed for past failures, but for current non-compliance until compliance is attained. However, this measure is imposed when the Committee believes that the deficiencies are serious and that continued non-compliance with AML/CFT obligations could lead to material risk exposure to the SP, the jurisdiction or the EU. Daily penalties are imposed to encourage the SP to implement the necessary remedial measures within the shortest timeframe possible, thereby ensuring timely compliance and reducing the risk of ongoing breaches.

In determining this, the Committee considers the extent to which the SP is willing to take the necessary remedial actions and the potential impact caused by delays in compliance.

Where the CMC has determined that SMOs are found, through an act or omission, whether intentional or due to gross negligence, including through the lack of proper oversight of subordinates, and to have caused or contributed to the commission of the breaches by the SP, an administrative penalty may also be levied on these officials in their personal capacity.

The Committee should consider imposing an administrative penalty when a case presents any one or a combination of the following scenarios:

- Where the breach is determined to be serious, repeated or systematic (as defined in sub-section 3.10 of this Section).
- Where the breach persisted over a significant period of time and the SP did not take active steps to remedy it.
- Where the SP has a history of non-compliance.
- Where the breaches manifestly led to significant or very significant risks of or facilitation of ML/FT.

- Where the deficiencies exposed the SP or the financial or other system or the Union to significant or very significant ML/FT vulnerability.
- Where breaches are isolated, however, their impact is considered significant or very significant in view of the value or volume of transactions or activities involved.
- Where the breaches identify structural and material failures in the implementation of the SP's policies, procedures and/or controls or their lack.
- Where the SP materially failed to make sufficient progress in implementing a follow-up or remediation directive and failed to remediate serious deficiency/deficiencies.
- Where the SP made a profit or avoided costs/losses as a result of the breach and thus should not be permitted to benefit from the breach, where this may be determined.
- Where, if seen in isolation, a breach may not be serious or material, but when assessed in combination with other breaches, this is deemed to be serious or material.

The above list is non-binding and non-exhaustive. Depending on the specific circumstances of the case, the Committee may identify and consider additional elements that could constitute or contribute to determining a breach.

Determining the Administrative Penalty Value

The value of the administrative penalty must be determined consistently to avoid arbitrary decisions. The Sanctions Calculation Tool provides a methodology to assist the CMC in computing the appropriate value of an administrative penalty, while at the same time affording the CMC an appropriate degree of discretion to cater for the specific circumstances of each case.

In determining the value of the administrative penalty, the Committee is to ensure that:

- The value does not exceed that which the FIAU is legally empowered to impose (*ultra vires*).
- The totality of all measures imposed for the AML/CFT breaches identified, including those imposed by other supervisory/regulatory authorities or bodies, must be proportionate, effective and dissuasive.

- The amount of the fine imposed should be commensurate with the nature and seriousness of the breaches, taking into consideration the aforementioned factors.
- The fine should be effective in that the SP cannot consider it as a mere 'normal cost of doing business', and it should be significant enough to impact the SP's annual income.
- The fine should be dissuasive to both the SP in question and other SPs.
- If the breach facilitated a large transaction or enabled multiple transactions, without or with minimum scrutiny, the fine should be proportionately larger than a breach that enabled a small or single transaction and vice versa.
- The fine should take into consideration the duration of during which the breach has subsisted.
- The fine should be significantly higher for repeated breaches.
- The fine should take into account the impact of non-compliance on the SP's own operations, or of the group to which it belongs (where applicable), the jurisdiction and the Union.
- The SP should not be able to gain financially from transactions or activities that are facilitated or enabled as a result of breaches of AML/CFT obligations. In these cases, the fine should at least equal the amount of any revenues generated (directly or indirectly) by the breach, where this may be calculated or estimated.
- The fine should consider any losses to third parties, where this can be determined.
- The fine should be proportionate to the size of the SP and the products and/or services affected by the breach.
- The fine should be proportionate to the financial strength of the natural or legal person held responsible.
- The fine is consistent with fines levied (based on the same legislative provisions) against SPs of similar size for comparable breaches.
- The fine should be proportionate to the ability of the SP to pay the penalty. Where the penalty may affect compliance with prudential regulations, the prudential regulator is consulted to ensure that compliance with prudential matters is safeguarded.

3.1.2 Periodic Penalty Payment

In determining whether to impose a daily penalty, in addition to an administrative penalty or as a stand-alone penalty, the CMC should consider whether:

- It believes that the SP should be subjected to a periodic penalty to be encouraged to take remedial action.
- It determined that the breach is serious in nature and the SP has not taken any steps nor committed to remediate the failure.
- Whether the SP is already subject to a Directive to take corrective actions, and the required enhancements are not being effectively acted upon.
- Whether the SP is late in providing information which is essential for the FIAU to fulfil any of its functions.

When imposing a periodic penalty, the CMC decides the value of the daily penalty imposed. This is established by considering factors including:

- The extent to which the SP has committed to taking the necessary remedial actions to ensure compliance with its legal obligations.
- The seriousness of the breaches determined, as well as the impact caused to the SP's operations, the jurisdiction and Union, by not taking the necessary immediate corrective actions.
- The reasons for non-compliance with the applicable legal obligations.
- Whether the SP has gained financially or third parties have lost in view of the delay in complying with its AML/CFT obligations, where this can be determined.
- The financial strength of the SP.

