SAMPANDRAHARAHA MALAGASY
IADIANA AMIN'NY
FAMOTSIAMBOLA SY
FAMATSIAMBOLA NY
FAMPIHOROHOROANA
(Financial Intelligence Unit)

REPOBLIKAN'I MADAGASIKARA
Fitiavana - Tanindrazana - Fandrosoana

SAMIFIN
HO AN'NY TOEKARENA

DIRECTIVE NO. 001/SAMIFIN/CAB/DG/22
ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND/OR TERRORIST FINANCING AND THE REPORTING OF SUSPICIOUS TRANSACTIONS

The Financial Intelligence Unit, in short « SAMIFIN »,
In view of the Constitution;
In view of Law No. 2014-005 of May 28, 2014 on terrorism and transnational organised crime;
In view of Law No. 2016- 020 of August 22, 2016 on the fight against corruption
In view of Law No. 2016- 021 of August 22, 2016 on Anti-Corruption Poles;
In view of Law No. 2018- 043 of February 13, 2019 on the fight against money laundering and terrorism financing;
In view of Law No. 2021- 015 of August 05, 2021, amending, supplementing and repealing certain provisions of Law No. 2016- 021 of August 22, 2016 on Anti-Corruption Poles;
In view of Ordinance N° 2019-015 of July 15, 2019 on the recovery of illicit assets
Considering the Decree N° 2015- 036 of June 30, 2015 on the creation, organisation and functioning of the Financial Intelligence Unit named " Sampandraharaha Malagasy Iadiana amin'ny Famotsiambola sy ny famatsiambola ny asa fampihorohoroana « SAMIFIN » ;

Considering the following:

i. Illicit financial flows, economic and financial offences, corruption and/or related offences constitute a permanent and growing threat to Madagascar's economic stability and call into question the credibility of the formal business sectors and professions. Faced with the increased development of phenomena related to money laundering and/or the financing of terrorism, transnational organised crime and corruption, both nationally and internationally, it is essential to find an appropriate and effective response. In addition to the hardening of the penal policy in terms of money laundering and/or terrorism financing, it is also essential to focus the fight against these scourges on prevention, on the involvement of all the actors of the public and private sector in order to decree a synergy of common action that in the long term will produce convincing results.

ii. Through the multiple attempts, typologies and modus operandi used by criminals and/or delinquents to disguise the origin of funds, to place the proceeds of crime and/or misdemeanor, to resort to legal and accounting tricks and other possible forms of circumvention, the confidence of the public and international investors in Madagascar within the framework of transparency and the business climate could be compromised.

iii. Madagascar's technical compliance in terms of AML/CFT with international standards must also take into account the country's capacity and the capacity of the institutions subject to AML/CFT to deal with the threats and take corrective measures in relation to the risks and areas of vulnerability identified. If the levels of violence and prevention put in place at the level of the sectors of activity and professions concerned are not adapted to the national context, the delinquents and/or criminals will always be able to continue to abuse all the existing systems in order to pursue their misdeeds, the impacts of which will be considerable, both for the country and for the economic operators. And without prejudice to the fact that some sectors of activity and/or professions would disappear due to the loss of their credibility.

iv. Even though the provisions of Law No. 2018-043 of February 13, 2019 on the fight against money laundering and terrorist financing adopts the risk-based approach, the high circulation of cash, significant cash transactions remain a problem and can be exploited by delinquents and/or criminals in the context of money laundering and/or terrorist financing.
In order to strengthen due diligence measures and mitigate any risk inherent in such a practice, the institutions and professions subject to this Directive should strengthen the anti-money laundering and anti-terrorist financing measures within their respective jurisdictions by establishing a threshold for cash transactions.

v. The growth of electronic money, which is the materialization of financial inclusion in Madagascar, is tending to be assimilated to bank accounts and may constitute a channel for money laundering and/or terrorist financing. And this is one of the reasons that pushed the legislator to introduce in the provisions of Law No. 2016-056 of February 02, 2017 relating to electronic money institutions as well as other subsequent texts an obligation to put in place an adequate anti-money laundering and anti-terrorist financing system for professionals in the sector.

vi. The other professions grouped in the category of Designated Non-Financial Businesses and Professions (DNFBPs) can constitute an ideal channel for criminals and/or delinquents to launder the proceeds of their crimes and misdemeanors, or even to finance terrorist acts. For this reason, it is necessary to strengthen measures aimed at identifying clients, beneficial owners and monitoring transactions.

vii. Vigilance, including the monitoring of transactions made by politically exposed persons (PEPs), reinforces prevention. This category of customers is exposed to risks of corruption and/or similar offences, money laundering and/or the financing of terrorism. The involvement of a politically exposed person in money laundering, terrorist financing, or any other offence similar to corruption will seriously damage social peace and deteriorate the moral value of Malagasy society.

ADOPTS THIS DIRECTIVE:

TITLE I: GENERAL PROVISIONS

CHAPTER I: Purpose, scope, definitions

Article 1. This Directive is drawn up in order to strengthen the implementation of measures for the prevention and detection of money laundering and/or terrorist financing as well as the associated underlying offences.
It sets out the obligations of professions subject to the fight against money laundering and terrorist financing, the implementation of the prevention and detection mechanism, and the procedures for reporting suspicious transactions to the Financial Intelligence Unit.

