WHITE RHINO INNOVATIONS, INC. DBA N-ACT

AML/CFT Policies & Procedures Manual

Version 1.3

For Internal Use – White Rhino DBA N-ACT

Table of Contents

1. Document History

Revision History

This log can be used by the Compliance Officer to track the updates to the AML Compliance programme documents. If the programme is reviewed and no significant changes are made to a document, then there should still be a line item that states that the programme was reviewed, and no significant changes were made. This document may also be used to evidence to reviewers and regulators that regular programme updates have occurred.

Date	Version	Description of Changes	Drafted by
08 January 2023	1.0	Completed, revised and updated scope, client onboarding details, KYB, KYC Tiers	White Rhino
01 March 2023	1.1	Revised risk classifications for both countries	White Rhino
27 October 2023	1.2	ML/TF/PF Definitions, Stages of Money Laundering, Client Risk Assessment forms, Business Declaration Form, Declaration of UBOs form, Internal Suspicious transaction form, Appendices A-D	Dr Ojas Kikani

Review & Approval

Date	Version	Full Name	Role
15 August 2022	1.1	Ojas Kikani	Board member
31 October 2022	1.2	Ojas Kikani	Board member

2. Glossary & Abbreviations

The following table is a list of common terms and abbreviations widely used throughout this document.

Abbreviation	Full description
AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism
AMLD5	5th Anti-Money Laundering Directive
BRA	Business Risk Assessment
CDD	Client Due Diligence
CRA	Client Risk Assessment
CSO	Customer Support O Table 32 - Accepted documents for type of company officer
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCO	Financial Control Officer
FIAT	Fiat currency denomination
FIU	Financial Investigative Unit
KYB	Know Your Business
KYC	Know Your Client
KYT	Know Your Transaction
ML	Money Laundering
MLAT	Mutual Legal Assistance Treaty
MLRO	Money Laundering Reporting Officer
OFAC	Office of Foreign Assets Control (US)
PEP	Politically Exposed Person
POA	Proof of Address
RO	Designated Reviewing Officer
SDD	Simplified Due Diligence
SOF	Source of Funds
SOW	Source of Wealth
STR	Suspicious Transaction Report
TF	Terrorism Financing
VA	Virtual Asset
VASP	Virtual Asset Service Provider

The following table provides definitions for certain terms widely used throughout this document.

Term	Description
Blockchain	A cryptographically secure digital ledger that maintains a record of all transactions that occur on the network and follows a consensus protocol for confirming new blocks to be added to the blockchain.
Virtual Asset	As established by the FATF definition: "A digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value." It is also popularly known as "cryptocurrency", "crypto asset" or "virtual currency"
Fiat currency	Currency, money or representation of value which is the money issued by a sovereign country or territory and that is designated to be legal tender. Examples of fat currencies include: Euros, British Pounds, U.S. Dollars, among many others

3. Definitions of Money Laundering, Financing of Terrorism and Proliferation Financing

Money Laundering

Money laundering has been defined as the act or attempted act to disguise the source of money or assets derived from criminal activity. It is the effort to transform "dirty" money, into "clean" money. The money laundering process often involves:

The placement of the proceeds of crime into the financial system, sometimes by techniques such as structuring currency deposits in amounts to evade reporting requirements or co-mingling currency deposits of legal and illegal enterprises;

The layering of these proceeds by moving them around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail; and

Integrating the funds into the financial and business system so that they appear as legitimate funds or assets.

Financing of Terrorism/Terrorist Financing

Terrorism is the act of seeking for political, religious or ideological reasons to intimidate or compel others to act in a specified manner. Terrorist financing is the financing of terrorist acts, and terrorists and terrorist organisations. This involves the generation and movement of funds for the sole purpose of committing terror acts or sustaining a terrorist network or organization.

A successful terrorist group, much like a criminal organization, is generally able to obtain sources of funding and develop means of obscuring the links between those sources and the uses of the funds. While the sums needed are not always large and the associated transactions are not necessarily complex, terrorists need to ensure that funds are available to purchase the goods or services needed to commit terrorist acts. In some cases, persons accused of terrorism may commit crimes to finance their activities and hence transactions related to terrorist financing may resemble money laundering.

Financing of Proliferation (PF) of Weapons of Mass Destruction/ Proliferation Financing

Proliferation financing is defined as "the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."

Proliferation of weapons of mass destruction can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles).

4. Business and AML Program Overview

1. White Rhino Innovations, Inc. DBA N-Act & it's related companies is hereby referred to as "we", "us", "our", "Company", "the Company".

2. The Company is a regulated VASP entity , under virtual currency service provider license 032324-A

3. The Company implements, monitors, upkeeps and where necessary establishes adequate procedures for the attainment of its AML/CFT policy objectives. The Company supports the regulatory objective of maintaining the reputation of the European Union with zero tolerance for criminal activity and creating a culture of compliance. Against this backdrop, the company ensure the development of internal policies, procedures and control for, inter alia:

- having an adequate management structure to supervise the Company's operations;
- appointing a MLRO with overall responsibility for AML/CFT compliance;
- carrying out appropriate CDD via established KYC or KYB procedures as outlined in the Risk Assessment and established Procedures;
- implementing a risk assessment procedure for assessing client risk;
- monitoring the client's activity and transactions;
- detecting and reporting any suspicious transactions/activity to the respective FIU;
- retaining and preserving all relevant client information and documentation in its possession that may be required by the relevant authorities for the investigation of suspicious activities;
- cooperating with relevant authorities as necessary and required by law;
- developing and maintaining procedures on internal control, risk assessment, risk management, compliance management and communications;
- regularly reassessing its AML/CFT policies, as to ensure its continued applicability with updates in legislation;
- training its employees on AML/CFT legislation, procedures, reporting and data handling requirements.

5. Document Review

1. This body of Policies and Procedures shall be reviewed at least on an annual basis and where otherwise it is required by a change in applicable legislation. The review will be initiated and carried out by the MLRO and approved by the Board of Directors.

2. The Policy review shall have in consideration whether:

- The Company has grown or shrunk to a point that certain policies and procedures may no longer be effective;
- The legal environment in which the Company operates has changed in a way that impacts the policies and procedures;
- The Directors, Managers or concerned employees have relevant feedback or are suggesting changes;
- The Policy is being effectively implemented and enforced, and what could be done to improve it.

6. Applicable Law

The central piece of legislative instrument under Estonian law regulating AML/CFT and applicable to the Company and its operations is the Law on preventing the use of the financial system for the purpose of money laundering or financing of terrorism. This transposes the European Union's 5th Anti-Money Laundering Directive[1] (**AMLD5**) into national law.