Based on these considerations, the Committee decides:

- The value of the periodic penalty.
- The application period for the determination of the final penalty.
- The fact that the periodic penalty is to continue to accrue until a specified condition is met.
- The date from when the penalty starts to accrue (which is to be reasonable).

- The condition which will stop (or pause) the accrual of the daily penalty.
- The manner in which the SP is to notify the FIAU of the fulfilment of the condition.
- Any capping of the penalty.

3.1.3 Method of Payment

An administrative penalty is to be paid as a lump sum. However, following due consideration of the SP's financial strengths, the Committee may, upon request, consider the payment of the said penalty by instalments. In determining the repayment period, the Committee must ensure that the penalty remains effective and proportional to the circumstances.

3.2 Directives requiring corrective actions

A Directive requiring corrective action is an essential non-pecuniary measure that requires the SP to take specific actions as directed to remedy the identified breaches and ensure compliance with AML/CFT obligations under the Act, Regulations and binding guidance issued by the FIAU. Directives bind the SP to take action to implement or improve AML/CFT policies, processes, or controls and/or to rectify or enhance their implementation, to achieve an effective AML/CFT system. Directives may also require attending AML/CFT training and enhancements to technological and human resources.

Directives to take corrective actions are an important tool to drive compliance. Therefore, the CMC has the power to issue Directives together with an administrative penalty or any other measure imposed.

The Committee may determine that the materiality of either a single failure or a combination of failures does not warrant imposing an administrative penalty. However, the CMC still ensures that any failure is addressed and future compliance is achieved. Therefore, the Committee may decide to issue a directive as a standalone administrative measure. This may be the case when the breach relates to:

- The SP's policies and procedures do not comprehensively address all key AML/CFT obligations, but the failure is not considered to be material.

- Controls are not fully commensurate with the SP's risk exposure.
- The SP applies controls and measures that are adequate to fulfil its AML/CFT obligations, but fails to document them.
- Failures relate to obligations that do not significantly impair the SP's understanding of its customers and their activities (such as failures relating to the verification of personal details or those relating to the non-application of policies, procedures or measures with respect to an insignificant number of customers).
- Depending on the size and nature of the SP, its documented business risk assessment does not cover all relevant risk factors. However, the SP demonstrates a comprehensive understanding of the risk factors and how they can expose its activities to ML/FT risks, and more importantly, has implemented the necessary controls.
- Staff require more tailored AML/CFT training.
- Any other deficiency noted by the Committee that may be sufficiently addressed through a directive.

There are two types of directives the Committee may impose:

1

Follow-up directives: These are more intrusive in nature, with Enforcement Officials being more actively involved and having a higher level of interaction with the SP implementing a follow-up directive. This would customarily include conducting meetings, reviewing sample files, and interviewing relevant personnel. In some cases, these checks may also be carried out on-site at the premises of the SP.

2

Remediation directives: These are less intrusive, and the level of Enforcement Official involvement depends on the extent of the remediation required. For minor issues, a declaration of compliance may be sufficient. For more significant issues, Enforcement Officials may hold additional meetings and perform a limited sampling of customer files to ensure corrective actions are being implemented.

More detail on the Directives requiring corrective actions may be found in the 'Corrective Actions Paper' on the FIAU website: [Corrective Actions Paper – June 2025](#).

3.2.1 Closure of Directives

The CMC is responsible for determining whether a SP has successfully adhered to a follow-up or remediation directive. A directive for closure is discussed at CMC only after a two-phase evaluation and only after the Enforcement Section is satisfied that the SP has undertaken effective and sustainable remediation. The outcome of a Directive is also to be communicated to the FIAU's Supervision Section and to the SP's prudential regulator.

Even if a Directive is completed, the CMC may still guide the SP to implement additional improvements to ensure the full sustainability of the remedial actions undertaken and comprehensive adherence to their legal obligations.

The Committee may decide that a directive is partially or fully closed with reservations. This means that although the CMC is generally satisfied with the remedial actions, it has reservations about specific aspects of the corrective actions undertaken. This is also to be communicated to the FIAU's Supervision Section, as well as to the SP's prudential regulator. This may trigger the Supervision Section to perform a new supervisory review to assess in more depth the implementation of effective controls against ML/FT risks.

3.2.2 Escalation to CMC during Directive implementation monitoring

At any point in time where the Enforcement Section believes that the SP is not genuinely and actively trying to ensure that it satisfies the requirements of a Directive, including by implementing the required action items or adhering to the timeframes imposed, or is otherwise not cooperating with the Enforcement Section, the case is escalated to the CMC which may decide to impose any other administrative measures as highlighted in this Guide. This may include the imposition of an administrative penalty, a daily pecuniary penalty, and a recommendation to the prudential regulator for any possible further regulatory action as deemed appropriate by the prudential regulator. Depending on the severity and materiality of the actionable items not adhered to, the CMC decides the most appropriate action.

3.3 Written Reprimands

A reprimand, which takes the form of a formal written warning, is intended to communicate to the SP that although the breach is not of particular concern and did not necessarily give rise to significant consequences or expose the SP or the jurisdiction to risks of ML/FT, it is nonetheless unacceptable and should not be repeated. This may be the case, for instance, when a breach appears infrequently and does not affect the SP's controls/mitigating measures or otherwise expose the SP to ML/FT risk.