Article 02. This Directive shall apply to the institutions subject to the provisions of Article 08 of Law No. 2018 - 043 of February 13, 2019 on money laundering and terrorist financing, namely:

i. Financial institutions ;
ii. Designated Non-Financial Businesses and Professions (DNFBP);

The detailed list of which is annexed to this Directive in accordance with Article 04 points 18, 20, 21 of the said Law and referred to collectively in this Directive as "reporting institutions" or "reporting professions".

Article 03. Money laundering is a process by which criminals and/or delinquents seek to conceal the origin and ownership of the proceeds of their criminal activities in order to avoid prosecution, conviction and confiscation of assets.

It consists of giving a legitimate appearance to the assets or capital derived from the

commission of reprehensible offenses and originating from criminal and/or delinquent activities.

Article 1 of Law No. 2018- 043 of February 13, 2019 on the fight against money laundering provides a broader definition and the constituent elements of money laundering.

Article 04. Financing of terrorism consists of providing, collecting funds, financial means, likely to be used in terrorist activities, to commit terrorist attacks.
The provisions of Article 02 of Law No. 2018- 043 of February 13, 2019 on the fight against money laundering and terrorist financing provides a broader definition of the concept of terrorist financing.

CHAPTER II: OBLIGATIONS OF REPORTING INSTITUTIONS

SECTION I: DESIGNATION OF ANTI-MONEY LAUNDERING AND ANTI-TERRORIST FINANCING CORRESPONDENTS

Article 05. Each reporting institution is required to communicate to the Financial Intelligence Unit and to their respective supervisory authorities:

- the identity of its managers and/or employees authorised to transmit suspicious transaction reports (STRs) in accordance with the provisions of Articles 27 and 28 of Law No. 2018-043 of February 13, 2019 on the fight against money laundering and terrorist financing ;

- the identity of its managers and/or employees in charge of responding to any request from the Financial Intelligence Unit, receiving acknowledgements of receipt of Suspicious Transaction Reports, and ensuring the dissemination of information, notices or recommendations from the Financial Intelligence Unit to the staff members concerned.

Article 06. An updated list of the correspondents of each entity must be transmitted to the Financial Intelligence Unit and to their regulatory authorities in the event of constant changes within them.

SECTION II: PREVENTIVE MEASURES

§ 1-Internal measures to combat money laundering and the financing of terrorism

Article 07. Without prejudice to the obligations and rules governing their respective professions, the institutions subject to this Directive shall have their own internal arrangements for combating money laundering and terrorist financing.

Article 08. The internal anti-money laundering and anti-terrorist financing measures put in place by each category of profession concerned by this Directive must take into account:

1. The risk-based approach;
2. The size and scope of each structure, both nationally and internationally;
3. The formulation of an AML/CFT policy including a description of the resources deployed in terms of compliance;
4. The elaboration of a written procedure distributed to all staff on the internal system in place;
5. The definition and implementation of a training and awareness program for the staff on the fight against money laundering and terrorist financing, translated into an Annual Training Plan;
6. The definition and application of vigilance measures in relation to certain categories of operations carried out by clients and Non Profit Organisations (NPOs);
7. The adoption of a mode of conservation of information and/or documents related to the identity of clients and beneficial owners, beneficiaries and holders of power of attorney, agents, beneficial owners, to suspicious transactions in the forms prescribed by the law;
8. The measures for monitoring and controlling strict compliance with the internal system for combating money laundering and the financing of terrorism;
9. The evaluation of the system put in place and the risks linked to money laundering and

terrorist financing;

10. The evaluation of risks linked to money laundering and/or terrorist financing for any new product or development of products already on the market.

Article 09. The institutions subject to this Directive shall take appropriate measures to identify, assess, understand and mitigate the money laundering and terrorist financing risks to which they are exposed.

The risk-based approach shall take into account the following parameters
:

i. Client factor: level of clarity on the beneficial owner, multiple legal and shareholding structure, natural and/or legal persons operating in sensitive sectors of activity and who may be exposed to money laundering and terrorist financing risks, non-resident client, profit and/or status of the client (Politically Exposed Person, association...), antecedents of the client, the way the business relationship is established.

ii. Geographical factor: client with a nationality and/or nationalities of a country considered risky according to the Financial Action Task Force (FATF) classification, transactions involving risky and/or non-cooperative countries, conflict zones (including non-profit organisations according to FATF criteria).

iii. Product and service factor: adequacy of the client's profit in relation to the declared activities, coherence of the transactions and declarations, flows in relation to the activities and/or professions known to the client, accompanied by convincing evidence, normal operation of the account(s) not showing atypical or unusual behavior, products and services provided in relation to the activities, distribution channels for the products and services provided, as well as the means of communication used to contact the clients.

§ 2-Evaluation of the internal system and risks related to money laundering and terrorist financing

Article 10. Depending on the risks identified, each category of profession subject to this Directive is required to carry out an evaluation campaign of the internal system put in place to identify the risks related to money laundering and terrorist financing.

Even if the reporting institution considers that the level of exposure to the risk of money laundering and terrorist financing within it is low and under control, it is required to carry out an evaluation campaign once a year.

Article 11. The evaluation of the internal anti-money laundering and combating the financing of terrorism system and the risks related to money laundering and the financing of terrorism must comply with the criteria.

Each profession may extend its evaluation to other aspects that are specific to it and that it considers may be a source of vulnerability and may constitute a channel for money laundering and/or terrorist financing within it.

Article 12. The results of the evaluation of the internal system for combating money laundering and terrorist financing made by the reporting institutions must be communicated in the form of an official report to the Financial Intelligence Unit and to the control and suspension authorities, respectively, and be accompanied by a detailed action plan to remedy the deficiencies identified and/or the improvements made in order to strengthen and make effective the internal system for combating money laundering and terrorist financing.