[1] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 of May 2018 on the prevention of the use of the Financial System for the purpose of money laundering or terrorist financing.

7. Applicable Business Model

As the Company's core business relies on the conversion of virtual assets to and from other currencies on behalf of its clients, it employs multiple operating business models, targeting different client audiences (individual and corporate clients), employing different providers, and onboarding procedures accordingly. Due to the differences in scope, it is important to make a distinction between its due client diligence and procedures where applicable.

Name	Client Type	Applicable Due Diligence
Settlement Services	Business Entities	Know Your Business (**KYB**)
Wallet Services	Natural Persons	Know Your Client (**KYC**)

Table 1 - Applicable Due Diligence for each service

7.1. Settlement Services

1. Settlement services are exclusively provided to institutional clients (hereinafter also "Merchant", "Merchants").
2. The Merchant is a validly existing business entity and/or established corporation which already offers goods and services to its customers and wishes to settle their received virtual asset funds in fiat currency.
3. The Company provides Merchants with the access to a web-based platform which enables them to accept virtual assets as payment for goods and services they provide.
3. The Merchant instructs the Company to provide, resourcing to a third-party provider, for the conversion of the virtual assets into fiat currency through traditional bank settlement.

7.2. Wallet Services

1. The wallet services provided by the Company is a mobile application that allows natural persons (hereinafter also "user", "users") to store, deposit and withdraw virtual currency, as well as exchange virtual currencies.
2.The wallet services are offered and available to users who are 18 years of age or older. Any registration by, use of or access to these services by anyone under 18 is unauthorized and in violation of these terms. By using the services, you represent and warrant that you are 18 years of age or older and that you agree to abide by these terms.

3. Users are able to spend their wallet balance with an associated debit card (issued and governed by a third-party issuer). Users are able to deposit and withdraw in FIAT currency to and from their account via bank transfer.
4. Users interacting with digital assets as investments should be aware that all investments involve risks, including the risk of loss of some or all assets. Losses are not insured, and the user assumes responsibility for all losses. Users are advised to exercise caution, conduct research, and not to transact more than they can afford to lose.

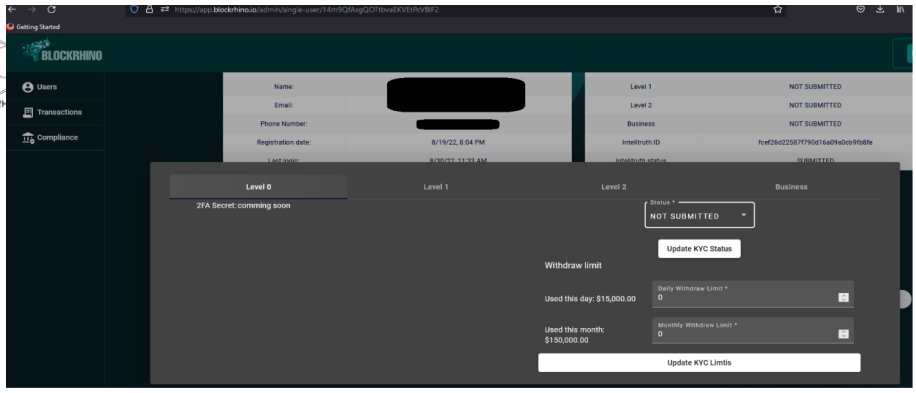
8. Due Diligence Procedures for Settlement Services

This section refers to the procedures in place for the on-boarding, recording and review of client profiles which apply to obtain an Account. Such process is based on our current AML Policies and Procedures, BRA, CRA and the available software integrations with our Back Office tools. Elements of these processes generally involve human review or intervention at one or more steps in order to complete.

8.1. Initial client review procedures

The initial client review attends the following procedure:

a) The RO will maintain an open tab of the Back Office Tool, by performing login with assigned credentials. The RO will also login and keep open the internal Compliance Intelitruth Channel, in order to receive real-time new client onboarding requests.
b) Each new KYB submission generates an automatic submission on a dedicated internal Intelitruth channel, where all ROs are notified. The name of the applicant and a link to the Back Office Tool are listed in each individual entry.
c) In the corresponding channel, a single RO takes ownership of the process, by adding an indicator mark on-channels. This ensures only one RO reviews the process.
d) In the Intelitruth Channel, the RO follows the link "NOT SUBMITTED" or accesses the corresponding file directly on the Management Tool (MT) under the Compliance Tab. The RO will click "Manage KYC".



e) ROs can easily consult the Client index in real time in the Back Office Tool, including any submitted documentations, and search and filtering by relevant fields, such as KYB Status, Updated date, Sector and Country of incorporation, and others.

f) After initiating KYB, the RO will review all the associated information and documentation required, considering, but not limited to, the following remarks:

- Certificate of incorporation or equivalent legal document
  - It should be an official document issued by a an official entity;
  - The type of document should be suitable to the specific type of incorporated entity, as described in the Business Entity Incorporation Document section;
  - For confirmation that the entity in the document exists, a search will be performed, using official databases publicly accessed for this purpose (which vary depending on the jurisdiction of incorporation);
  - The name of the company should be searched against Sanction lists;
  - All company details on the document will be compared and must match the ones submitted at onboarding.
- Jurisdiction of incorporation
  - It should be assessed whether the country is correctly identified and whether it is a High Risk jurisdiction;
  - Non-serviced jurisdictions will not be accepted.
- Official Website of the Business
  - The link should be pointing to a publicly visible website;
  - The website Policies or Terms should mention the name of the company and the company's address referred upon onboarding;
  - The products and services mentioned on the website should match the company's stated business activities.
- Sector of Business

- The company's sector should be accurate and correspond to the actual company industry;
- The company's sector will be evaluated considering a risk based approach;
- A company operating in a non-serviced sector will not be accepted;
- A company operating in a sector considered High-Risk will be required extra steps of due diligence;
- The company's sector will be compared to match the sector mentioned in the certificate of incorporation, the country's official Registry and the official website.

g) Applicants who have not yet completed KYB and have not been through the review process and manually approved by the RO are not able to settle any funds to their bank account.

h) The RO will screen the company for possible Sanctions, by searching for matches of its legal name and registration number with publicly available sanction lists.
This is especially relevant for companies incorporated outside of the European Union and any high risk jurisdictions.

i) During the client profile review, the RO must create notes for every comment on the quality of information and/or documentation submitted, every concern and consideration raised, any follow-up to request more information, any emails/messages exchanged (either directly or through a CSO).