Written reprimands impinge on the SP's compliance history and are thus taken into consideration by the Committee when assessing any future cases of non-compliance.

3.4 Publication of Administrative Measures

Article 13C of the PMLA requires the FIAU to publish all the administrative measures imposed by the Committee. Publications play an important role in ensuring SP accountability in complying with AML/CFT obligations. They are crucial to make administrative measures issued by the Unit dissuasive and to prevent non-compliance by other SPs by raising awareness of their AML/ CFT obligations.

Publications are anonymous in all cases where the administrative measure either does not include a fine or includes a fine not exceeding €50,000. Administrative measures that include a penalty exceeding €50,000 include details identifying the SP subject to the measure. However, and as explained in the *Publication of AML/CFT Administrative Penalties and Measures Policies and Procedures* as well as in terms of Article 13C of the PMLA, there may be instances where an administrative measure is not published or otherwise this is published anonymously even if there is a penalty in excess of €50,000.

All the details included in the publication, as well as when updates to the publication are to be made, are explained in the *Publication of AML/CFT Administrative Penalties and Measures Policies and Procedures*, available on the *FIAU website*.

3.5 Recommendations or notifications to other regulatory/supervisory authorities or other bodies.

Article 13 of the PMLA and Regulation 24 of the PMLFTR require that the FIAU notify the respective EU supranational bodies and the domestic prudential regulator or body of any enforcement action taken.

Where the SP forms part of a larger group in a foreign jurisdiction, the Enforcement Section may also notify the foreign AML/CFT Supervisor/s of the administrative measure imposed on the domestic SP.

In addition to these notifications, when deemed necessary, the Committee may also:

- i) Recommend that the prudential regulator or body consider taking further administrative measures to ensure proportionate action is taken in response to the risk arising from the identified breaches.
- ii) Highlight potential prudential or governance concerns that are beyond the FIAU's remit by issuing a recommendation for the attention of the prudential regulator or body.

More detail on the collaboration between the Enforcement Section and other authorities may be found in **Section 6** of the Guide.

The following are examples of findings or breaches that may be relevant to the aforementioned authorities or bodies:

- Serious, systematic and/or repetitive breaches that materially impact the reputation of the sector/ jurisdiction/EU.
- The remedial action requires considerable time and/or resources, leading to high exposures to serious unmanaged risks.
- Failure to rectify severe breaches or root causes even after a directive is imposed.
- If concerns are identified in relation to the SP's business operations or governance which fall outside the scope of the FIAU.

3.6 Specific recommendations on key persons within the subject person

There may be cases where breaches of AML/CFT obligations by the SP are attributable to wilful conduct or gross negligence of natural persons who are responsible for the management or administration of the SP.

Where the Committee is concerned that the measures it may legally impose might not be sufficient, or it believes that action must be taken by other regulatory/supervisory authorities or bodies responsible for exercising discipline over the SP's senior management officials, the Committee may apart from bringing all the relevant facts of the case to the attention of the respective authority or body, highlight the above concerns in its communications to that authority or body.

This allows the authority or body to assess the case and determine whether further action is necessary. In these scenarios, the Committee may make a specific recommendation to the relevant supervisory/regulatory authority (under which competence that SP falls) to consider taking action to limit or restrict the person's position with the SP, or to take any other action it may deem appropriate.

The following are examples of findings, breaches or situations that may be relevant to the relevant authorities or bodies:

- Cases where senior managing officials of the SP were cognisant of serious or systematic breaches and failed to rectify them in a timely manner or tried to mislead the Authority about the gravity of the failures.
- Findings evidencing serious failures by SMOs, to adequately understand, appreciate, and discharge the fundamental responsibilities of their role in combating ML/FT.
- A senior managing official is charged with or convicted of a serious crime, or the Unit has adverse information in their regard.

3.7 The termination of business relationships

The Committee is empowered to require the SP to terminate a business relationship when there is knowledge or reasonable suspicion that, in connection with a particular business relationship, ML/FT is taking place or has taken place, or else has been attempted, or that the business relationship in question may increase the risk of ML/FT, the Committee is empowered to require the subject person to terminate such business relationship.

The termination of a business relationship would be appropriate where there are no feasible applicable measures (final or interim) that the SP or the Committee can adopt to sufficiently mitigate the risk arising out of a specific business relationship or set of business relationships, and the only plausible way to manage the ML/FT risk is to terminate that relationship.

3.8 Any other administrative action the Committee legitimately directs

The Committee may take any other measure or action that it is legally empowered to take in virtue of its powers at law, if it deems it necessary and appropriate in view of the circumstances and risks observed.

3.9 Interim Measures

The Committee may be informed that during a supervisory intervention, material risks have been identified which the SP is not adequately addressing. When these risks require urgent addressing, the Committee may determine that they must be mitigated without waiting for the conclusion of standard supervisory and enforcement processes.

In these situations, the Committee may adopt interim measures, which are taken before breaches are determined by the CMC. These cannot take the form of administrative penalties but are targeted at managing risk.

The Committee may decide to implement any of the measures explained in **Sections 3.2, 3.5, 3.6, and 3.7** above as an interim measure. This does not preclude the FIAU from taking additional administrative measures to address the past failures committed by the SP to ensure future compliance.