The deadline for transmitting the official report referred to in the first paragraph of this Article is thirty (30) days from the end of the evaluation campaign.

Article 13. Without prejudice to their ultimate responsibility for compliance with their obligations, the reporting institutions may have recourse to one or more third parties in order to implement the system for combating Center for Money Laundering and Terrorist Financing, in accordance with the provisions of Article 16 e/ of Law No. 2018- 043 of February 13, 2019 on

Combating Money Laundering and Terrorist Financing under the following conditions:

1. The third party is an institution located or having its registered office in Madagascar or a person belonging to an equivalent category under foreign law and located in a third country that imposes equivalent obligations in terms of the fight against money laundering and terrorist financing;

2. The information collected by the third party is made available to the reporting institution, under the conditions provided by the control and supervisory authority.

SECTION III: Implementation of Preventive Measures and Operational Requirements

§ 1: Suspicious Transaction Reports (STR)

Article 14. Any profession subject to this Directive shall be required to transmit a Suspicious Transaction Report to the Financial Intelligence Unit, pursuant to the provisions of Article 27 of Law No. 2018-043 of February 13, 2019 on the fight against money laundering and terrorist financing, whenever there is reasonable cause to suspect and may involve:

- All goods and/or assets of any nature whatsoever held in their books when they could be linked to a crime or a misdemeanor in the process of money laundering and / or financing of terrorism, and in general to transnational organised crime;
- All assets that can be considered as belonging to terrorists, terrorist groups, persons and/or entities linked to them;
- Transactions involving sums of money or property that could be the proceeds of a crime or misdemeanor and/or be part of a money laundering or terrorist financing process;
- Any operation for which the identity of the principal or beneficiary remains doubtful despite the diligence carried out in accordance with the provisions in force concerning the identification of customers,
- Operations for their own account or for the account of third parties with legal entities, including their subsidiaries or institutions, acting in the form of or on behalf of trust funds or any other instrument for the management of an assigned asset, the identity of the constituents and/or beneficiaries of which is not known;
- Any legal and/or financial arrangement designed to promote anonymity and make it difficult to identify the beneficial owners;
- Any false declaration aiming to alter the reality of the activities of a legal entity;
- Any production of false documents, falsification of accounting documents with the aim of circumventing the legislation in force, the financial, tax and accounting system.

Depending on each category of profession, additional indicators may be completed by the Financial Intelligence Unit and their respective regulatory authority.

Article 15. A Suspicious Transaction Report may relate to one and/or more operations, transactions, both domestic and cross-border.

When the suspicious transaction report relates to an operation that has not yet been executed, it is accompanied by an indication of the time limit for its execution.

The report may only concern operations or transactions that have already been executed when it was impossible to postpone their execution or when it became apparent, after the operation was carried out, that the funds could have been linked to a crime or misdemeanor or that postponing the execution of the operation would be likely to prevent the prosecution of the beneficiaries of money laundering or terrorist financing.

Article 16. Any Suspicious Transaction Report sent to the Financial Intelligence Unit must be made in the form prescribed in Article 28 of Law No. 2018-043 of February 13, 2019 and in accordance with the form annexed to this Directive, through the dedicated digital exchange system made available to the reporting institutions by the Financial Intelligence Unit.

Transaction reports in EXCEL and PDF format must be attached to the said declaration.

Non-exhaustive indicators that may be considered suspicious operations are attached to this Directive and may be completed by the reporting institutions according to the risk areas identified and/or the occurrence of cases within their respective institutions.

Article 17. In addition to the Suspicious Transaction Reports transmitted to the Financial Intelligence Unit, the regulated professions shall initiate, in parallel, an in-depth analysis of the circumstances in which the suspicious transaction took place, the functioning of the account(s) opened in the name of their client in order to identify other so-called "atypical" transactions, with no apparent economic link.

Article 18. At the end of each month, the reporting institutions must send to their respective control and supervisory authorities a summary of the declarations made to the Financial Intelligence Unit.

The summary of suspicious transaction reports sent to the control and supervisory authorities must not mention the details of the report itself, nor the identity of the suspected natural persons and/or legal entities.

Article 19. The reporting institutions are obliged to systematically communicate information to the Financial Intelligence Unit concerning certain transactions identified as presenting a risk of money laundering or terrorist financing, the threshold of which is fixed by supplementary directive, taking into account the specificity of each category of profession.

The same obligation extends to all information related to transactions involving virtual assets, such as crypto-currencies, bitcoin and other forms of virtual assets, without threshold limitation.

§ 2: Procedures for the execution of oppositions on suspicious transactions, Orders on Request for the purpose of freezing an account, requests from competent authorities

Article 20. Any institution subject to this Directive that has been notified by the Financial Intelligence Unit and/or any judicial decision ordering the blocking of accounts or the freezing of assets must carry out such notification immediately and promptly.

Article 21. In the interest of transparency, each profession that has been notified of a freezing decision must make an official return to the Financial Intelligence Unit within a period not exceeding forty-eight (48) hours from the date of receipt of the request to oppose the execution of suspicious transactions, mentioning: the date of the effectiveness of the freezing, the account number(s) concerned, the identity of the account holders, the representatives of the account(s), and the amount of the blocked assets.

The same obligation is applicable even if no account and/or assets have been blocked at the level of the institution and/or profession concerned.

