



www.21Academy.education

1

Introduction to Anti-Money Laundering (AML) and Funding of Terrorism and understanding the impact of non- compliance

19th November 2020

Luke Mizzi

CAMILLERI PREZIOSI
ADVOCATES

2

Agenda

- The Money Laundering Reporting Officer
- The Monitoring Function

Introduction

Subject persons are required to have internal and external reporting procedures in place to report any knowledge or suspicion of ML/FT to the FIAU and any knowledge/suspicion that funds or property are the proceeds of criminal activity.

THE MONEY LAUNDERING REPORTING OFFICER

The Role of the MLRO

Subject person is to appoint one of its officers as the MLRO whose core functions are to:

- ❖ receive reports from the subject person's employees of knowledge or suspicion of ML/FT, or that a person may have been, is or may be connected with ML/FT;
- ❖ consider these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT;
- ❖ report knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FIAU; and
- ❖ respond promptly to any request for information made by the FIAU.
- ❖ act autonomously, if necessary without reference to or undue influence from management.

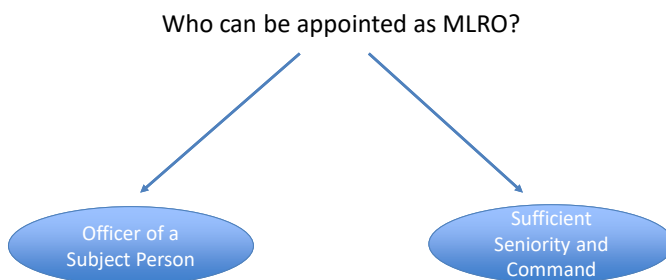
Additional features of the role

- Keeping up an internal register of both internal and external STRs
- Maintaining documentation of the MLRO evaluation and determination process in respect of STRs and other investigations
- The regular generation of management information (MI) on internal and external STR reporting trends
- Cultivating an awareness of developing money laundering typologies
- Remaining up to date with AML/CTF legislation as per guidance released by the FIAU
- Monitoring the internal effectiveness of the AML/CTF procedures
- Being aware of countries that do not have adequate AML/CTF frameworks in place
- Being aware of the content of lists of suspects and sanctions issued by law enforcement and regulatory authorities
- Contributing to the content of staff training, whilst also maintaining a sustained high level of staff AML/CTF awareness between training sessions
- Preparing for and dealing with regulatory visits and inspections

Key skills and qualities of an effective MLRO

- Capability to identify, quantify and manage risk
- An intimate knowledge and understand of the organisations products and services as well as the typical customer profile
- The ability to recognise potentially suspicious activity
- Absorb and analyse information, usually under pressure
- Capacity to recognise if additional information is required before any reporting decisions are made
- Excellent verbal and written communication skills
- Staff should feel comfortable in approaching and discussing any concerns with the MLRO
- Possessing the confidence to make and substantiate decisions
- Being able to take decisive decisions

Appointment of MLRO



Officer as a Subject Person

For identifying an individual to be appointed as MLRO, there must subsist an employment relationship between the officer and the subject person, such as:

- An officer in employment or
- An executive director of the subject person

However, the functions of a MLRO **cannot be**:

- Outsourced
- Carried out by a non-executive director of the subject person
- Carried out by a person who merely occupies the position of company secretary of the subject person and does not hold any other position within the organisation, or
- Carried out by a person who undertakes internal audit functions within the organisation

Officer as a Subject Person

There are also situations where the person appointed as MLRO need not be an officer in employment or executive director, such as:

- an insurance company managed by a company that is enrolled to act as an insurance manager in terms of the Insurance Intermediaries Act.83.
 - Here, a company may enter into an arrangement with the insurance manager to have the duties attributable to the MLRO of the insurance company carried out by the MLRO of its manager;
- a collective investment scheme that is subject to the PMLFTR and that does not have a physical operational set-up in Malta other than a registered address and a board of directors, does not engage any employees and is not involved in the acceptance and processing of subscriptions and the collection of funds from investors.
 - Here, the duties attributable to the MLRO can be carried out by the administrator's MLRO.
- a group comprising two or more subject persons that can avail themselves of the exemptions allowed in terms of Regulation 16(2)(b) and (c).
 - Here, subject persons may designate one of their employees as the group-wide MLRO, with each individual subject person considering whether the appointment of a designated employee is necessary to assist the MLRO to meet his/her functions effectively; and
- a group comprising two or more subject persons, it is possible for the employee of one subject person to be seconded with another subject person forming part of the same group to act as its MLRO. When the group also includes an entity to which subject persons within the group have delegated fulfilment of their AML/CFT obligations, it is possible for an employee of sufficient seniority and command within that entity to be seconded with a subject person within the group as its MLRO.

Only if administrator is recognised under ISA + administrator is subject to authorisation/licensing /recognition of an EU MS and subject to AML/CFT obligations

Factors influencing the choice of the MLRO

- The decision as to who should be given the responsibility of the MLRO role, within an organisation should be taken by following three stages;
 - i. Decide on the scope of the role and the various aspects of it
 - ii. Identify the key skills required to discharge the role competently
 - iii. Taking into account the first two points, decide who is the most appropriate person for the role.
- Other factors include:
 - Size and nature of the organisation
 - Scope of the role as defined by the FIAU
 - The organisations products are services
 - The seriousness with which the organisation regards its AML/CTF obligations
 - The person's ability to operate at a senior level and have the respect of the firm's senior staff as that of regulatory agencies.
 - Whether an individual can be trusted not to under or over-report

Sufficient Seniority and Command

MLRO:

- must occupy a senior position within the institution
- must be able to communicate directly with the Board of Directors
- must have the authority to act independently in carrying out his/her responsibilities + full access to all records, data, documentation and information of the subject person for the purposes of fulfilling his/her responsibilities

When the subject person is a sole trader or a sole practitioner with no employees or no persons working within his/her practice, the subject person must carry out the functions of MLRO himself/herself.

Case study: the need for an MLRO to be of seniority

- An MLRO (an associate director) of a bank branch in Malta, receives an internal STR from an employee, in relation to an account held by a high-net worth individual. Large deposits are held and managed by the bank.
- The basis of the STR compiled revealed that the customer made a couple of high value transactions towards a country the has known AML/CTF deficiencies.
- Upon reaching out the relationship manager (RM) a sufficient explanation was not given. Instead, the RM stated that these payments were genuine.
- Not being satisfied with this response, the employee who submitted the STR decided to carry out further investigation. It was then identified that the jurisdiction is known to harbour terrorists.
- The basis of the STR was in fact that the customer might be involved in some sort of terrorist-financing.

Case study: the need for an MLRO to be of seniority

- The MLRO then decides to speak to the RM, who reiterates there is no rational explanation for the transfers.
- The RM, who happens to be the local managing director of the bank, explained that such questions to customers will make them opt for banking alternatives. He also stated we should refrain from interfering in customer's activities.
- From this example we learn that the given the superiority the managing director holds, the MLRO is now hesitating to do the right thing and file an external STR to the FIAU.
- The harsh reality is that MLROs sometimes find themselves in such situations and taking the necessary actions may not go down well with some colleagues.

Therefore, the autonomy to make such decisions in good faith, without constraints or undue commercial influence, ordinarily requires the MLRO to have sufficient seniority.

Appointment and Resignation of MLRO

Appointment:

- MLROs are to register themselves on the FIAU's Compliance and Supervision Platform for Assessing Risk (CASPAR), which is accessible through the FIAU's website. (The status of the role of the MLRO as a controlled function requiring the registration of a particular individual is indicative of the seriousness with which the role is viewed by the regulatory authorities. The role therefore needs to be viewed with equal seriousness internally).
- When the prior approval of a supervisory authority is required to proceed with the appointment of the MLRO, the MLRO should register only once the relevant supervisory authority has issued the approval.
- In all cases, the FIAU reviews all new registrations received through CASPAR to ensure that there are no obstacles to proceed with the registration.