3.10 Lack of clear-cut breaches

There may be cases where, although no clear-cut AML/CFT breaches are identified, the CMC remains dissatisfied with the effectiveness or adequacy of any aspect of the SP's AML/CFT regime. The elements giving rise to the CMC's concern or dissatisfaction may vary depending on the specific circumstances of the case and as such can only be assessed and determined on a case-by-case basis. In these circumstances, the CMC is to consider whether a follow-up or remediation directive is required to address that concern.

Over-arching considerations.

To determine the administrative measure(s) to impose, the Committee considers the following:

i) Seriousness of the Breach

This is established by understanding the gravity as well as the consequence or potential consequence of a breach. This is determined by considering:

- The importance of the obligation that was breached.
- The duration of the breach.
- The value and volume of transactions processed and the extent to which these transactions were allowed to be processed in view of the breaches committed.
- The extent to which the SP was proactive in taking the necessary remedial measures.
- The overall level of regard towards ensuring good and effective AML/CFT controls.
- The extent to which the breach was committed as a result of the behaviour, decision-making or attitude of senior management.
- The consequences or damage resulting from the breach, including risks of facilitation of ML/FT, and the possible reputational impact to the jurisdiction or the European Union

ii) Systematic nature of the breach

A breach is considered systematic when there is a failure in the SP's broader systems, controls, or culture, leading to structural issues rather than isolated one-off failures. Therefore, the result of a systematic breach is more widespread. This can be caused either because a SP's own policies, procedures or measures implemented are in themselves systematically deficient or otherwise, while the policies, procedures and measures are correct, their implementation as observed from the sample of files reviewed, or from other documentation, was systematically deficient.

iii) Repetition of the breach

This refers to the recurrence of the same or similar breach of the AML/CFT obligations, where the failure has been previously identified and should have been addressed. Therefore, it highlights that any previously implemented remedial action was neither sustainable nor effective in addressing the root cause of the problem, leading to the repetition of the breach.

Section 4: The Sanctions Calculation Tool

Section 4:

The Sanctions Calculation Tool

To ensure uniformity in the application of administrative penalties and to guide it through a more consistent approach, the Committee uses a Sanctions Calculation Tool (SCT). The SCT provides the CMC with the administrative penalty to consider imposing for each individual breach confirmed. The Committee takes into account several aggravating and mitigating factors attributed to the SP's operations and the case specifics. The SCT also provides a final aggregate amount that the Committee should consider in its final deliberations in deciding what penalty to impose for all the breaches observed in the case.

The SCT is designed to ensure that a penalty calculation results in a fine that is legally permitted in terms of the PMLFTR. However, the Committee may, at its discretion and in line with the considerations highlighted in the Sanctions Policy, in view of considerations that are specific to the circumstances of the case, decide to increase or decrease the administrative fine determined through the SCT. In these cases, the Committee ensures it has a justified reason for varying the amount and that such justification is duly documented.

The SCT safeguards the principle of proportionality to ensure that not only material failures result in a higher administrative penalty, but that this is also proportionate to the size of the SP. Also, the tool ensures that repeated failures increase the administrative penalty.

The Sanctions Tool is split into two main components that consider various factors:

1

Breach focused component – consists of factors specific to the obligation breached by a SP. These include a determination of the level of seriousness of the breach committed by a SP, the extent to which the breach is a one-off circumstance or is indicative of systematic and repetitive failures, the duration of the breach and the domestic and/or foreign impact of the breach.

2

Overall considerations component – takes into account aggravating or mitigating factors aimed at assessing the overall level of compliance by the SP. These include a consideration of the SP’s profile in terms of overall level of compliance, remediation undertaken, extent of cooperation, regard and commitment to AML/CFT obligations. In addition it considers, the size of the SP relative to the sector it operates in, the possible risks to ML/FT facilitation caused by the lack of controls implemented, any action taken by other Authorities on the SP in view of unmanaged ML/FT risks or otherwise because of prudential or governance concerns, and the extent of the SP’s financial stability.

In determining the administrative measures, including any penalty to impose for operational breaches, the CMC utilises a different mechanism that is more specific to the different operational breaches being addressed. This mechanism takes into account specific factors, including but not limited to the instances where the SP has been found in breach, the days late (if applicable), the period of non-reporting, any instances of repeated failures, and the actions taken to remedy the breach, if any.

4.1 Three Pillar Considerations

An overview of the considerations built into the sanctions tool is provided hereunder:

4.1.1 Pillar 1: Gravity and Impact of the Breach

As part of its deliberations, the CMC determines which findings should be pursued as breaches of AML/CFT regulations. All confirmed breaches are subsequently recorded in the SCT.

In determining the base amount of the penalty to be imposed per breach identified, the SCT has been calibrated to consider the following breach-specific considerations:

i) Seriousness

While all AML/CFT obligations are important and need to be adhered to, breaches of AML/CFT obligations carry varying degrees of seriousness. Therefore, each AML/CFT obligation at law has been weighted depending on how severely the non-compliance undermines the effectiveness of controls in preventing ML/FT. By way of a clear example, the most onerous obligation is to report to the FIAU suspicious behaviour/activity/transaction. Therefore, this carries the highest weight. On the other hand, the failure to verify the registered/residential address of a customer, while still important, carries much less weight.

ii) Qualitative (systematic) and Quantitative (repetitive)

The SCT also considers whether there is a structural failure caused by the breach with regard to AML/CFT systems and controls and policies, or a failure of the entity to put these in place adequately. The following guides the Committee in its selection.

