UIFAND
UNITAT D'INTEL·LIGÈNCIA FINANCERA D'ANDORRA

TECHNICAL COMUNIQUÉ CT-01/2024

Veedors digitals

Andorra la Vella, 25th January 2024

Dear Sirs and Madams,

The First Additional provision of *Law 24/2022, of June 30, on the digital representation of assets through the use of cryptography and distributed ledger technology and blockchain* (hereinafter, "Law 24/2022"), published in the Official Gazette of the Principality of Andorra on July 20, 2022, establishes that "*Legal entities engaged in financial activities that operate with digital assets, whether through primary or secondary markets, as defined in this Law, are considered obliged entities in the terms referred to in Law 14/2017, of June 22, on the prevention and fight against money laundering or values and the financing of terrorism*" (hereinafter, "Law 14/2017"). Additionally, the First Additional provision of Law 24/2022 adds that "*Individuals or legal entities acting as "veedors digitals" are considered obliged entities in the terms referred to in Law 14/2017, of June 22, on the prevention and fight against money laundering or values and the financing of terrorism*."

In accordance with section vii.2 of Article 8 of Law 24/2022, "*the "veedor digital" must be a lawyer or certified economist...*," and although they are non-financial obliged entities, anti-money laundering and counter-terrorism financing (hereinafter, "AML/CTF") controls and other risk mitigation measures by these groups may not be adequate in business relationships established as *"veedors digitals"*.

In this regard, **the most relevant characteristic is that the *"veedors digital's"* clients are virtual asset services providers (hereinafter, "VASPs")**, which are any natural or legal person who as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies; ii) exchange between one or more forms of virtual assets; iii) transfer of virtual assets; iv) safekeeping or administration of virtual assets or instruments enabling control over virtual assets; v) participation in and provision of financial services related to an issuer's offer or initial sale of a virtual asset[1], **which, due to the nature of its activity, are inherently exposed to a multitude of AML/CTF risks.** Precisely for this reason, it is essential to specify as concretely as

[1] In accordance with article 3.21 of Law 14/2017.

possible the obligations of the “veedors digitals” in terms of money laundering and the financing of terrorism (hereinafter, "AML/CTF") prevention.
Therefore, considering the legal requirements and obligations of the “veedors digitals” outlined in both Law 24/2022 and *Decree 478/2022, dated November 23, 2022, published in the Official Gazette of the Principality of Andorra on November 30, 2022, approving the Regulation for the development of the requirements to act as a “veedor digital”, the obligations of the “veedor digital”, and the disciplinary and sanctioning regime*, it is necessary that the internal AML/CTF control systems developed by the “veedors digitals” be sufficiently robust to carry out their tasks appropriately and efficiently.

For this reason, this Technical Communiqué aims to specify and detail the AML/CTF obligations to which the “veedors digitals” are subject, providing a comprehensive description of these obligations. Special emphasis is placed on understanding and mastering the activity to which the “veedor digital” is becoming bound or that the provider of virtual assets services is undertaking, as well as understanding the characteristics of the virtual assets with which the service provider operates, in relation to potential AML/CTF risks.

Based on the abovementioned, the minimum obligations to which “veedors digitals” are subject are detailed below:

a) Appointment of the Internal Control and Communication Body and the representative before the UIFAND

In accordance with the provisions of Article 40.2 of Law 14/2017, Article 15 of the Regulation implementing Law 14/2017 approved by Decree 76/2022, dated March 2 (hereinafter, the Regulation), and CT-04/2018 issued by the UIFAND on June 21, 2018, the “veedors digitals” which are legal entities must appoint an Internal Control and Communication Body (hereinafter, "OCIC") and notify it to the UIFAND. In the case of the “veedors digitals” being natural persons, this person assumes the role of OCIC, although notification to the UIFAND is also required.

Moreover, obliged entities to be register as “veedors digital”, even if they have already communicated their OCIC to the UIFAND in connection with their economic activity, such as lawyers or economists, must formally notify the UIFAND, using the prescribed form[2], of the modification of their activities, including that of a “veedor digital”.

[2] Available on the UIFAND website at the following link: https://www.uifand.ad/en/publications/forms

b) Preparation of their Individual Risk Assessment

Based on the legal obligation stipulated in Article 5 of Law 14/2017 and its regulatory development in Article 3 of the Regulation, “veedors digitals”, as obliged entities, must have an Individual Risk Assessment (hereinafter, "ERI").