Resignation:

- Subject person must notify the FIAU of the resignation/removal of MLRO
- MLRO must notify FIAU if departure was linked implementation of the subject person's obligations under PMLFTR or any regulatory implication that the FIAU should be aware of
- MLRO's account is to be deactivated from CASPAR

DESIGNATED EMPLOYEE

If a new MLRO is pending approval of supervisory authority, the subject person should inform the FIAU and provide the FIAU with details of the employee who for the interim period will be assuming the role of reporting officer.

Common problems that MLROs encounter

- Lack of authority
- Intimidation by senior members of an organisation
- Absence of adequate resources
- Inadequate level of awareness among staff of money laundering risks and their obligations
- The challenge of dealing with internal staff as well as customer when an STR has been made and consent to proceed is delayed
- Poor recording keeping

Example: Wachovia Bank

- In March 2010, Wachovia Bank, settled the biggest action to that the date brought under the US Bank Secrecy Act. It paid federal authorities \$110 million in forfeiture for allowing transactions later proved to be connected to drug smuggling, and incurred a \$50 million fine for failing to monitor cash used to ship 22 tons of cocaine.
- A shocking detail that emerged from the case was the fact that a London-based MLRO, flagged the transactions back in 2006. However, he was scolded by management for submitting STRs.
- Similar to the case study, the MLRO was intimidated by senior management instead of being praised.
- Some of the most harmful problems encountered by MLROs originate from the territorial mindset of CRMs, or directors who are mainly driven by monetary incentives and their roles to generate and retain valuable customer relationships.

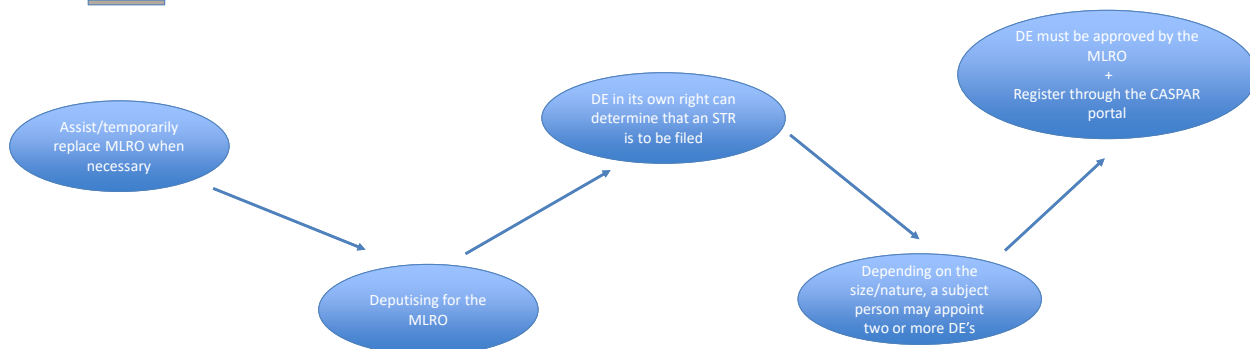
Difficulties that arise from CRMs need to service customers

- Obstruction in the sharing of CDD and business information needed by the MLRO to properly evaluate internal SARs
 - Appeals to management by CRMs, which may impede the MLROs probing into customer affairs
 - A feeling of defensiveness resulting from a realisation by the CRM that they too should have formulated a suspicion about the customer.
- ❖ Management action is needed required to ensure that MLROs are entitled to free and unobstructed access to CDD and business information. It is the responsibility of the management to protect the MLRO's right to ask any and all questions that maybe be deemed necessary when evaluating internal STRs.
 - ❖ MLROs who do not benefit from adequate management support will find themselves in very difficult and compromising circumstances.

What can the MLRO do?