The mechanism is valid for the execution of requests issued by the competent court, transmitted by the Financial Intelligence Unit to any person subject to the present Directive.

Article 22. With regard to professional secrecy and information, in application of the provisions of Article 43 of Law No. 2018-043 of February 13, 2019 on the fight against money laundering and terrorist financing, it is formally prohibited to disclose and/or communicate to the accused and/or their representatives: information, confidential documents relating to requests made by SAMIFIN and ongoing investigations including oppositions on suspicious transactions.

The same restrictions extend to any communication concerning the contacts and coordinates of the correspondents with the Financial Intelligence Unit.

§3: Freezing, seizure and confiscation related to the recovery of illicit assets

Article 23. Pursuant to the provisions of Ordinance No. 2019- 015 of July 15, 2019 on the recovery of illicit assets, any profession subject to this Directive that has been notified of a decision to freeze, seize and/or confiscate assets by specialized public administrations, law enforcement officers or the competent courts must execute it immediately and without delay.

The modalities of execution of the freezing, seizure are referred to the application of Ordinance No. 2019-015 of July 15, 2019 on the recovery of illegal assets in all its provisions.

§ 4: Obligation to execute the requisitions of the judicial authorities

Article 24. Professional secrecy and the protection of information and personal data shall not constitute a reason for not responding to any request made by the Financial Intelligence Unit.

§5: Implementation of the United Nations Security Council resolutions on the fight against terrorism and the proliferation of weapons of mass destruction

Article 25. In application of Resolutions 1267, 1373, 1989 of the United Nations Security Council on the fight against terrorism and other subsequent resolutions, the professions subject to this Directive are required to inform the Financial Intelligence Unit and their respective control and supervisory authorities without delay of the existence of listed and/or sanctioned persons, entities in their databases.

Article 26. In the event of suspicion, discovery and/or possession of assets belonging to and/or that may belong to terrorists, terrorist organisations and/or entities or persons affiliated with them, the professions subject to this Directive must initiate the procedures for freezing the assets concerned, in particular: the referral of the matter to the Ministry of Foreign Affairs for the purposes of a request to freeze the assets, the information of the competent authorities as provided for in Article 25 of this Directive.

Article 27. The freezing of assets provided for in Articles 25 and 26 shall extend to:

1. Funds or other property owned or controlled by the designated entity or person and not only those likely to be linked to a specific terrorist act, plot or threat;
2. Funds or other property owned or controlled wholly or jointly directly or indirectly, by the designated persons or entities;
3. Funds or other property derived from or generated by funds or other property owned or controlled, directly or indirectly, by the designated persons or entities;
4. Funds or other property of persons and entities acting on behalf of or at the direction of the designated persons or entities.

CHAPTER III: Vigilance measures

SECTION I: CUSTOMER DUE DILIGENCE MEASURES

§ 1 - Customer knowledge

Article 28. The reporting institutions are required to know their clients. Knowledge of the client extends from the moment of entry into the relationship and throughout the business relationship and must be updated whenever there is a change, in particular in the status and/or situation of a client, the nature of the existing business relationship between the parties and/or other relevant information that may affect the business relationship in a general way.

Article 29. Before entering into a relationship, the institutions subject to this Directive are required to:

- ascertain the identity, domicile and registered office of their clients, their beneficial owners and the beneficial owner(s);
- understand the business relationship envisaged and which may exist between the parties;
- determine the nature of the products, distribution channels, operations and/or transactions, services that will be used during the business relationship.

Article 30. The verification of the identity of a natural person is materialized by a control of the original of an official document having legal value on the territory of the Republic of Madagascar and in the course of validity, in particular, a national identity card, a travel document, a resident card. Verification of domicile and occupation is carried out by checking any document that can be used as proof.

Article 31. In the case of a natural person who exercises a commercial activity, the reporting institution is required, in addition to the documents listed in Article 30 of this Directive, to request and examine the legal and commercial documents attesting to the legality of his activity; in particular: an extract from the trade register, a valid professional card, a tax identification card as well as any other documents that it deems useful depending on the category of profession concerned.

Article 32. The identification of a legal person and/or a legal entity that does not have legal personality is made on the basis of the original or a certified copy of any act or extract from the official register that establishes its name, its legal form and its registered office, as well as the powers of the persons acting on its behalf.

The regulated professions shall ensure, under the same conditions as those laid down in Articles 29 and 30 of this Directive, the true identity and address of the persons authorised to act on behalf of the legal person or structure to be identified.

Article 33. Reporting institutions must have the information necessary to understand the ownership and control structure of the legal person and of the unincorporated legal entity and to determine the natural persons who ultimately own or control them.

Article 34. In addition to the formalities prescribed in Articles 30, 31 and 32 of this Directive, reporting institutions may also inquire by any other means into the veracity of the information gathered and documents presented by their customers at the time of entering into the relationship and throughout the business relationship when they have doubts about the authenticity and relevance of the data produced. However, provided that such practices do not violate the protection of privacy, the legal provisions on personal information.

Article 35. In the event of fraud, falsification and/or production of false documents perpetrated by their clients, the reporting institutions must terminate the business relationship in the manner prescribed by the laws in force regarding the reporting and termination of relationships and immediately inform the Financial Intelligence Unit in the form of a Suspicious Transaction Report. And without prejudice to any legal action that the regulated profession or the regulatory authority may take against the author.

§ 2 - Identification of clients and beneficial owners

A - Occasional clients

Article 36. The identification of occasional customers shall be carried out in the manner and under the conditions laid down in Articles 30 to 32 of this Directive.