Commented [c1]: Image here not coming up

j) Whenever there are concerns regarding the approval/rejection of an applicant, the RO will mark the applicant entry with the status of “Pending Approval" on the Intelitruth Compliance Channel (with a reaction on the corresponding Intelitruth notification). This action signals other ROs of the action taken for that client.

k) In the case of insufficient and/or inappropriate submitted information/documentation, the RO must contact the applicant through their stated profile email address requesting additional documentation. Until the RO is sufficiently satisfied with the information/documentation provided, the corresponding account will not be approved.

At any point during this process, if any doubts arise the situation should be escalated to involve the MLRO or a Senior Compliance Officer and assist in the process.

l) In the case of insufficient and/or Inadequate information or documentation the RO may:

- Refuse to approve and block the account due to perceived risk - the applicant will be informed via their designated profile email of the denial of onboarding, without mentioning the specific reasons that triggered this result;
- Set the account as pending approval - proceed to contact the applicant via their designated profile email requesting additional clarifications and/or documentation;

- Escalate the matter to a Senior Compliance Officer or MLRO if the case requires further analysis and in case of suspicion of money laundering, fraud or perceived unlawful behaviour.

m) Once the RO is satisfied with the information and/or documentation received, they should approve the KYB on Back Office Tool. This action will automatically trigger a message notifying the account approval.

The RO will also add a checkmark reaction to the corresponding Intelitruth notification on the Intelitruth Compliance Channel (with a reaction on the corresponding Intelitruth notification). This action signals other ROs of the action taken.

Commented [c2]: Image here not coming up

n) Whenever the information requested is not acceptable or the applicant does not respond to the ROs email query within 10 business days, the account will be blocked. The RO will select the option "block all activity" in the corresponding profile (blocking both incoming virtual asset transactions and outgoing settlements) or "suspend settlements" (blocking all outgoing settlements to the bank account). The identification of the account will also be added to the record of Blocked Accounts.

o) At any moment during the process, if the RO is suspicious of illicit behavior, the situation should be escalated and the MLRO notified.

8.2. Follow-up Client Review Procedures

1. Profiles who have been reviewed and approved for Initial Business Due Diligence, will be required to provide additional information once they have reached a set threshold amount in settlements to their bank account.

2. In such cases, the Client will be contacted by the RO and required to submit further information and documentation.

3. Until this process is completed, clients are unable to settle any accrued amount to their bank account.

4. Depending on the specific type of incorporated entity, the RO will ask the client for some of the following information and documentation to be submitted:

- Bank statement not older than 3 months;
- The indication of the percentage held by the beneficial owners, that is, the person or persons who own or control, directly or indirectly, a sufficient percentage of shares or voting rights or participation in the capital of the legal person (if not applicable, the indication of the persons who exercise control by other means over the legal person or, ultimately, of the persons who hold the top management);
- Identity documents for all natural persons that have a significant control over the business;
- Proof of address documents for all individuals with significant control over the business;
- A declaration of their status as PEP for all individuals with significant control over the business;
- A document signed by the board of directors or CEO authorising representatives to operate and manage the account on behalf of the company.

8.3. Business Due Diligence

1. As part of our onboarding process, the Company will require documentation to verify the client's proof of incorporation. In this regard, the section Document Acceptance Policies - Business Incorporation refers to a non-exhaustive list of documentation which we can accept as proof.

2. Any documentation that is not specifically mentioned in the list should be analysed in terms of its adequacy in identifying both the entity by name as well as its address (in case of proof of address). Where in doubt, the employee must not accept the client before confirming with the MLRO, Designated Employee or one of the Senior Officers of the Company.

3. If we are unable to complete the necessary procedures due to the reluctance offered by the client to provide the necessary documents, data or information, we cannot enter into the business relationship or carry out the occasional transaction with such client and, if there is a suspicion of ML/FT, the MLRO or Designated Person is to file a report with the FIU. Any funds held by us must be frozen in accordance with our Reporting Procedures.

8.3.1. Simplified Business Due Diligence (Tier B1)

1. Upon onboarding, the Company requires information and documentation pertaining to the business activities involved. The client must provide information, such as contact details, country of incorporation, business sector, company's legal name, business address, store URL and bank settlement information. Additionally, a certificate of incorporation or equivalent (depending on the company's category) must be submitted for the account creation to be concluded.
2. If the RO is unable to ascertain all relevant information, the client will be contacted to provide clarifications and information/documentation as necessary.
3. For sole traders within the same limit of withdrawals, the RO will request for: identity document; proof of address dated within the last 3 months; selfie holding the ID card. These documents are verified through our identity verification provider.

Hi <Client Name>, Thank you for your registration with White Rhino Innovations, Inc. DBA N-ACT To complete your account verification, please provide the following information/documents: 1. Your ID Card; 2. Proof of your Personal Address dated within the last 3 months; 3. A selfie holding your ID card; It goes without saying that the information and contents of this documentation must be clearly visible and legible. Please bear in mind that the next batch of settlements will only be possible after this process is complete. If you have any questions at all, don't hesitate to ask! Cheers,
Table 2 - Business due diligence for sole traders - Email template

8.3.2. Initial Business Due Diligence (Tier B2)

Whenever withdrawals exceed amounts above 500 EUR and below 10,000 EUR per year, the following information and documentation is requested:

- Owner/Representative full name;

- Business tax identification number;
- Business proof of address.

8.3.3. Full Business Due Diligence (Tier B3)

1. Whenever withdrawals equal or exceed amounts of 10,000 EUR per year, the following documentation is requested:
   - A company bank statement not older than 3 months;
   - Identification document of all individuals with significant control over the business;
   - Proof of address of all individuals with significant control over the business;
2. If the company is publicly listed, the Company will require a document signed by the Board of Directors or CEO authorising representatives to operate and manage the account on behalf of the company.
3. For sole traders within the same limit of withdrawals, the RO will request for a bank statement not older than 3 months (in addition to the elements requested in Tier 2).
4. The aforementioned information is requested as part of the following forms:
   - Declaration form for Business Entity (Appendix B), to be completed and signed by the business representative on behalf of the business entity.
   - Declaration form for Business Entity UBOs (Appendix C), to be completed and signed by each Ultimate Beneficial Owner.

Hi <Client Name>,

You will reach your yearly withdrawal limit soon! We don't want to get in your way, though, and we'd be happy to increase your associated limit. In order to do so, we are required by law to obtain some additional information and documentation.

Here's what we need:

1. The **Business Declaration Form** attached (completed and signed);
2. The **Business Owner Declaration Form** attached (one **per each** individual, completed and signed).
3. A **company bank statement** dated within the last 3 months.

For each business owner in the above declaration, please also provide:

4. An **identification document** (e.g. National Identity Card; Driving License; Passport; Residence Permit Card);
5. A **proof of address dated within the last 3 months** (e.g. tax bill, tax authority documentation, bank statement, utility bill).