- In order to avoid situations in which employees with concerns about customer relationships are pressured by managers not to ask questions or raise their concerns, they must be encouraged to communicate directly and confidentially with the MLRO.
- Whenever behaviour of this nature occurs, the MLRO must consider why a manager has behaved in the way and consider whether collusion exists between the manager and potential money launderers.
- Even in situations where collusion may not exist, the reason for pressuring the employee is to not asking questions should be fully investigated. Disciplinary action should be taken as needed.
- The perception of AML/CFT compliance teams and MLROs as both approachable and easily accessible is an essential prerequisite to encouraging intimidated employees to share their fears and concerns, despite any contrary management pressure.

Designated Employee



Documentation

Subject persons must have in place documented reporting procedures that provide for:

1. The appointment of one of the subject person's officers of sufficient seniority and comment as MLRO;
2. The consideration of internal reports by the MLRO;
3. Reasonable access for the MLRO or another designated employee to information held by the subject person which may be of assistance for the purposes of considering the report;
4. A procedure whereby the MLRO or another designated employee submits a report to the FIAU;
5. Notifying the FIAU and the relevant supervisory authority of the details of the appointed MLRO and any subsequent changes thereto and the appointment of a designated employee, if any
6. The approval by the MLRO of any employee designated by the subject person who shall work under the MLRO's direction.

THE MONITORING FUNCTION

Monitoring Functions

1. Day-to-day monitoring function

- Optional – depending on the nature, scale and complexity
- Appoint an officer at management level to monitor the day-to-day application of policies, procedures and controls
- Can be carried out by the MLRO or another officer at management level

Delegation of MLRO task to an officer of subject person/management level

- Ensuring continued compliance with the requirements of the PMLFTR, the FIAU's Implementing Procedures or other guidance issued by the FIAU;
- Day-to-day oversight of the subject person's AML/CFT measures, policies, controls and procedures;
- Regular oversight reporting, including reporting of non-compliance, to senior management;
- Addressing any FIAU feedback about the subject person's risk management performance or AML/CFT measures, policies, controls and procedures;
- Contributing to designing, implementing and maintaining internal AML/CFT compliance manuals, policies, procedures and systems;
- Conducting or seeing to periodic internal AML/CFT training for all relevant staff members and employees.

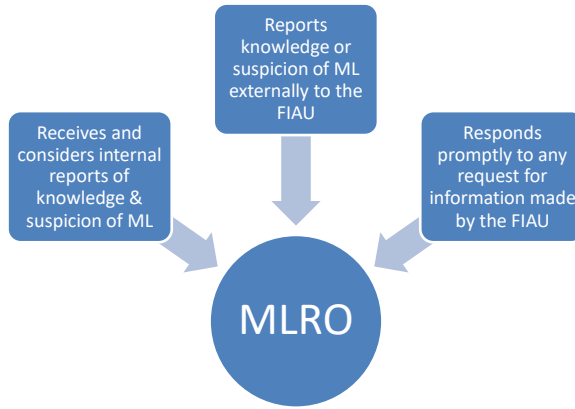
Monitoring Functions

2. General oversight function

- The board of directors or equivalent is ultimately responsible for ensuring compliance with AML/CFT obligations
- Designate one of its members to ensure such compliance

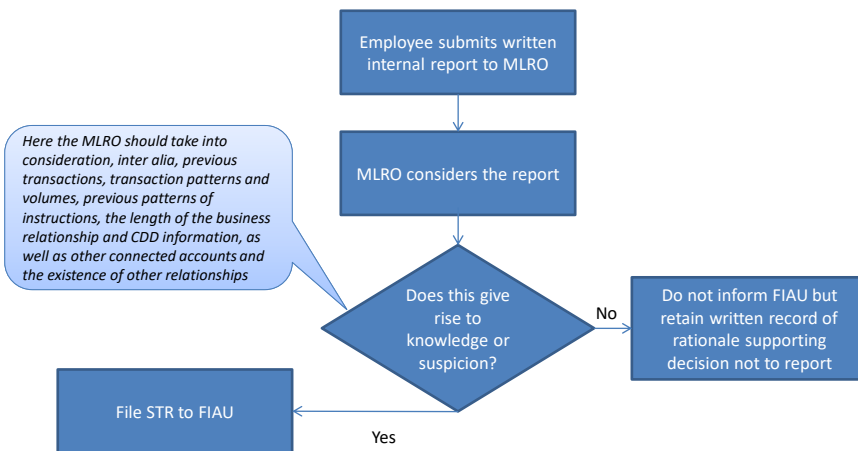
In order for the MLRO and its monitoring functions to operate successfully, senior management are responsible to offer the necessary resources.