Article 37. On the basis of their knowledge of the client and on their own initiative, the

regulated professions may classify an occasional client as a regular client.

If the case arises, the regulated professions must take all measures to collect all the information concerning their clients and to comply with the provisions of Articles 29 to 31 of this Directive.

B -Economic beneficiary

Article 38. Pursuant to the provisions of Article 15 of Law No. 2018- 043 of February 13, 2019 on the fight against money laundering and terrorist financing, in the event that the client does not appear to be acting on his own behalf, each regulated profession shall inquire by all means as to the identity of the person on whose behalf he is acting.

If, after verification, there is still doubt as to the identity of the beneficial owner, it must terminate the business relationship and submit a suspicious transaction report to the Financial Intelligence Unit.

C- Beneficial owner

Article 39. The professions subject to this Directive are required to identify the beneficial owner(s) of the legal person of a transaction(s) before entering into a relationship and throughout the business relationship.

The beneficial owner of a legal person is the natural person(s) who: holds, directly or indirectly, 25% or more of the capital or voting rights; or exercises, by any other means, a power of control over the management, administrative or executive bodies of the legal person or over the general assembly of its members.

In the case of an operation, it is the person for whom the operation is carried out or an activity is performed.

Article 40. The reporting institutions are obliged to keep and update all the information relating to the beneficial owners of the legal entities within their respective jurisdictions.

A register of beneficial owners shall be established and updated at the level of each reporting institution. At any time, the Financial Intelligence Unit, the investigative bodies and the competent judicial authorities within the framework of investigations into money laundering and terrorist financing may have access to it on request.

Article 41. In the event that it is impossible to identify the beneficial owner(s), the reporting professions must refrain from entering into a business relationship.

Article 42. If during the course of the business relationship, the regulated professions are no longer able to identify the beneficial owner(s) or do not obtain the documents and/or information requested from their clients within thirty (30) days of receipt of their official request by their client, they must terminate the business relationship and transmit a suspicious transaction report to the Financial Intelligence Unit.

§3-Classification and risk rating of customers

Article 43. The professions subject to this Directive must define policies and apply procedures for the classification of their customers before entry and throughout the business relationship.

The classification of customers must be appropriate to the profile of each customer and the exposure to the risk of money laundering and/or terrorist financing.

Article 44. Clients are classified as follows:

i. Regular customer: a natural person and/or legal entity with whom a reporting institution has a business relationship; or with whom it is planned to establish a professional or commercial relationship which is supposed, at the time the contact is established, to be of a certain

duration and includes any contractual relationship, whether formalized or not, that takes place within the framework of an activity.

ii. Occasional customer: a natural person and/or legal entity who seeks the assistance of a general reporting Institution for the sole purpose of preparing or carrying out a one-off transaction or of being assisted in the preparation or carrying out of such a transaction, whether it is carried out in a single transaction or in several transactions that appear to be linked together.

iii. Sensitive customer: a natural person and/or legal entity in a business relationship with a reporting institution, who by reason of his status, his function, the nature of his activities exposes him to risks related to money laundering and/or terrorist financing.

Article 45. Are classified as sensitive customers:

- Politically Exposed Persons as defined in Article 4 point 21/ of Law No. 2018- 043 of February 13, 2019 on the fight against money laundering and terrorist financing, the list of which is annexed to this Directive;
- Non-profit organisations, charities, foundations, religious associations, religious congregations, as listed in the annex to this Directive;
- Any legal entity with "complex" shareholding chains and/or multiple legal structures, the details of which are annexed to this Directive;
- Any legal entity having Politically Exposed Persons as shareholders;
- Any correspondent bank having a business relationship with the reporting institution;
- Any legal entity established and/or covering countries considered to be at risk according to the FATF criteria (tax havens and/or former tax havens, non-cooperative countries, conflict zones, etc.) ;
- Any legal entity operating in sectors of activity deemed to be at risk, the list of which is published by the Financial Intelligence Unit;
- Any sensitive client must be systematically noted as high risk and is subject to reinforced monitoring.

Article 46. Depending on the risks identified by the regulated professions, particularly in relation to the profile of the client, the geographical area, the types of transactions and the sectors of activity, a rating related to money laundering and/or terrorist financing must be assigned to each client and to the category of clientele set out in Article 44 of this Directive.

Article 47. The risk rating to be applied to a customer may be low, medium or high.

§ 4-identification of Politically Exposed Persons (PEPs)

Article 48. Reporting institutions must have adequate risk management systems in place to determine whether a potential customer, his beneficial owner, and/or beneficial owner is a Politically Exposed Person.

The family circle and/or circle of influence of a Politically Exposed Person are considered as such, with the same due diligence measures to be applied.

A list of Politically Exposed Persons, their family circle and circle of influence is attached to this Directive.

Article 49. Any entry into a relationship with a Politically Exposed Person or an Ultimate Beneficiary having the status of a Politically Exposed Person must obtain the prior consent of the governing body of the profession subject to the Directive.

Article 50. Reporting institutions are required to take all reasonable measures to identify the origin of the assets and funds of any client, beneficial owner of persons classified as Politically Exposed Persons.

They must apply enhanced due diligence measures with respect to Politically Exposed Persons.

Article 51. Any possibility of entering into a relationship, business relationship, opening an account or carrying out any other operation or remote transaction must be subject to the implementation of appropriate measures to guarantee the identification of customers.