It goes without saying that the information and contents of this documentation must be clearly visible and legible.

Please bear in mind that the next batch of settlements will only be possible after this process is complete.

If you have any questions at all, don't hesitate to ask!
Cheers,

Table 3 - Business and UBO identification for Tier B3 - Email template

Hi <Client Name>, Your profile is associated with higher withdrawal limits. This means there are a few extra steps to verifying your account. This is **required by law**. If you could just provide us with some additional information and documentation, we'll get it done in no time. Here's what we need: 1. The **Business Declaration Form** attached (completed and signed); 2. The **Business Owner Declaration Form** attached (one **per each** individual, completed and signed by **each** individual - one per each). 3. A **company bank statement** dated within the last 3 months. For <u>each business owner</u> in the above declaration, please also provide: 4. An **identification document** (e.g. National Identity Card; Driving License; Passport; Residence Permit Card); 5. A **proof of address dated within the last 3 months** (e.g. tax bill, tax authority documentation, bank statement, utility bill). It goes without saying that the information and contents of this documentation must be clearly visible and legible. Please bear in mind that the next batch of settlements will only be possible after this process is complete. If you have any questions at all, don't hesitate to ask! Cheers,
Table 4 - Business and UBO identification for Tier B3 upon account approval - Email template

8.3.4. Enhanced Due Diligence for specific business sectors

1. In some instances, a business entity may be required additional due diligence beyond Full Business Due Diligence during the initial onboarding phase. This specifically applies in cases where the type of business entity engages in an activity or sector considered to be of inherent High Risk or

is incorporated in a High-Risk jurisdiction, as described in the CRA matrix. Common cases may include, but not limited to:

- Businesses incorporated in a High Risk jurisdiction;
- Businesses with an unusually complex ownership structure;
- Businesses providing Financial Services;
- Businesses operating in a designated High-Risk sector or activity, as outlined in the Business Sector Acceptance Policy section. For example, business operating in Gambling, Commodities or Art & Antiques.

2. Any such Business Entities that are identified at onboarding are automatically classified as High Risk, and are requested to perform Full Business Due Diligence upfront.

3. Businesses engaging in the provision of Financial Services are required to provide at least the following additional information and documents:

- The list of jurisdictions where the business provides services;
- The type of clients served (individual, institutional or both);
- A proof of operating license or description for exemption of one;
- A document containing approved AML Policies, where Risk Policy and applicable KYC policies are detailed.

4. Businesses engaging in the provision of gambling or betting services or must provide at least the following additional information and documents:

- The list of jurisdictions where the business provides services;
- A proof of operating license or description for exemption of one;
- The user acceptance policy, including how client age is verified and enforced;
- A document containing approved AML Policies and applicable KYC policies are detailed.

Hi <Client name>,

Thank you for your registration.

As I was reviewing your profile, however, I have noticed you seem to provide financial services.
The provision of financial services (such as banking services, trading of financial products, facilitation of cryptocurrency transactions) is a regulated activity in most jurisdictions.
In such cases, as a regulated entity, we are required by law and internal policy to ask a few more questions regarding your activity, as well as obtain additional documents before proceeding.

In order to complete this process, we kindly ask you to provide the following documents:

1. The **Business Declaration Form** attached (completed and signed);

2. The **Business Owner Declaration Form** attached (completed and signed by **each** individual - one per each).

3. A **company bank statement** dated within the last 3 months.

For each business owner in the above declaration, please also provide:

4. An **identification document** (e.g. National Identity Card; Driving License; Passport; Residence Permit Card);

5. A **proof of address dated within the last 3 months** (e.g. tax bill, tax authority documentation, bank statement, utility bill).

We will also need the following information, specifically for your business category:

6. The list of jurisdictions where you provide financial services (if not already explicit in your Terms & Conditions).

7. Clarify whether you provide services to individuals or companies.

8. Send proof of the license to provide financial services or, alternatively, the license's number and a link for the verification, if available; or, in the absence of license, a thorough description of why the business is not required or exempt from licensing in the operating jurisdiction(s).

9. Provide document(s) containing your internal AML policies and account verification procedures. This must include your Anti-money laundering and Countering Financing of Terrorism policies under AMLD5 or corresponding regulation, your Risk Policy, your employed KYC processes, your designated Compliance Officer, as well as other applicable requirements.

It goes without saying that the information and contents of this documentation must be clearly visible

and legible.

Please bear in mind that the next batch of settlements will only be possible after this process is complete.

If you have any questions at all, don't hesitate to ask!
Cheers,

Table 5 - Business Due Diligence for Clients providing Financial Services - Email template

Hi <Client name>,

Thank you for your registration.

As I was reviewing your profile, however, I have noticed you seem to provide services related to gambling activities.
As this is a regulated activity in many jurisdictions, we are required by law and internal policy to perform extra due diligence, asking a few more questions, as well as obtain additional documents before proceeding.

In order to complete this process we kindly ask you to provide the following documents:

1. The **Business Declaration Form** attached (completed and signed);

2. The **Business Owner Declaration Form** attached (completed and signed by **each** individual - one per each).

3. A **company bank statement** dated within the last 3 months.

For each business owner in the above declaration, please also provide:

4. An **identification document** (e.g. National Identity Card; Driving License; Passport; Residence Permit Card);

5. A **proof of address dated within the last 3 months** (e.g. tax bill, tax authority documentation, bank statement, utility bill).

We will also need the following information, specifically for your business category:

6. The list of jurisdictions where you provide services (if not already explicit in your Terms & Conditions);

7. A proof of operating license (or a description for exemption of one);

8. Your user acceptance policy, including how client age is verified and enforced, and how the services are restricted to adults.

9. A document containing approved AML Policies and applicable client identification (KYC) policies.

It goes without saying that the information and contents of this documentation must be clearly visible and legible.

Please bear in mind that the next batch of settlements will only be possible after this process is complete.