Internal reporting procedures



27

Internal reporting procedures



28

External reporting

Knowledge	<ul style="list-style-type: none"> • Objective criterion, i.e. the existence of knowledge of ML/FT • Where the MLRO, or any other employee of the subject person, is aware or is in possession of information that indicates that any ML/FT activities may have taken place, are taking place, or will be taking place, the MLRO should immediately proceed with filing a report with the FIAU
Suspicion	<ul style="list-style-type: none"> • More subjective but must at least extend beyond speculation and be based on some foundation • MLRO should attempt to supplement this with objective criteria, e.g. mismatch between quantum of transaction and salary of customer, or unwillingness of customer to provide requested due diligence information
Reasonable grounds to suspect	<ul style="list-style-type: none"> • Goes beyond mere suspicion • On the basis of objective facts, the subject person ought to have suspected that ML/FT existed, even though a suspicion was not formed

Any disclosures made by the subject person to the FIAU should be made as soon as is reasonably practicable, but not later than 5 working days from when knowledge or suspicion of ML/FT arises or from the existence of reasonable grounds to suspect ML/FT.

Example: reporting suspicions about people met throughout course of employment

- A stockbroker is introduced to a customer by a law firm.
- The stockbroker and customer meet to discuss the services that can be provided. During the meeting, it becomes apparent that the customer has derived his property from criminal activity.
- Therefore the stockbroker decides that the customer does not meet the ideal customer profile and declines the relationship – this decision originates from the fact that the stockbroker is suspecting the customer of engaging and benefiting from criminal activity.
- A report is then made to the MLRO following such suspicions. Because the stockbroker declined the relationship on behalf of his firm, it is clear that he did not put himself or the firm in danger of laundering funds.
- Had the stockbroker decided not to report a suspicion of criminality, he could have committed an offence.

What constitutes suspicion?

Examples from UK courts:

- *“A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not”.*
- *“Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation.”*
- *“It seems to us that the essential element in the word ‘suspect’ and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be ‘clear’ or ‘firmly grounded and targeted on specific facts’.”*
- *“Parliament intended suspicion as a subjective fact to be sufficient
(1) to expose a person to criminal liability for money laundering and
(2) to trigger disclosures to the authorities. Parliament did not require, in addition, that the suspicion be based upon ‘reasonable’ or ‘rational’ grounds. There are good practical reasons for this. Unlike law enforcement agencies, banks have neither the responsibility nor the expertise to investigate criminal activity to satisfy themselves that the grounds for their suspicion are well founded, reasonable or ‘rational’.”*

It is imperative to highlight that not all transactions should be considered as suspicious, even if its nature may appear to be unusual or outside of customer profile – only further investigation can determine suspicion.

Example: problems in making determinations about suspicion

- The police have contacted the MLRO of a private company to discuss one of their clients, ABC Ltd.
- ABC Ltd was recently subject to a review by the internal review team.
- The ultimate beneficial owner (UBO) of the company is Mr. G and is in turn controlled by a trust company in the Seychelles.

Following a call with the police, the MLRO examines the file in detail and discovers the following facts.

1. Mr. G is a former Spanish general counsel to an African country.
2. His sister is a current member of the Spanish parliament.
3. Incorporate in 1996, ABC Ltd is a bearer share company, of which such shares are held by Mr. G and not the trust company.
4. ABC Ltd owns shares in a large publicly owner company that produces military equipment.
5. In 1999, ABC Ltd entered into an agreement with a French company for the procurement of contracts for the supply of electricity generators in Africa.
6. It is not clear whether ABC Ltd had the necessary expertise to be able to discharge its obligations under the agreement.
7. The same year ‘commissions’ were received in the account of ABC Ltd, and were then transferred to third-party accounts in Switzerland

Example: problems in making determinations about suspicion

- It is clear that the relationship with this Mr. G possesses significant risks that the MLRO has been able to identify. However the question remains as to whether Mr. G is involved in criminal activity, or whether ABC Ltd or its assets have been resulted from the proceeds of crime.