These measures may include the authentication of the identification documents present, the request for additional documents, the possibility of an independent verification of the customer's situation by a third party of confirmed reputation, the payment of an initial deposit and/or advance into an account opened in the customer's name with a financial institution subject to the FATF recommendations or the sending of a letter with acknowledgement of receipt to the customer's address.

SECTION III: SPECIFIC AND ENHANCED VIGILANCE MEASURES

§ 1-As regards entities and/or shell banks

Article 52. Any business relationship and/or service with and/or on behalf of fictitious entities, holding anonymous accounts and/or those under fictitious names are prohibited.

§ 2-In respect of transactions

Article 53. In addition to the obligations and vigilance measures set forth in this Directive, reporting institutions are also required to be alert to any transaction and/or operation or financial arrangement involving large sums of money carried out under unusual and complex conditions and which does not appear to have any economic justification or lawful purpose carried out by its customers.

If the case arises, each profession must initiate a thorough examination and inquire of the client as to the origin and destination of the funds, the reason for the transaction, the identity, domicile, profession of the latter and of the beneficiary, and the existence of a valid economic link.

Article 54. In addition to the internal positive system for combating money laundering and terrorist financing based on the risk-based approach, depending on the products, existing distribution channels, identified risk areas, and services provided, the regulated professions that handle large volumes of cash and carry out significant transactions on behalf of their clients may establish an internal threshold for each type of operation carried out by its clients.

The threshold applied by the reporting institution must be included in the AML/CFT due diligence procedures after being approved by the professional association or order to which it belongs and/or by its regulatory authority.

Article 55. Without prejudice to the implementation of obligations specific to their respective professions, the reporting institutions are required to keep a register dedicated to the fight against money laundering and terrorist financing, depending on the nature and/or characteristics of the operations and/or transactions they are intended to carry out.

The document called "internal register of transactions" is used to collect all information, in particular:

- The characteristics and details of the operation and/or transaction;
- The origin and destination of the funds, the purpose of the transaction;
- The complete identity of the principal, the beneficial owner(s), the beneficiary (ies), the address, the profession and other information deemed relevant by the reporting institutions.

The confidential report drawn up for this purpose must be kept by the reporting institutions.

At any time, the Financial Intelligence Unit and/or the supervisory and control authorities for each category of profession may obtain communication of the aforementioned register and the documents related thereto.

Article 56. Reporting institutions must have a permanent understanding of the expected operation of the accounts opened in their books and of the services performed on behalf of their

clients, so as to identify atypical transactions with no recognized economic purpose.

Article 57. Increased vigilance must be applied to transactions made by:
- A Politically Exposed Person (PEP) ;
- Non-Profit Organisations (NPOs), foundations, non-governmental organisations;
- Any of the sensitive customers listed in Article 44 of this Directive.

Article 58. Without prejudice to the instructions issued by the supervisory authorities for each category of reporting institution, the obligation set forth in Article 56 of this Directive applies to:
- all operations from and/or to financial institutions which are not subject to obligations at least equivalent to those provided for in this Directive with regard to customer identification, transaction monitoring or which are located in countries considered to be risky or non-cooperative;
- All transfers of funds to foreign countries and/or national territory whose execution must obey the regulations of the foreign exchange code;
- All operations related to electronic money;
- All operations executed by electronic transfers;
- Any operation, legal and financial arrangement involving legal entities registered abroad (transfer, repurchase, merger, others...).

§ 3- With regard to the direct debit of exports

Article 59. In addition to the obligations and vigilance measures set forth in this Directive, reporting institutions are required to declare to the Financial Intelligence Unit any direct debit transaction for exports, including free remittances that have not been fully discharged within twelve months of their implementation

TITLE III: PENALTIES

Article 60. Without prejudice to the pronouncement of sanctions by the judicial authorities, their respective control and supervisory authorities, any failure to exercise due diligence or to organize internal procedures for the prevention of money laundering and the financing of terrorism shall be subject to the strict application of the provisions of Law No. 2018- 043 of February 13, 2019 on combating money laundering and the financing of terrorism.

TITLE IV: FINAL PROVISIONS

Article 61. The present Directive enters into force upon its notification to the Professional Association and/or Order or group of each profession subject to it.

Article 62. Depending on the risks identified, the evolution of Malagasy legislation, the phenomenon of the fight against money laundering and the financing of terrorism and taking into account the specificity of each category of profession, additional directives may be issued as necessary after consultation with each control and supervisory authority, professional associations and/or orders, in particular on the procedures for reporting suspicious transactions and vigilance measures.

Article 63. A guide for processing suspicious transaction reports drawn up by the Financial Intelligence Unit is made available to the regulated professions in order to help them implement the technical and operational aspects relating thereto.

Antananarivo, June 14, 2022.

SERVICE DE RENSEIGNEMENT FINANCIER – SAMIFIN – REPOBLIKAN'I MADAGASIKARA

Le Directeur Général

RAKOTONARISON Mamitiana

APPENDIX 01: "Designated Non-Financial Businesses and Professions"
or
"DNFBPs"

"Designated Non-Financial Businesses and Professions" or "DNFBPs" means any natural or legal person who conducts, advises on, and controls transactions involving the movement of funds, including:

a) Casinos and gaming houses, including online casinos;
b) Real estate agents and brokers;
c) Vehicle dealers in road, rail, inland waterway, sea and air transport;
d) Jewelers, dealers in precious stones and metals;
e) Lawyers, notaries, other independent legal professionals;
f) Accountants, auditors ;
g) Legal representatives and managers of casinos and groups, circles and companies organizing games of chance, lotteries, betting, sports or horse-riding prognoses;
h) Certified public accountants and employees authorised to practice the

profession of certified public accountant;

i) Judicial administrators and judicial representatives;

j) auctioneers;

k) Cash-in-transit companies ;

l) Trust and company service providers ;

m) Any person acting in the capacity of trustee or manager of a trust or similar legal arrangement governed by foreign law and owning property in Madagascar.