If you have any questions at all, don't hesitate to ask!
Cheers,

Table 6 - Business Due Diligence for Clients providing Gambling Services - Email template

8.3.5. Due Diligence on the Business Beneficial Owners

1. As part of our on-boarding process, and at the appropriate Tier, the Company does require documentation to verify the client's ultimate beneficial owners (UBOs).
2. The identification of the natural persons who are the ultimate beneficial owners consists in the following elements:

- A Business Owner declaration form, which must be completed and signed (Declaration form for Business Entity UBO – Appendix C
- A valid and accepted Proof of Identity Document (following our Document Acceptance Policies)
- A Proof of Address Document (following our Document Acceptance Policies)

9. Due Diligence procedures for wallet services

9.1. Initial Client Review Procedures

The initial client review attends the following procedure:

a) The RO will maintain an open tab of the Back Office Tool on the browser, by performing login with assigned credentials. The client on-boarding requests will be regularly checked.

b) The RO will simultaneously maintain an open tab of the service provider Onfido on the browser and regularly check for new client on-boarding requests.

c) The Back Office is updated with every new on-boarding request that completes the identity verification process Applicants failing to complete this process are not allowed to access any features or functions of the mobile app.

d) Applicants are automatically blocked in the following situations:
   - The identity verification is not concluded;
   - The client claims to be a Politically Exposed Person;
   - The results from Onfido's assessment are not all marked as “clear” and were not ascertained by the RO as false positives.

e) Upon the successful verification on Onfido the RO will review the following elements:
   - ID Scans;
   - Facial Scans;
   - Address and phone number;
   - SOW/SOF Self-Declarations;
   - Sanctions, PEP, Adverse Media and Watchlist report;
   - Document Verification Report;

f) The RO will review the details of the SOW and SOF self-declarations whenever necessary.

g) The RO should insert notes in the Back Office in the following, but not limited to, circumstances:
   - The reasons of the decision to reject/suspend the Client;
   - Any comments on the quality of the documentation or actions to be taken by the RO;
   - Any requests and replies received from the Client concerning information supplied or missing.

h) In case of insufficient/inadequate information or documents, the RO may:
   - Refuse to approve the client and block the account;
   - Request Support to contact the Client via Intercom and request additional information/documents pending approval;
   - Report the matter to the MLRO in case of suspicion of ML or any other criminal behaviour.

i) Requests of Information must be as follows:
   - the RO must ensure that any request for Information must tally with the appropriate procedure in place for the given circumstances and risk rating of the client;
   - all tickets issued to a CSO are gathered in a separate tool where it’s possible to access all the requests performed for each client;

- once the RO is satisfied with the information and documentation received a recommendation shall be made to increase the limits in accordance with the Capital Limitation Policy;
- RO's decision will be communicated to the client via Intercom;
- failure of a client to provide the information or documents requested within 10 days will automatically result in the Blocking of the Account till all information is provided.

j) If the client is a confirmed PEP, the RO will engage with a CSO in order to contact the client and further obtain clarifications/documents, such as the client's title/position, motivation to open the account or intended volume of deposits (see PEP Acceptance Policy section).

Based on the information collected, the RO will determine the type and corresponding risk of the PEP. He will then proceed to request further clarifications/documents and apply the EDD measures for PEPs, as outlined in the PEP Acceptance Policy section. Some of the actions may involve, and not limited to requesting a SOW and SOF information and documentation or a declaration of no illicit behaviour. In this case, one of the following procedures should be followed:

i) if a confirmed PEP is accepted, the RO must determine if the client has access and has enrolled in other third party provided services. If so, the RO must inform the provider(s) and share the appropriate due diligence details, in accordance to the section Obligations to notify of new clients who are PEPs.

ii) if a client was accepted, fagged as PEP, but determined to be a false-positive PEP, the RO must determine if the client has access and has enrolled in other third party provided services. If so, the RO must inform the provider(s) and share the appropriate due diligence details, in accordance to the section Obligations to notify of new clients who are PEPs.

9.2. Ongoing Transaction Monitoring

The RO will receive updates of all details and actions related to the transactions through the Back Office Tool and will add a note in the client Profile for any unusual or suspicious behavior and the action taken in accordance. This is done in accordance with the rules and methods of control established in the Transaction Monitoring Policy section.

9.3. Additional Due Diligence following increase in deposit limits

9.3.1. Basic Profile Limit

1. All clients that complete successful verification and SDD are afforded a deposit limit of the designated Tier A1 amount before triggering the need for a POA document. Once this limit is exceeded the RO must request the client to submit a POA document to continue depositing funds and making use of the App.
3. This procedure shall not apply to any Higher Risk clients.

9.3.2. Advanced Profile Limit

1. All clients that complete successful POA verification are afforded a deposit limit of the designated Tier A2 amount before triggering the need for a POF document.
2. The RO must regularly review the Back Office under "EDD Required" and the daily transaction history provided by the FCO to view profiles that have reached said limit. Once this limit is exceeded the RO must request the client to submit additional information/document as outlined in the Enhanced Due Diligence section to continue depositing funds and making use of the App. The level of documentation and information requested will depend on the risk profile of the client.
3. This procedure shall not apply to any Higher Risk clients.

9.4. Natural Persons Due Diligence

1. As part of our on-boarding process the Company will require documentation to verify the client's identification and address. In this regard, the list stated in the Document Acceptance Policies - Individual Identity Document section is a non-exhaustive list of documentation which we can accept as proof. Any documentation that is not specifically mentioned in that list should be analysed by the RO for signs of its adequacy in identifying both the client by name as well as his address (in case of proof of address).
2. Where in doubt the RO must not onboard the client before assessing the MLRO or one of the Senior Officers of the Company.
3. The Company is required to adopt standards that may be required by settlement service providers, card service providers, as well as the FIU's implementing procedures.
If we are unable to complete the necessary procedures due to the reluctance by the client to provide

the necessary documents, data or information, we cannot enter into the business relationship or carry out the occasional transaction with such client and, if there is a suspicion of ML/FT, the MLRO or Designated Person

is to file a report with the FIU. Any funds held by us must be frozen in accordance with our Reporting Procedures.

9.4.1. Simplified Due Diligence (Tier A1)

1. The Company requires the identity verification of every client through scans and certified copies of the identification documents.
2. The identification documents submitted by the client are reviewed and verified through an identity verification provider which provides both a document and a watchlist (political exposure, sanctions, adverse media, monitored lists) report.
3. A proof of address is requested once the user reaches more than €2,000 in deposits.

9.4.2. Customer Due Diligence (Tier A2)

1. The Company is required to monitor all clients' AML-CFT risk levels to ensure that its product and services are not being used for illegal activities which could harm the Company, its staff and ultimately its clients.
2. In order to make use of certain features, the client will have to provide further personal data other than that provided upon initial registration. This information is required for the purpose of completing the due diligence corresponding to each profile – such as the date of birth, place of birth, occupation, phone number and residence address, information on the SOW and SOF, political exposure, and reason for acquiring, disposing of or investing in virtual assets.
3. Additional information and documentation may be required depending on the risk status, the information submitted, the use of the App and to access additional features of the App, such as obtaining the Debit Card or depositing funds in excess of set amounts. We may ask for additional information and documentation at any time through one of the indicated contact methods.
4. Should we fail to receive the information and documentation requested within a reasonable time we may have to temporarily or even permanently block the client's account until the matter is resolved.