The following reasons need to be addressed:

a. MLRO is unable to formulate a suspicion of any particular criminal conduct on the part of Mr. G

There is no requirement to be able to suspect a particular type of criminal conduct. It is enough for him to simply suspect criminality.

b. MLRO does not think that any one aspect of the relationship is sufficient for him to formulate suspicion.

It is not necessary for any one aspect of a relationship to create a suspicion. Very often it is a combination of multiple factors during the lifespan of a relationship.

c. The conduct with which the officer is uncomfortable occurred before the relevant primary legislation was introduced.

The test of criminal conduct applies retrospectively in almost all jurisdictions. Thus, even if suspicious conduct in relation to an existing customer relationship occurred prior to the introduction of AML/CFT legislation, it is still reportable.

STRs filing timeframe

- Any disclosures should be made to the FIAU as soon as is reasonably practicable, but not later than 5 working days from when the knowledge or suspicion of ML/FT first arises or from the existence of reasonable grounds to suspect ML/FT.
- These 5 working days shall be deemed to start to run in accordance with the below:
 - in cases where, subsequent to the receipt of an internal report, the MLRO determines, on the basis of additional information and/or documentation other than what is contained in the internal report received by the MLRO, that there is knowledge or suspicion of ML/FT, the 5 working day period shall start to run from when such a determination is made by the MLRO;
 - notwithstanding the above, where the subject person is in possession of information that constitutes a reasonable ground to suspect ML/FT, the 5 working days shall start to run from when the subject person came into possession of or became aware of that information, independently of when the same information was brought to the attention of the MLRO.

Actions after reporting

- _ If once an STR is filed the subject person decides to maintain the business relationship with the customer who is the subject of the STR, the subject person should:
 - _ classify the customer as a high-risk customer; and
 - _ remain vigilant and monitor the activities of that customer to a larger extent.
- _ Before taking any decision related to a customer and services provided thereto which may have an impact on the analysis or any future investigation (e.g. deciding to terminate the business relationship with the customer), it is advisable to first hold discussions with the FIAU to ensure that the steps taken by the subject person do not hinder the analysis or the investigation.

The frequency of reviews and monitoring ultimately depends on the level of risk a customer poses. For example, a politically exposed person (PEP) should be subject to regular enhance due diligence (EDD) reviews.

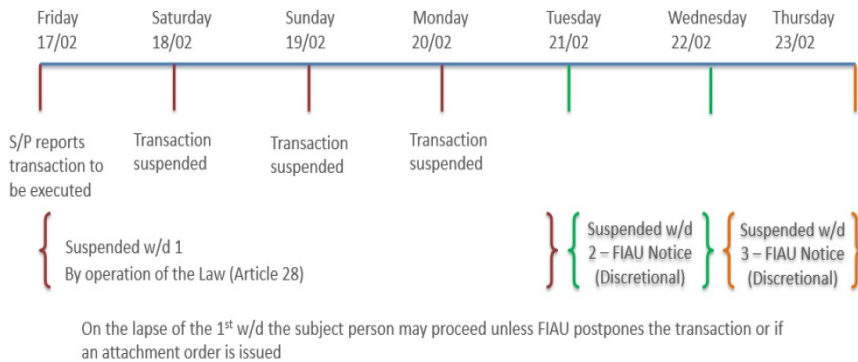
Actions after reporting

- _ When filing an STR, subject persons are required to delay the transaction to allow the FIAU time to consider whether or not to oppose the execution of the transaction.
- _ When it is not possible for subject persons to refrain from carrying out a transaction that is known or suspected to be related to ML/FT prior to informing the FIAU, subject persons must carry out the transaction and inform the FIAU immediately after the transaction is affected.
 - _ However, the impossibility to do so must be due either to the nature of the transaction (e.g., the system used to process the transaction does not allow at any point human interference, such as automated clearing or settlement systems) or because refraining from executing the transaction is likely to frustrate efforts to investigate or pursue the beneficiaries of the suspected criminal activity.