For qualitative failures, the Committee considers the extent of any systematic failure. The complete absence of a policy, process or system is considered a significant systematic failure. This includes situations where a policy/procedure is missing, both in documenting and in practice, as well as cases of disregard by senior management towards important AML/CFT requirements.

There may be situations where the Committee considers a failure to be moderately systematic. This occurs when a policy/procedure is in place, yet the failures identified are not minimal and undermine its effective implementation. For example, the SP may have implemented a transaction monitoring system, which does not capture various material products the SP offers; Therefore, its implementation is neither truly effective nor comprehensive.

The CMC needs to have some degree of objective judgement when determining the extent to which a failure is systematic, and the extent of these systematic issues. In doing so, the CMC uses its expertise, as well as the FIAU's understanding of how policies/procedures and measures are implemented by peers within the same SP sector.

The SCT also considers the quantitative aspect of the breach, i.e., the number of instances the breach was repeated. Therefore, a one-off instance will have a much lower impact than a situation where most files reviewed have been found in contravention of the legal obligation.

iii) Duration

Classifying the duration of an AML/CFT breach typically involves analysing how long the breach persisted before detection or resolution. For example, if a breach persisted for more than 2 years, it is a material time, as opposed to instances where breaches are detected and resolved in a much shorter period, such as less than 6 months.

iv) Impact on the Jurisdiction

Breaches of AML/CFT obligations impact both a SP's ability to protect its own business from harm but may also have an impact on the jurisdiction at large. This is particularly relevant if the SP has material exposures to the ML/FT threats as observed in Malta's National Risk Assessment (NRA) and the EUs Supra National Risk Assessment (SNRA), and the breaches identified confirm that the SP is not effectively managing these exposures. To quantify the extent of the breach's impact, the tool considers internal information available through CASPAR and the risk assessment carried out by the FIAU on the SP.

The impact of specific AML/CFT breaches on the jurisdiction may be further amplified or reduced depending on the following transaction-related factors:

1) Transactions processed/exposed without effective controls (if applicable)

This aims to cover the transactional activity that has been allowed to pass through a SP's system as a result of shortcomings or weaknesses in the controls implemented. To understand the extent of this, the transactions allowed in view of weak/ineffective controls is seen as a percentage of the total transaction volume that has been assessed during the supervisory review. This may lead to an increase in the impact on the jurisdiction.

2) Egregious transaction (if applicable)

This aims to cover risks from processing egregious transactions that stand out in comparison to transactions traditionally processed by the subject person. When the Committee determines that egregious transactions have been processed without the necessary supporting documentation or clarifications, it considers the extent to which the egregious transaction stands out.

If the Committee determines that the subject person has processed egregious transactions without adequate scrutiny, the CMC is to consider increasing the 'Jurisdictional Impact' of specific impacted breaches.

v) Impact on the group, cross border or Union

To the extent that it applies to the SP and as deemed relevant, the CMC also considers the actual or potential impact of the breach on the at group, cross-border or within the Union.

Outcome of Pillar 1: Breach Category & Penalty Base Amount

Depending on the outcome of all the factors considered under Pillar 1, the breach is automatically classified into one of four categories:



Category 1: A breach with minor gravity and impact.



Category 2: A breach with moderate gravity and impact.



Category 3: A breach with significant gravity and impact.



Category 4: A breach with very significant gravity and impact.

4.1.2 Pillar 2: Regard to AML/CFT obligations

This pillar considers the overall regard the SP has towards its AML/CFT obligations, both before and after the compliance review. It includes the SP's overall level of compliance and a list of aggravating and mitigating factors tied to the case under discussion.

Overall Level of Compliance

Consideration is given to the overall level of compliance by the SP. This aims to assess the extent to which the SP is compliant with its AML/CFT legislative requirements. In doing so, the tool considers the totality of the failures which are serious, systematic or repeated (as defined in Pillar 1). The following criteria are taken into consideration:

Aggravating Factors

To set the level of pecuniary sanctions, the Committee considers any of the following aggravating factors:

- SP has not cooperated with the Authority when carrying out its review.
- The breach was intentionally committed: the SP appears to have known about the breach and took no action, or else took a course of action that generated the breach.
- The SP has not remediated, nor is there a commitment to remediate.
- The same breach had already been identified by the CMC following a previous supervisory intervention.

Mitigating Factors

To set the level of pecuniary sanctions, the Committee considers any of the following mitigating factors:

- The SP's senior management has taken all reasonable measures to prevent the breach from happening.
- The SP voluntarily took measures to ensure that similar breaches cannot be committed again in the future.
- The SP promptly and effectively brought the complete breach to the FIAU's attention.

4.1.3 Pillar 3: Size of the subject person

The size of the SP impacts the overall administrative penalty, considering that the larger the size, the greater the potential exposure to ML/FT risks requiring more robust controls.