9.4.3. Enhanced Due Diligence (Tier A3 and above)

1. Currently, except in specific high-risk cases that are escalated directly by the MLRO, the application of EDD always takes place by default in the following instances:
   - If the client has reached the prescribed Tier Limit that demands EDD;
   - If the client is considered to be High Risk;
   - If the client is a confirmed PEP;
   - If the RO believes that the client profile or provided information is unclear or demands additional scrutiny.
2. In event that the escalation to EDD has to be applied, the below procedure is to be followed:
   a) The RO is to send the client the standard template email through Intercom as it appears below informing the client of having reached the limits and requesting the following information:
      - New deposit limit amount requested and underlying reason (if a Deposit Limit is triggered);
      - Current SOW/SOF Documentation (view Document Acceptance Policies - Individual SOW and SOF section for document acceptance details);
      - Alternative SOW, if any, and documentation thereon.
      - The country or countries of origin of such SOW.
   b) The RO must approach the client with an intimation to submit to Enhanced Due Diligence Plus in the Event that client is Flagged under Adverse Media or Sanctions and it is difficult to ascertain if the person is the same one.

Dear <Client Name>,

Thank you for your decision to join our platform! We look forward to having your account up and running as soon as possible! But in order for us to do that we need your help.
We are required by law to obtain some additional information and documentation from you before we can proceed with your account application.

In this regard kindly provide us with your replies to the following questions:
1. How much money and cryptocurrency do you roughly estimate you will deposit in the span of a year?
2. What is you main source of income at present
3. In which country does the income referred to in Question 2 originate?
4. Do you have additional sources of income you intend to use to fund your account? If so, where does this income originate?
5. From where do you anticipate you will be depositing the funds you will be using to fund your account? (ex. Bank Account)
6. What do you hope our product can help you with?

As part of our process of requesting such information, you may also provide us this information via a 10 minute Face to Face video call with one of our Customer Support Specialists to visually confirm your identity and status as well as to address the above queries rapidly. In this regard kindly indicate your preferred time for contact should you wish to do so.

We thank you in advance for your kind cooperation and look forward to hearing from you.

Kind Regards,
Customer Support Representative

Table 7 - Enhanced Due Diligence - Email template for questionnaire request

Dear <Client Name>
Thank you for your decision to join our platform! We look forward to having your account up and running as soon as possible! But in order for us to do that we need your help.

Currently, your profile does not fall within our current client acceptance policy without first carrying out some additional checks to confirm your identity, residence and background. This process consists of a short questionnaire and the need for some additional documentation that can include official bank statements and/or criminal records.
As part of our process of requesting such information, you may also provide us this information via a 10-minute Face to Face video call with one of our Customer Support Specialists to visually confirm your identity and status as well as to address the above queries rapidly. In this regard kindly indicate your preferred time for contact should you wish to do so.
Without the completion of this process, we aren't authorised to provide the service. Would you be willing to answer some questions and provide additional documentation?
We thank you in advance for your kind cooperation and look forward to hearing from you.
Kind Regards,
Customer Support Representative

Table 8 - Enhanced Due Diligence Plus - Email template for call request

Dear <Client Name>,

You have just reached your annual deposit limit! But do not worry we've got your back.
We look forward to having your limits increase as soon as possible! But in order for us to do that we need your help.

In order for your profile to qualify under the category of High Net-Worth Client and have higher Deposit Limits per Annum we are required by law to obtain some additional information and documentation from you before we can proceed with increasing your limits. In this regard kindly provide us with your replies to the following questions:

1. How much money and cryptocurrency do you roughly estimate you will deposit in the span of a year?
2. What is your main source of income at present?
3. In which country does the income referred to in Question 2 originate?
4. Do you have additional sources of income you intend to use to fund your account? If so, where does this income originate?
5. From where do you anticipate you will be depositing the funds you will be using to fund your account? (ex. Bank Account)
6. What do you hope our platform can help you with?

As part of our process of requesting such information, you may also provide us this information via a 10 minute Face to Face video call with one of our Customer Support Specialists to visually confirm your identity and status as well as to address the above queries rapidly. In this regard kindly indicate your preferred time for contact should you wish to do so.

We thank you in advance for your kind cooperation and look forward to hearing from you.

Kind Regards,
Customer Support Representative

Table 9 - Deposit Limit Enhanced Due Diligence - Email template for questionnaire request

a) Once the Client has provided us with the relevant information the RO must:

- Review the replies in light of the client's risk profile and information;
- Compile a list of documents to request from the Client on the basis of SOW/SOF Documentation Policy.
- Determine an adequacy of the Client's reply to Tier 1 and provide a new limit on condition of receipt of the documents.

Dear <Client Name>

Thank you for your response.

<IF DEPOSIT RELATED>

After due consideration we have decide to raise your annual deposit limit to <amount> EUR <or the equivalent in any other currency>

In order for use to complete this process we require some documentation from you to support your replies. In this regard kindly provide us with a scan/photo of the following documents:

- *(Evidence of the Source of Wealth)*
- *(Evidence of the Alternative Sources of Wealth)*
- *(Evidence of Source of Funds - Where applicable)*

Kindly note that the information and contents of this documentation must be clearly visible and legible, and that the document is in English.

<IF DEPOSIT RELATED>

Once we have received and assessed such documents, we will unlock the new Deposit Limits for your account. You will be notified directly through this current channel or via the App.

We thank you in advance for your kind cooperation and look forward to hearing from you.

Kind Regards,

Customer Support Representative

Table 10 - Deposit Limit Enhanced Due Diligence - Email template for documents provision

9.4.4. Use of Automated Systems

1. Whilst it is up to the Company to determine whether a system should be automated or whether manual monitoring would equally yield the required results such a decision depends on several factors such as the size of the Company's set-up, the number of clients and transactions, the level of risk to which it is exposed, the costs incurred, and so on. It is expected that the Company will scale and process hundreds of thousands of transactions on a regular basis, and it must therefore adopt automated systems. This ensures transactions are being monitored effectively and efficiently that permit more accurate, detailed reports on alerts to the RO.

The Company makes use of a third-party identity verification platform, which allows individual clients to upload scans of the identification documents, facial images, and short video clips as proof of liveliness. This service further performs authentication checks on the submitted identity documents, as well as visual checks, to compare the client's uploaded facial image with the image appearing on the uploaded document. Moreover, this platform performs screening of the personal data against databases of Sanctions, Politically Exposed Persons and Adverse Media. The platform is integrated with the Company's own systems and workflow for individual client onboarding, allowing the RO to review client profiles who are specifically fagged.

The MLRO and RO also have full access to the client records for manual review if necessary.