This assessment must be prepared before initiating activities to identify the potential AML/CTF risks to which the “veedor digital” will be exposed and, consequently, design suitable mitigating measures. In this regard, obliged entities must create and incorporate a new section within their ERI through a sufficiently detailed study regarding the “veedor digital” activity, considering it in relation to the overall risk level of the entity.

Additionally, the ERI must consider the risks detected by the VASPs, as well as the measures implemented by the provider. In any case, when facing a specific AML/CTF risk, the “veedor digital” cannot simply rely on knowing that the virtual asset service provider has implemented some mitigating measure; rather, they must design the necessary actions to ensure that the risk is under control and that the implemented measures are appropriate and efficient according to their design.

c) Application of Due Diligence Measures

In accordance with the provisions of Article 8 of Law 14/2017 and considering the applicable rules for “veedors digitals”, they must apply due diligence measures in the following cases:

- when establishing a business relationship (Article 8.a of Law 14/2017),
- when there is a suspicion of money laundering or financing terrorism, regardless of any derogation, exemption, or threshold (Article 8.e of Law 14/2017),
- when there is a suspicion about the veracity, adequacy and validity of previously obtained customer identification data (Article 8.f of Law 14/2017), and finally,
- when such transactions are listed as susceptible to entail money laundering or terrorist financing or are qualified of special monitoring by the UIFAND by means of a Technical Communiqué (Article 8.g of Law 14/2017).

In accordance with Article 9 of Law 14/2017, due diligence measures include the following:

- identification and verification of the client's identity based on reliable documents before establishing a business relationship or occasional transaction,

- identification and verification of the beneficial owner's identity before establishing a business relationship or occasional transaction, and understanding the control structure and ownership of the client (Article 10 of Law 14/2017),
- understanding the purpose and nature of the business relationship,
- implementation of measures to assess and understand the source of funds, and finally,
- continuous monitoring of the business relationship.

According to Article 9.3 of Law 14/2017, "*Parties under obligation determine the extent of such customer due diligence measures on a risk-sensitive basis."* **Therefore, due diligence measures must be graduated based on the risk determined by the "veedor digital" according to the client's typology, the service provided, or the type of business relationship established, among other factors** (see Articles 11 and 12 of Law 14/2017). For example, the risk associated with a client involved in issuing digital assets will not be the same as that of a client providing custody services for digital assets, with the former posing a higher risk.

Additionally, regarding enhanced due diligence measures, special attention should be given to their application concerning business relationships or transactions involving high-risk countries, as designated by the FATF and the European Commission, published by the UIFAND on its website through Technical Communications.

Furthermore, the "veedor digital" must have mechanisms for identifying politically exposed persons (PEPs) and adopt suitable measures to determine the origin of funds and wealth.

Otherwise, **the "veedor digital" must ensure that its client, hence the VASP, also has relevant due diligence procedures in line with its activity and the inherent risks**. In this sense, the "veedor digital" should:

- be aware of the nature and complexity of its clients,
- know the internal AML/CTF procedures of its clients,
- know the jurisdictions to which its clients are exposed, and if applicable, the AML/CTF regulations related to virtual asset service providers in those jurisdictions, and also,
- understand the activities carried out by its clients and the associated risks. Therefore, it is advisable for the "veedor digital" to have a document and/or list with possible scenarios of money laundering and terrorism financing that include virtual asset service providers and virtual assets.

Additionally, according to Article 9.6 of Law 14/2017, the "veedor digital" must also ensure that their clients comply with the requirements of this legal provision, which results in the following obligations:

- Conducting a risk analysis related to the development of new products and business practices that include the use of emerging technologies, which must include a detailed study of the threats faced and system vulnerabilities arising from the activities that the virtual asset service provider intends to carry out.
- Determining, based on the detected risks, the corresponding mitigating measures to address identified needs and shortcomings.

Thus, the obligations derived from Article 9.6 of Law 14/2017 apply both to known clients expanding their activities related to new technologies and to newly established clients engaging in activities related to new technologies.