The size acts as a mitigating factor, and the penalty amount is applied proportionately to the size of the SP. The following is a non-exhaustive list of criteria that are taken into account during the calculation of the sanction, in accordance with the nature of the SP's business activity:

- **Turnover:** This refers to the turnover generated from all the SP's activities during the period in which the breach occurred. If it persisted over multiple years, the cumulative turnover generated throughout those years may be considered. In a group context, the Committee may also take into account turnover generated at the group level.
- **Income:** The income generated from all activities carried out by the SP during the period in which the breach occurred. If it persisted over multiple years, the cumulative income generated throughout those years may be considered. In a group context, the Committee may also take into account the income generated at the group level.
- **Customer size:** Is the average of the active customer numbers across the years in which the breach was committed.

4.1.4 Final Considerations

Once pillars 1, 2, and 3 are completed, the Committee considers whether additional adjustments to the penalty amount are due by considering the following, where applicable:

Profits earned/losses avoided by the breaches committed

If the SP made a profit or avoided a loss as a result of the breach, it should not be permitted to benefit from the breach. Where this can be determined, the administrative penalty imposed by the Committee should, as a minimum, be equal to the amount of benefit derived or loss avoided, unless this amount is higher than the maximum penalty that the Committee is empowered to issue.

However, the Committee ensures that it holds the necessary evidence to confirm the amount of benefit derived/loss avoided before proceeding to impose any such amount. If the amount is not evidenced, then the usual procedure to determine the amount of fine to impose is to be followed. Evidence may include, but is not limited to, correspondence, invoices, contractual relationships and transactional information between the SP and its customer(s).

Impact on third parties, customers and other market users

The Committee is to consider the losses caused to third parties as a result of the breaches, and the loss or risk of loss caused to customers or other market users, as far as these can be determined. Where this is quantifiable, the administrative penalty imposed by the CMC should, as a minimum, be equal to losses to third parties caused by the breaches, unless this amount is higher than the maximum penalty that the Committee is empowered to issue.

The CMC ensures that it holds the necessary evidence to confirm the losses to third parties or customers or market users caused by the breaches before proceeding to impose any such amount. If the amount is not evidenced, then the usual procedure to determine the amount of a fine to impose is to be followed. Evidence may include, but is not limited to, correspondence, invoices, contractual relationships and transactional information between the SP and its customer(s).

Actions by other Authorities

In the case of any action taken by other Authorities for the AML/CFT breaches committed by a SP, the CMC will determine whether the quantum of the penalty needs to be adjusted to ensure proportionality of the enforcement action being imposed.

Proportionate, Effective and Dissuasive

Finally, the CMC shall always ensure that the resulting administrative penalty is regarded as proportionate, effective, and dissuasive. If adjustments are required, the reasons for these adjustments must be documented.

Section 5: Communication with the subject person

Section 5: Communication with the subject person

Once the enforcement process is initiated, the SP is formally notified through the ENL and is provided sufficient detail as to the process, timeframes and CMC Members involved in deciding on the potential breaches that had been observed.

Details of the IPM (when requested) are communicated well in advance, and clear opportunities for further representations are formally provided.

Once the Committee has reached a determination regarding the existence of one or more breaches and the corresponding administrative measures to be imposed, the outcome is formally communicated to the SP by means of a sanction letter. This letter is the official notification of the Committee's determination and the administrative penalties and/or measures being applied as a result.

The breaches, shortcomings or concerns are clearly and distinctly listed in the sanction letter. The CMC identifies the specific provision/s of the law, Implementing Procedures or Guidance Notes that have been breached or are linked to identified concerns. The sanction letter sets out in detail the reasoning behind the Committee's decision/s, including a clear explanation of how the breach or breaches were established based on the documentation and applicable regulations. It also outlines how any SP representations or submissions were duly considered during the Committee's deliberations. Furthermore, the letter provides a comprehensive description of the specific administrative measures imposed.

Where the CMC determines that the imposition of a daily penalty is required, it ensures that this is clearly communicated to the SP, including the necessary details for the SP to understand the value, the timeframes and what actions are required to carry out the necessary corrective actions and cease the accrual of the daily penalty.

When the CMC determines that a directive to take corrective actions is needed, the SP is officially notified through the sanction letter. The sanction letter clearly sets out the purpose of the directive and its nature (i.e. whether it constitutes a follow-up directive or a remediation directive) and specifies the actionable steps required to restore compliance with the applicable AML/CFT legal obligations.

Where a follow-up directive is issued, the sanction letter highlights that all case-specific communications and discussions about the action plan are to be conducted through the Enforcement Section, which has the discretion to agree on the details of the action plan. The sanction letter also includes a standard action plan template to ensure that all required information is duly provided by the SP.

Where a remediation directive in the form of a declaration of compliance is issued, the sanction letter likewise includes a template to guide the SP on the information to be included in the declaration.

When communicating the administrative measure(s) imposed, the sanction letter clearly explains that additional action may be taken by the CMC, both if similar or other failures are identified in the future, as well when determining that the required corrective actions have not been implemented.

Where applicable, the prudential regulator is also provided with a copy of the sanction letter.

If the Committee concludes that it may proceed with offering Settlement, the Settlement Letter provides sufficient detail for the SP to understand which breaches it has committed as well as the remedial actions required. The Settlement Agreement also provides sufficient detail for the SP to understand the initial amount of the administrative penalty, as well as the reduction applied and the conditions for the reduced amount. During the settlement meetings, the SP is provided with sufficient detail to understand the final outcome of the terms of the settlement being agreed to.