Actions after reporting

- When the FIAU considers it necessary to oppose the execution of a suspicious transaction, a notification of this opposition is to be made to the subject person concerned by any written means. In those cases when the FIAU opposes the execution of the transaction following the receipt of information from a subject person, the notification of opposition must be made to the subject person by not later than 1 working day following the day on which the information was received by the FIAU.
- Within this 1 working day, the subject person is prohibited from carrying out the relevant transaction. If, after the passage of 1 working day, following notification to the FIAU, the subject person has not received notification from the FIAU to suspend that transaction, the subject person can proceed with executing the transaction.
- When the FIAU suspends the execution of the transaction, the suspension is effective for a period of 1 working day, following the day of notification of the opposition by the FIAU. The FIAU may, however, authorise the execution of the transaction before the expiration of this period by any written means.
- The FIAU may, if it considers necessary, extend the period of suspension by a further 1 working day. When the FIAU decides to extend the period of suspension, it should notify the subject person in writing before the previous 1 working day suspension period expires.
- In practice, therefore, a transaction may be delayed by a maximum of 3 working days, following the day the subject person notifies the FIAU.

Actions after reporting



STRs filed by related industries

Company service providers	<ul style="list-style-type: none"> • CSPs contributed to almost 3% of the total number of STRs received by the FIAU in 2018. • Fraud once again featured as one of the most common suspected predicate offences identified, together with corruption and bribery. • Other suspected predicate offences included tax related crimes, smuggling, drug trafficking, arms trafficking, environmental crime and extortion. • The most common red flags identified by this sector included adverse media on the subject of the report, a lack of co-operation from the subject when asked to provide details or documentation on a transaction or operation, transactional activity that is unexplained or inconsistent with the subject's known profile, as well as an unnecessarily complex company or transaction structure.
Investment services licensees	<ul style="list-style-type: none"> • An increase was noted in 2018 in the number of STRs submitted by investment services licensees. • In the disclosures made to the FIAU by this sector, the most prevalent suspected predicate offence was corruption and bribery, followed by fraud. • Suspected insider trading and market manipulation were also reported in a few instances. • In the disclosures made to the FIAU in 2018, the most predominant typologies were the use of bank accounts and banking services in Malta and abroad. Other typologies identified included the use of cryptocurrencies and forex trading. The reasons for suspicion within this sector varied. As was noted in other sectors, adverse media on the subject of the report was one of the reasons resulting in a disclosure to the FIAU. • However, other red flags identified included transactional activity that is unexplained or inconsistent with the subject's known profile, a lack of adequate supporting documentation, as well as a lack of co-operation from the subject when asked to provide details or documentation on a transaction or operation.

STRs filed by related industries

Trustees and fiduciaries	<ul style="list-style-type: none"> • Trustees and fiduciaries accounted for 1% of the total number of disclosures received by the FIAU in 2018. • The disclosures made identified a number of suspected predicate offences, with the most prevalent being bribery and corruption. This was closely followed by fraud and tax related crimes. Other suspected predicate offences included extortion, arms trafficking, drug trafficking, forgery and FT. • The most common red flags and reasons for suspicion identified by this sector included a lack of co-operation from the subject when asked to provide details or documentation on a transaction or operation and adverse media on the subject of the report. • In a few other disclosures suspicion was raised due to changes in the proposed ultimate beneficial owner after identification details are requested, an unnecessarily complex company or transaction structure and a sudden, inexplicable lack of contact from the client.
---------------------------------	--