The outsourcing third party and its contractual obligations are regulated by written agreement.

9.4.5. Use of Face to Face Verification equivalent

1. It is generally recommended that Face to Face (F2F) is done as it provides us with the ability to lower the risk scoring of said client and conduct the due diligence process faster. Due to the nature of the business and onboarding being exclusively online, instead of physical presence, we use a live video call as equivalent replacement.
2. In certain circumstances specified in the BRA Matrix, we are required to conduct a F2F video call with certain high profile clients. Due to the high risk and deposit limits the following circumstances may request a F2F verification:

- Any High-Risk clients on a case-by-case basis;
- High or Medium Exposure PEPs.
- Any client who reaches the transacted volume of the last tier.

9.4.6. Establishing Jurisdiction

9.4.6.1. Multiple Nationalities

1. As part of our onboarding process for natural persons, it is important to ascertain if the individual has more than one acquired nationality and where they are currently residing. Those questions are asked directly to the client at the onboarding stage.
2. While the majority of clients will have only one nationality (their nationality of birth) matching their current place of residence, this is not always the case. We accept users having more than one acquired nationality. However, clients can only create a single account and must choose only one of their selected nationalities (stated nationality).

9.4.6.2. Residence vs Nationality

1. While under some national frameworks, an individual may be considered legally resident in more than one place at the same time, for onboarding purposes, the client must disclose a single place of residence.

2. It is important to note that the main criteria when ascertaining a client's jurisdiction for acceptance is their acquired residence, in combination with any acquired nationalities. Residence is implied to be an established legal permanent residence where the individual has established ties.

9.4.6.3. Acceptance Policy

1. We cannot accept clients that:
   - are residents in a non-serviced jurisdiction, independently of their acquired nationalities;
   - have a SOW/SOF originating from a non-serviced jurisdiction, independently of their acquired nationalities or residence.
   - are citizens, have established permanent residence permit in the United States of America or are otherwise deemed to be a "US Person", even if they have acquired residence outside of the United States of America.

2. We are able to accept clients with multiple acquired nationalities. They, however, can only create a single account under one chosen nationality.

3 We are able to accept clients who acquired nationality from a non-serviced jurisdiction and acquired residence in a serviced jurisdiction (except in the case of "US Persons", described above). In such cases, a document proving established residence in a serviced jurisdiction is required as evidence. Even if a relationship can be established, due to its nationality, the client will be considered High Risk, independently of any other factors.

9.4.6.4. Indicators of different residence

1. At the onboarding stage, there are specific profile indicators that may suggest that a client has a different jurisdiction of residence. Specifically, the following scenarios are subject to further investigation:
   - Client is a national of a non-serviced jurisdiction;
   - Client has a different stated nationality of birth than his submitted identification document;
   - Client has a different stated country of residence than his stated nationality (does not apply if both are territories within the European Union);
   - Client has a SOW/SOF originating from a jurisdiction that is different from his country of acquired nationality or acquired residence.

2. In such cases, the RO must further inquire the clients to provide evidence that they are residents of a supported country. The client must successfully respond to such an intimation within 48 hours or the account will be blocked. Furthermore, the CSO must be satisfied that the client is permanently established in the supported country and does not have SOW/SOF from a non-serviced jurisdiction.

3. Should the CSO establish or the RO suspect that the Client is substantially established in a non-serviced jurisdiction or that the SOW/SOF from a non-serviced jurisdiction the account will be blocked immediately.

Dear <Client Name>

Thank you for your decision to join our platform! We look forward to having your account up and running as soon as possible! But in order for us to do that we need your help.

We are required by law to obtain some additional information and documentation from you before we can proceed with your account application. In this regard kindly provide us with your replies to the following questions:

1. *Do you hold any alternate residence in the <Country of Nationality/Birthplace>?*
2. *Have you traveled to the <Country of Nationality/Birthplace> recently? and If so, how regularly?*
3. *Do you have any business/financial connections or sources of wealth connected to the <Country of Nationality/Birthplace> or any other country?*
4. *What is your primary source of income at present?*
5. *From which country does this income originate?*

We thank you in advance for your kind cooperation and look forward to hearing from you.

Kind Regards,
Customer Support Representative

Table 11 - Nationality clarification - Email template for questionnaire request

9.4.7. Politically Exposed Persons

9.4.7.1. Definition & Scope

The Company generally considers a Politically Exposed Person (PEP) as a natural person who is or who has been entrusted with prominent public functions including:

- head of State;
- head of government;
- minister and deputy or assistant minister;
- a member of parliament or of a similar legislative body;
- a member of a governing body of a political party;
- a member of a supreme court;
- a member of a court of auditors or of the board of a central bank;
- an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces;
- a member of an administrative, management or supervisory body of a State-owned enterprise.
- a director, deputy director and member of the board or equivalent function of an international organization;
- a relative or close associate of a person with prominent public functions.
- The Company does not consider middle-ranking or more junior officials as PEPs.

9.4.7.2. Acceptance Policy

1. This policy is aimed at addressing the methodology behind on-boarding clients who are considered PEPs and the additional verification elements the Company collects for such clients before establishing a relationship.
2. As a general rule, all PEPs are considered High Risk clients. Still, some PEP may be higher risk than others. The aim in this classification is to lower the risk level by increasing the amount of due diligence on such a person and their on-going monitoring.
3. During the onboarding stage, clients are required to declare if they are a PEP. This information is further complemented with an automated screening against known PEP databases (screened through a third party provider),, which may result in a positive or negative fag for suspected PEP.
4. A client will be fagged for review by the MLRO or RO if either:
    - Declared to be a PEP through self-declaration;
    - Suspected to be a PEP through automated screening;
5. The MLRO or RO are required to review the client information and report information to ascertain if the client is a true or a false positive.
6. If the client is confirmed to be a PEP, further information will be collected, depending on its type of political exposure, as described above. The client will be unable to conclude his onboarding until the required information and/or documentation is provided.
7. Below you find examples and the due diligence required of each risk level - Tables 10 and 11, respectively.