APPENDIX 02: SECTORS OF ACTIVITY CONSIDERED AT RISK

- Casino, gaming houses, gambling, horse racing, online gaming;
- Car dealership ;
- Import and sale of second-hand vehicles;
- Import and export of cash products (vanilla, letchis, cocoa, etc.), precious stones, gold;
- Mining and gold activities;
- Wholesalers of basic necessities ;
- Wholesalers of second-hand clothes;
- Real estate and construction;
- Sale of building materials;
- Jewelry and jewelry;
- Purchase and wholesale of cattle.

The above list is not exhaustive. Depending on the risks identified and without prejudice to an update made by the the Financial Intelligence Unit, the reporting institutions may extend the sectors of activity that they consider to be at risk.

SERVICE DE RENSEIGNEMENT FINANCIER
REPOBLIKAN'I MADAGASIKARA
SAMIFIN

APPENDIX 03: INDICATORS OF A SUSPICIOUS TRANSACTION

- Transactions planned or carried out with no relation to the client's assets or apparent income, or to his commercial or professional activity;
- Important cash manipulations without economic justification;
- Important cash deposits;
- Unnecessarily complex operation in relation to the aim;
- Investments disproportionate to the activity or financial structure of the company;
- Invoicing to unknown clients whose identity is not proven and whose financial standing cannot be verified;
- Fractionalization of cash payments;
- Credit movements disproportionate to the size of the newly created company;
- mismatch between the client's profile and his income;
- Income tax declaration contradictory to the client's practical income;
- Suspicious behavior of the client and unusual and complex transactions;
- International transfers from high-risk countries;
- International transfers to non-profit organisations;
- Transaction refused by a financial institution when a court order or a judicial requisition prevents it, the transaction involves a person subject to an asset freeze measure, when the client does not provide justification for the transaction (e.g. declaration of origin or destination of funds);
- Use of inactive accounts;
- Use of transit accounts (accounts with multiple transfer orders and low balances);
- Cash receipts followed by transfer orders to banks or "offshore" companies.

Note: the indicators set out in this document are not exhaustive. They may be completed by the reporting institution according to the risk areas identified at its level and its customer typology.

.

SERVICE DE RENSEIGNEMENT FINANCIER
REPOBLIKAN'I MADAGASIKARA
SAMIFIN

APPENDIX 04: POLITICALLY EXPOSED PERSONS

Domestic and foreign Politically Exposed Persons ("PEPs") are individuals who hold, or have held, prominent public positions as well as their direct family members or persons known to be closely related to them.

I. "Foreign PEPs": refers to natural persons who hold or have held important public positions in another State, namely :

a) Heads of State or Government;

b) Members of royal families ;

c) High ranking Officials within the public authorities:

- Ministers, Minister Delegate or Vice-Minister, Secretary of State;
- Parliamentarians: Senators, Deputies ;
- Heads of institutions ;
- Civil servants occupying high responsibility positions equal to or higher than that of Ministry Director, - Members of the Supreme Court;

d) Members of the Supreme Courts, Constitutional Courts or other high jurisdictions whose decisions are not subject to appeal, except in exceptional circumstances;

e) Members of the courts of auditors or of the boards of central banks;

f) Ambassadors, businessmen and high-ranking military personnel;

g) Members of the administrative, management or supervisory bodies of public enterprises;

h) Senior officials of political parties;

i) Persons known to be closely associated with a PEP, including any close relative, family member by direct lineage or marriage, or any person connected by business relationships.

II. « National PEPs »: refers natural persons who hold or have held important public positions in Madagascar, including the following individuals :

a) Heads of State or Government ;

b) Senior officials within the public authorities:

- Ministers ;
- Senators ;
- Members of Parliament ;

- Heads of institutions ;
- Heads of Provinces, Commissioners General, Regional Prefects, Regional Chiefs, -Chiefs of Districts President of the Special Delegation (PDS) of a territorial authority of a level higher than or equal to the communes;
- Mayors ;
- Civil servants holding positions of high responsibility at a level equal to or higher than that ofdirector of a ministry;
- Members of the Corps of Administrators, Inspectors and Commissioners in the Public Administration, Judges, administrative and financial Magistrates, regardless of their grade and function;
- Any person who performs the functions of public authorizing officers and accountants;
- Corporate executives who sit on the boards of public institutions and companies with public participation;

c) High-ranking military personnel :

- General officers and Senior officers of the army, the Police and the Gendarmerie;
- Heads of higher military training at the company level;
- Inspectors of the General Inspectorate of the State, the General Inspectorate of the Malagasy Army and the General Inspectorate of the National Gendarmerie;

d) Head of a political party;

e) Persons known to be closely associated with a PEP, including any close relative, family member through direct lineage or marriage, or any person connected by business relationships.

III. **"PEPs of international organisations"** means persons who perform or have performed significant functions in or on behalf of an international organisation, including senior management, in particular, directors, deputy directors and members of the Board of Directors, and all persons performing equivalent functions. The notion of PEP does not cover middle or lower ranking persons falling under the above categories.