Spike in STRs reported

- Overall the FIAU has reported a 157% increase in STRs between 2017 and 2019. The FIAU, last year saw a 65% spike in suspicious activity reports, driven in part by a rise in reports from Satabank. The FIAU received 2,778 suspicious activity reports last year, up from 1,679 in 2018. Over the years there had been a consistent increase in suspicious transaction reports.
- According to the last FIAU annual report, banks and remote gaming companies reported the most suspicious activity among their clients- the most significant being the remote gaming sector. Remote gaming licensees registered an increase of 745 STRs, bringing their total submissions for 2019 to 1,445, around a 106% increase in reporting from 2018.
- Accounting for 52% of all STR submissions, the remote gaming sector secured the spot for top reporting sector in 2019, a position traditionally held by credit institutions, which filed the second largest number of STRs, still contributing to 35% of the STR submissions received. Credit institutions registered a considerable 33% increase from 724 STRs in 2018 to 962 STRs in 2019. Together, remote gaming companies and credit institutions filed 87% of all the STRs the FIAU received in 2019.
- In addition to the above results, significant increases were observed in the STRs filed by auditors, advocates, external accountants and supervisory authorities. Whilst on the other hand, insurance licensees, investment services licensees, trustees and fiduciaries filed less STRs in 2019 than they did in 2018.

Permissible and prohibited disclosures

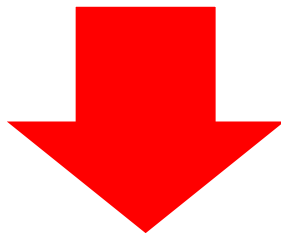


Permissible disclosures:

Disclosures to the supervisory authority relevant to that subject person or to law enforcement agencies in accordance with applicable law

Disclosures to any competent court, tribunal or other judicial authority in or outside Malta that the subject person refrained from carrying out a transaction

Any *bona fide* communication or disclosure made by a subject person or by an employee or director of such subject person



Prohibited disclosures:

When a subject person has a suspicion that ML/FT is occurring, both the subject person as well as any official or employee of a subject person, are prohibited from disclosing to the person under investigation or to a third party, that an investigation is being carried out, may be carried out, or that information has been or may be transmitted to the FIAU

Disclosure of such information would give rise to the offence of **tipping off** and may prejudice an investigation

Confidentiality and tipping off

- Any STR should be completed as soon as possible after the transaction and not in the presence of the subject of the report. The subject of the report must not be advised of the suspicions or the submission of a report by the reporting firm.
- It is an offence to disclose to anyone that a suspicion has been formed or that information has been communicate to the FIAU.
- To guard against the fears of being sued for breach of customer confidentiality, legislation offers statutory protection against breach of confidentiality for all information that is included in a disclosure report.

Financial Action Task Force (FATF) recommendation 21 requires that:

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

Points to keep in mind:

Developing an ML/FT risk appetite framework

- Establishing and interpreting your company’s risk tolerance

Withstanding challenge

- Providing ‘reasonable measures’ of due diligence in the event of an inspection

De-risking

- Deciding when to cease business with a high-risk client

Data protection

- Balance AML/CFT compliance requirements with GDPR principles

Conclusion:

- An MLRO should hold a position of sufficient seniority within their firm. The position should allow them to design, implement, and enforce their firm's compliance systems and procedures.
- Essentially, MLROs must be able to assess money-laundering risk. This skill requires not only an understanding of criminal methodologies but an understanding of the behaviour and business practices of customers and clients, who may themselves be exposed to risk.
- An MLRO should have a strong grasp of the concept of legal professional privilege since they might be required to disclose sensitive information to the FIAU – with legal implications for their firm and its employees.
- While an MLRO does not necessarily need to be legally-trained, knowledge of the field is useful. Alternatively, an MLRO might seek legal advice about this aspect of their role.

Conclusion:

- Employees and MLROs need to be aware of the legal obligation to report. Employees should feel they can report without any fear of facing repercussions.
- Important to keep in mind the timelines, for both internal and external reporting.
- Recent spikes in STR reporting over the last couple of years, highlights the growing importance of AML/CTF matters. More responsibility is being shouldered in respect to reporting and this continues to be of paramount significance.
- The result of non-compliance to such AML laws can result in financial risk, legal risk, reputational risk and the risk of sanctions.



www.21Academy.education