Section 6: Cooperation with Prudential Regulator

Section 6: Cooperation with Prudential Regulator

Over the years, the FIAU has established a range of informal and formal procedures in collaboration with other domestic regulatory authorities, covering various areas, including matters related to enforcement. These procedures intend to enhance cooperation between the FIAU and other competent authorities, with the overarching objective of protecting the interests of end consumers and safeguarding the integrity of the financial system.

The following section outlines selected processes and aspects falling within the scope of these procedures, providing practical examples of the cooperative efforts undertaken.

6.1 Decision Letters

When the FIAU issues a letter outlining the outcome of a recently conducted examination, it informs any other authority that may be impacted by this action. This ensures that all relevant authorities are promptly apprised of information that may affect their supervisory or enforcement responsibilities, thereby enabling them to take informed decisions and implement any necessary actions in a timely and effective manner.

6.2 Prudential Concerns

During the conduct of its routine operations, the FIAU occasionally identifies prudential-related concerns associated with specific SPs holding licences or an authorisation issued by, and falling within the regulatory scope of, Malta's regulatory regime, including but not limited to the MFSA and the MGA. These concerns are conveyed to the relevant regulator on an ad-hoc basis by means of formal written communication. This communication brings to the regulator's attention information that may be of interest and relevance to its mandate, especially issues that are of a prudential or licensing/authorisation nature.

Specifically for communications with the MFSA and MGA, Prudential concerns referred to them are classified into three categories according to their materiality.

**Category 1**

Covers the most severe cases involving serious, repeated, or systematic breaches where the SP's capacity to remediate is believed to be jeopardised.

**Category 2**

Includes matters that, while not necessarily systematic, pose significant and/or insufficiently managed ML/TF risks, such as loss or manipulation of client data, provision of false or misleading information, interference with AML/CFT functions, or refusal to cooperate on corrective actions.

**Category 3**

Covers less AML/CFT focused concerns but still very relevant prudential issues, including unlicensed activities, breaches of licence conditions, weaknesses in governance, risk management or financial soundness.

Cases exhibiting potential criminal elements or suspicion of money laundering or terrorist financing are promptly escalated to the FIAU's Intelligence Section and/or law enforcement and other competent authorities through pre-established channels and operational arrangements.

6.3 Joint Action

There may be situations where, due to the nature of the case and the materiality of the concerns identified, the FIAU, in collaboration with one or more other relevant authorities, may decide to take joint action with respect to a particular SP. This collaborative approach typically arises when the complexity and seriousness of the issues at hand warrant coordinated efforts from multiple regulatory bodies at the national level. A common form of such joint action involves the initiation of a joint examination or a review into the same SP, facilitating a comprehensive and multifaceted review from different fronts. However, this course of action should not be considered the standard or expected procedure in most cases.

6.4 Exchange of Information

The FIAU remains committed to continuously exploring opportunities for cooperation with other authorities across a broad range of areas. This cooperation is reflected through regular meetings where the authorities exchange information on ongoing reviews and conduct information sharing activities. Matters concerning specific subject persons and regulatory developments that may affect their respective mandates are also discussed.

These meetings also provide a forum for discussions on potential training and educational initiatives for officials across the participating authorities, as well as opportunities for joint training sessions that may be offered to SPs.

Section 7: Enforcement Lifecycle

Section 7: Enforcement Lifecycle

The enforcement lifecycle encompasses a series of procedural steps followed by the FIAU from the notification of a potential breach to the SP through to the final resolution and closure of the enforcement action, including any required corrective actions.

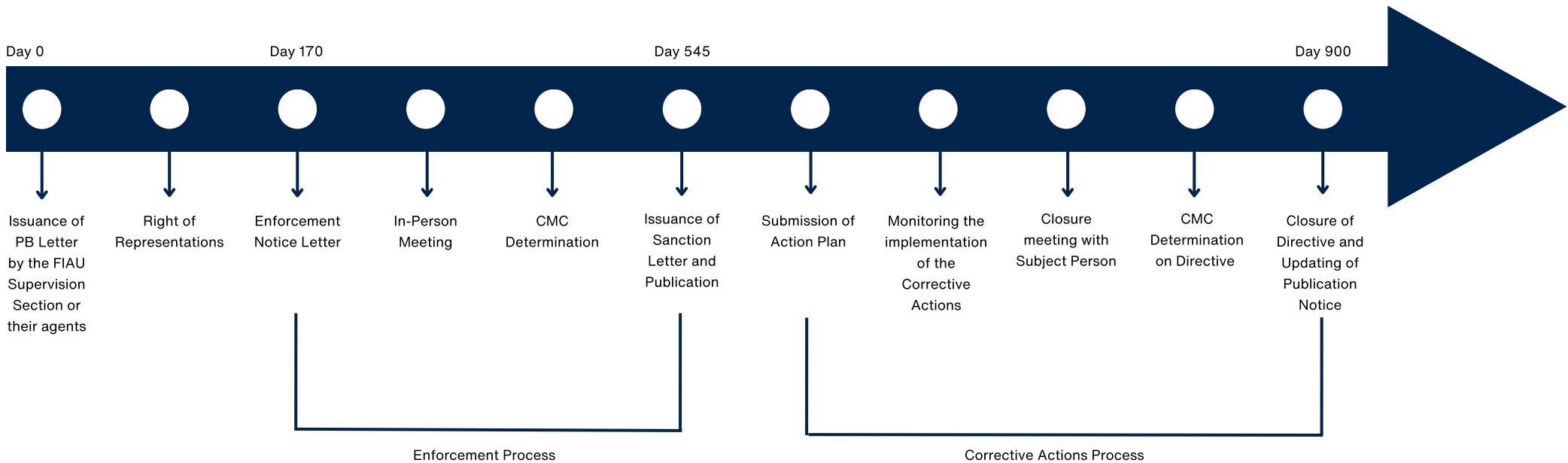
It starts from the date of the potential breaches letter up to the closure date of the directive to take corrective actions. Where no directive is issued, the enforcement lifecycle runs until the date of the sanction letter explaining the CMC's decision. Where an appeal has been instituted by the SP, the enforcement lifecycle is halted until such time as the appeal has been decided. A directive to take remedial action can be initiated and closed even during the appeal proceedings. The court appeal proceedings is excluded from the Enforcement Lifecycle since this is not directly dependent on the FIAU's resources and procedures.