IV. **PPE Relatives**

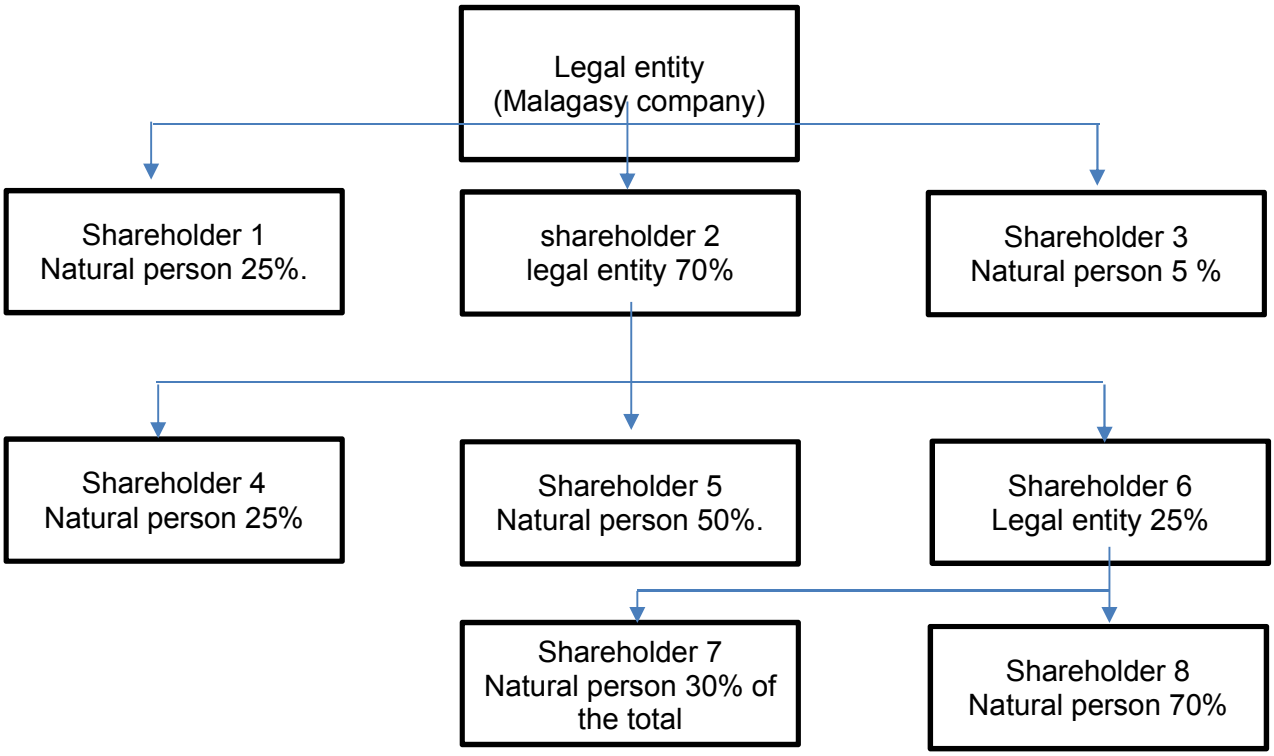
PEP close relatives extend to the family circle and the circle of influence.

The family circle which extends to direct family members and the circle of influence, known to be closely related to a PEP are also to be classified as PEP.

PPE RELATIVES	
FAMILY CIRCLE	**CIRCLE OF INFLUENCE**
Spouse, partner, fiancé(e)	Co-Beneficial Owner
Ascendants: father, mother	Co-partner/Shareholder
Descendants: children	Person representing the PPE and carrying its interests by acting in its name in an official or unofficial way (Lawyer, notary, proxy, representative)
First degree relatives including spouse: father-in-law, mother-in-law, son-in-law, daughter-in-law	Personal Advisor
Little children	Personal employees: driver, bodyguard, housekeeper, nanny,...

SERVICE DE RENSEIGNEMENT FINANCIER
REPOBLIKAN'I MADAGASIKARA
SAMIFIN

APPENDIX 05: HOW TO IDENTIFY A BENEFICIAL OWNER



The natural persons to be considered as beneficial owners are Shareholders 1 and 5 because they hold respectively 25% and 35% of the company MALAGASY.

SERVICE DE RENSEIGNEMENT FINANCIER
REPOBLIKAN'I MADAGASIKARA
SAMIFIN

APPENDIX 06: NON-PROFIT ORGANISATIONS

Non-Profit Organisations, abbreviated to "NPOs", are classified as "high risk" because they can be used for terrorist purposes or terrorist financing.

A non-profit organisation is classified as "high risk" if it:

- Receives donations from countries deemed at risk by the FATF, conflict zones,
- Operates in conflict zones or countries considered to be at risk by the FATF.
- Has one or more beneficial owners with the status of Politically Exposed Person;
- Operates in areas considered to be at risk;
- Is not known and/or has no reputation in its areas of operation,
- Lacks clarity and transparency in management (lack of certification of annual accounts, etc.)

However, depending on their risk assessment, reporting institutions may classify as medium risk non-profit organisations that:

- Are supported and funded by internationally recognized bodies (World Bank, European Union, ...);
- Carry out verifiable activities, works and projects;
- Do not have leaders or board members who are Politically Exposed Persons;
- Publish annually their activity and financial reports;
- Do not meet the criteria for high risk classification above.

SERVICE DE RENSEIGNEMENT FINANCIER
REPOBLIKAN'I MADAGASIKARA
SAMIFIN