Finally, **it is worth noting that in terms of due diligence, the obligations of the "veedors digitals" and VASPs[3] are different** and, consequently, do not involve a transfer of obligations from one to the other.

d) Obligation to Report Suspicious Transactions

According to the obligation outlined in Article 20 of Law 14/2017, "veedor digital", as obliged entities, are required to: i) report to UIFAND any transaction or project related to funds for which there is certainty, knowledge, suspicion, or reasonable grounds to suspect that they are the product of criminal activity or related to terrorism financing, and promptly respond to any additional information requests from UIFAND, and ii) provide UIFAND with all the information requested in the exercise of its functions.

Reports of suspicious transactions must be prepared in accordance with the instructions available on the UIFAND website and submitted using the designated form[4], duly completed.

[3] VASPs are designated as obliged entities according to article 2.1.f) of Law 14/2017.

[4] Available on the UIFAND website at the following link: https://www.uifand.ad/en/publications/forms

e) Obligations Regarding Internal Control Measures, Internal Regulations, and Training

The "veedor digital", in line with the provisions of Article 40 of Law 14/2017 and its regulatory development in Articles 15 et seq of the Regulation, and considering that they are largely assimilated to financial obliged entities, must specifically:

- Establish internal control procedures and measures, as indicated in Article 17 of the Regulation. This includes examining and assessing the adequacy of internal control systems in terms of AML/CTF, having written internal policies and control procedures, and having a channel and procedure for reporting suspicious transactions, among other things.
- Additionally, in accordance with Article 42 of Law 14/2017, in relation to Article 18 of the Regulation, the "veedor digital" must implement measures, including training plans and specific courses on AML/CTF for their employees. This training should cover applicable legislation, money laundering typologies related to virtual assets, possible scenarios, and the procedures established by the entity to prevent money laundering and terrorism financing. The mentioned training should be adapted to the employee's responsibility and tasks.

  In line with the above, as mentioned earlier, the custodian must not only know its client but also understand the nature of its activity and the associated risks. Therefore, relevant training is necessary, relating to technical operation and in connection with the services that VASPs can provide and the inherent risks. The AML/CTF training required by current legislation should be complementary to training obligations of a more technical nature imposed on the "veedor digital" in compliance with other legal provisions that may require training by other authorities.

  Finally, note that this is a sector in constant evolution regarding both products and services related to virtual assets. Therefore, periodic and updated training is crucial for effective monitoring and continuous oversight, in line with Article 9.6 of Law 14/2017.

f) Obligation to Report Violations and Whistle-blower Procedures

In accordance with Article 91 of Law 14/2017, the "veedor digital" has the obligation to report to UIFAND potential or actual violations committed by other members within its entity, as well as by its clients. In this regard, it must:

- Have an internal, specific, anonymous, and independent channel so that its employees or persons in comparable positions can report possible internal violations, in accordance with Article 91.3 of Law 14/2017. However, the whistleblower may choose to report directly to UIFAND, and
- Directly report to UIFAND situations or conduct by virtual asset service providers, to whom it provides services as a "veedor digital", which they consider or have reason to believe may constitute potential or actual violations of any obligations related to AML/CTF.

g) Obligations Derived from Document Retention

Legal obligations establish a document retention period of five (5) years, including data and information obtained in compliance with Law 14/2017. This is related to the due diligence process, information obtained about the virtual asset service provider's activity, correspondence, meeting minutes, or other documentation related to the business relationship, and the results of the conducted analyses (Article 37 of Law 14/2017).

h) Obligation to Ensure No Business Relationship with Persons on UN List and Legislation related to the Conflict between Ukraine and the Russian Federation

Chapter nine of Law 14/2017 aims to prevent persons and entities linked to terrorism, terrorism financing, as well as proliferation or financing of weapons of mass destruction from using the financial (or non-financial) system to promote or carry out criminal activities.

Specifically, concerning the conflict between Ukraine and the Russian Federation, *Law 5/2022 of March 3, on the application of international sanctions* (hereinafter, Law 5/2022) and its subsequent regulatory development, seek to prevent the Principality from becoming a refuge for illicit activities, following measures issued by the Council of the European Union.

Therefore, the "veedors digitals", must ensure that none of the persons with whom they have business relationships (including members of senior management or directors of virtual asset service providers, as well as beneficial owners) appear on the consolidated list related to United Nations Security Council resolutions or the list locally published under the Law 5/2022.

This Technical Communication will come into effect the day after its publication.

Carles FIÑANA PIFARRÉ
Head of the UIFAND