The Enforcement Lifecycle depends on various considerations, including:

- The extent of the scope of the supervisory intervention.
- The extent of the seriousness of the findings identified following the supervisory intervention.
- The extent of the representations submitted by the SP, together with any requests for extensions.
- The ease with which an in-person meeting date can be set.
- The extent to which the subject person has already initiated/completed remedial actions.
- The extent to which the remedial actions necessary are implemented, and the cooperation throughout the remedial process.
- The extent to which remedial actions have been effectively implemented and tangible progress has been achieved.

Based on current practices and experiences, the diagram below highlights the average enforcement lifecycle for a standard case. It should, however, be noted that there may be factors, both within and outside the FIAU's control, which may result in the enforcement lifecycle extending beyond the anticipated timeframes. Accordingly, the timeframes set out above are only indicative and intended to provide a general illustration of the average duration of the process, not a definitive or binding expectation.

Enforcement Lifecycle for a Standard Case



Section 8: Appeals

Section 8: Appeals

In terms of Article 13A of the PMLA, SPs have the right to appeal administrative penalties imposed by the FIAU when the penalty exceeds Euro five thousand (€5,000). The appeal needs to be filed before the Court of Appeal (Inferior Jurisdiction) within 20 days from notification of the administrative penalty. Once an appeal is filed, the penalty is not final and due, thus not enforceable. Any follow-up actions the SP carries out are undertaken on a 'without prejudice' basis to the pending appeal and thus cannot be used as evidence during the appeal proceedings. In fact, it is the norm for the SP to proceed and comply with the follow-up directives to enhance their AML/CFT control framework, independently of any appeal proceedings.

Once the FIAU is served with an appeal by an SP from one of its administrative decisions, the thirty (30) days for the filing of its reply start running.

Within a reasonable time from the service of the appeal application, the FIAU must submit the case documentation folder to the Court and provide a copy to the subject person during the first sitting. This folder includes, *inter alia*, all information and documents used by the FIAU Supervision Officer (or MFSA/MGA officers acting as agents) to identify potential breaches when drafting the Potential Breaches Letter, as well as all material considered by the CMC when reaching its final decision.

Once the FIAU is notified of an appeal, the Publication Notice on the FIAU's website is amended to show that an appeal has been lodged. A short description of the appellant's grievances is given, together with an indication of the appellant's request to the Court. This is done within five days of the notification, and in line with the FIAU's Publication Policy (Publication of AML/CFT Administrative Penalties and Measures Policies and Procedures).

When the appeal judgment is delivered, the Publication Notice is again amended with the Appeal Decision Notice, containing a short description of the Court's decision, i.e., a clear indication of whether the administrative penalty was revoked in whole or confirmed in its entirety, and when a penalty is revoked in part, which parts of the administrative penalty were altered or revoked.

This amendment is made no later than five days following judgment in line with the Publication Policy. Where the administrative penalty is revoked entirely or is reduced to the extent that its value no longer exceeds Euro fifty thousand (€50,000), the name of the SP is removed from the Publication, to reflect the anonymity requirement for administrative penalties not exceeding Euro fifty thousand (€50,000).

Conclusion

Conclusion

This Enforcement Guide intends to promote transparency, consistency, and fairness in the enforcement process. By outlining applicable standards, procedures, and expectations, the Guide serves as a resource for SPs, other stakeholders involved in AML/CFT, and the public. While this Guide provides general direction, each case is evaluated on its specific facts and circumstances, and the FIAU, through the CMC, retains discretion to take appropriate action in accordance with applicable laws and regulations. This Guide may be updated as necessary to reflect changes in law, policy, or practice.

Annex I

List of Documents

1. Common Issues Related to the Money Laundering Reporting Officer.
2. Corrective Actions Paper – June 2025.
3. Governing Principles and Framework.
4. Implementing Procedures Part 1.
5. Optimising Subject Persons' Representations.
6. Publication of AML/CFT Administrative Penalties and Measures.
7. Settlement Policy.

© Financial Intelligence Analysis Unit, 2026

Reproduction is permitted provided the source is acknowledged.

Questions on this document may be sent to:

[*enforcement@fiaumalta.org*](mailto:enforcement@fiaumalta.org)

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

Telephone: (+356) 21 231 333

E-mail: info@fiaumalta.org

Website: www.fiaumalta.org