Direct PEP exposure		
ID	**Type of Exposure**	**Examples of individuals**
PD3	Low Direct Exposure	● Members of the administrative, management or supervisory boards of state-owned enterprises; ● Anyone exercising any of the above functions within an institution of the European Union or any other recognized international body.
PD2	Medium Direct Exposure	● Members of the governing bodies of political parties; ● Mayors of a municipality or directors of a municipal administration; ● Members of courts of auditors, or of the boards of central banks; ● Ambassadors, chargé d'affaires and other high-ranking officers in the armed forces; ● Anyone exercising any of the above functions within an institution of the European Union or any other recognized international body.
PD1	High Direct Exposure	● Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries; ● Members of Parliament or similar legislative bodies; ● Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; ● Anyone exercising any of the above functions within an institution of the European Union or any other recognized international body.
Indirect PEP exposure		
ID	**Type of Exposure**	**Examples of individuals**
PI3	Low Indirect Exposure	Family Members and Close Business Associates of Low Exposure PEPs **Family** ● the spouse, or any person considered to be the legal equivalent to a spouse; ● the children and their spouses, or persons considered to be the equivalent to a spouse; ● the parents. **Business** ● a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement with that PEP; ● a natural person known to have close business relations with that PEP;

		• a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.
PI2	Medium Indirect Exposure	Family Members and Close Business Associates of Medium Exposure PEPs **Family** • the spouse, or any person considered to be the legal equivalent to a spouse; • the children and their current spouses, or persons considered to be the equivalent to a spouse; • the parents of the PEP. **Business** • a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement with that PEP; • a natural person known to have close business relations with that PEP; • a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.
PI1	High Indirect Exposure	Family Members and Close Business Associates of High Exposure PEPs **Family** • the spouse, or any person considered to be the legal equivalent to a spouse; • the children and their spouses, or persons considered to be the equivalent to a spouse; • the parents of the PEP. **Business** • a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement with that PEP; • a natural person known to have close business relations with that PEP; • a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.

Table 12 - Indirect PEPs exposure and examples

Direct PEP exposure		
ID	**Enhanced Due Diligence Required**	**Acceptance Policy**
PD3	● Receipt of Official Government SOW/SOF Documentation ● Receipt of other SOW/SOF Documentation (where applicable) ● Receipt of Declaration of No Illicit Behaviour	Acceptance discretion can be delegated to MLRO, RO or Designated Employee.
PD3	● Face 2 Face video call; ● Receipt of Official Government SOW/SOF Documentation; ● Receipt of other SOW/SOF Documentation (where applicable); ● Receipt of Declaration of No Illicit Behaviour.	Acceptance discretion can be delegated to MLRO, RO or Designated Employee.
PD1	● Face 2 Face video call; ● Receipt of Official Government SOW/SOF Documentation; ● Receipt of other SOW/SOF Documentation (where applicable); ● Receipt of Declaration of no illicit behaviour.	Acceptance must be approved by the MLRO and by Board Member majority vote.
Indirect PEP exposure		
PI3	● Receipt of relevant SOW/SOF Documentation (where applicable); ● Receipt of Declaration of no illicit behaviour.	Acceptance discretion can be delegated to MLRO, RO or Designated Employee.
PI2	● Face 2 Face video call; ● Receipt of relevant SOW/SOF Documentation (where applicable); ● Receipt of Declaration of no illicit behaviour.	Acceptance discretion can be delegated to MLRO, RO or Designated Employee.
PI1	● Face 2 Face video call; ● Receipt of relevant SOW/SOF Documentation (where applicable); ● Receipt of Declaration of no illicit behaviour.	Acceptance must be approved by the MLRO and by Board Member majority vote.

Table 13 - PEPs exposure and Due Diligence required

10. In all cases, if the PEP has access and enrolled in additional services, the respective provider may be required to be informed, in accordance with the Obligations to Notify the provider section.

11. The list of prominent public functions is by no means exhaustive, and we are required to assess on a case-by-case basis whether a particular public function presents characteristics that would fall to be considered as a 'prominent public function'.

12. The definition of what constitutes a "family member" can vary across jurisdictions. We do not consider indirect family relationships to be considered under this definition.

13. Below you may find the email templates to request the call and the questions that must be posed upon it.

Dear <Client Name> *Thank you for your decision to join our platform! We look forward to having your account up and running as soon as possible! But in order for us to do that we need your help.* *As your profile falls under the category of a PEP (Politically Exposed Person) we are required by law to obtain some additional information and documentation from you before we can proceed with your account application.* *As part of our process of requesting such information we would kindly invite you to have a 10-minute Face to Face video call with one of our Customer Support Specialists to visually confirm your identity and status as well as to address some of our standard queries rapidly. In this regard kindly indicate your preferred time for contact.* *Furthermore, we would require scans of the following original documentation from you:* ● *Documentary evidence of your Source of Wealth (such as your Official Government Payslip);* ● *Documentary evidence of your Source of Funds (that is the source from where you wish to deposit to your account - including but not limited to a bank statement);* ● *Any alternate Source of Wealth or Funds which will be used to fund you account; and* ● *A copy of the Declaration of No Illicit Behaviour signed by you as the account Holder (attached below).* *Kindly note that the information and contents of this documentation must be clearly visible and legible, and that the document is in English or Portuguese.* *We thank you in advance for your kind cooperation and look forward to hearing from you.* *Kind Regards,* *Customer Support Representative*

Table 14 - PEP clarification - Email template for call request

- What is the Title of your role that makes you a PEP?
- What is the nature of this role?
- What are your responsibilities and obligations tied to this role?
- What special public/executive powers do you enjoy as part of this role?
- Do you confirm that you have never used such powers or your influence in a manner to advance your own personal gain or that of a close personal/business relationship?
- Do you confirm that you are and never were subject to any undue influence or coercion by any third party whom you aren't legally required to answer to?

Table 15 - PEP clarification - Questionnaire upon the call

9.4.8. Refusing a client

1. In the case the RO decides to refuse a customer at the onboarding stage, either due to perceived excess risk or other factors, the client must be informed of this fact.
2. No matter the facts that originated the ROs' decision to not accept the client, the client must not be informed of the specific reasons. Instead, the follow-up communication should mention only general risk considerations. Below is a template that can be used in this context.

Dear <client's name>,

Thank you for your interest in our services.
After reviewing your submitted profile information with careful consideration, we regret to inform you that we will not be able to proceed with the opening of your account.

This decision was made in line with our internal policies, after assessment of all risk factors involved. We know this is unfortunate, but as a regulated entity we are required to follow certain procedures and sometimes make difficult decisions.

Thank you for understanding.

Kind Regards,
<Compliance Representative>

Table 16 - Account closure due to risk

10. Capital Limitation Policy

As part of the Company's general risk management strategy, it has imposed a series of limits on the amounts of funds that can be exchanged, withdrawn, deposited or spent at a given time. These limits reflect certain security measures associated with the volume of capital involved that require certain requirements to be followed.

In view of the company's model and scheme of operations the risk assessment has appropriately identified a number of risk factors and mitigating/controlling measures that reflect certain risks of ML/FT. In this regard the current risk view of the following transactions is tied to our ability to monitor and control such transactions. Consequently, as part of its policies and procedures the Company imposes the following capital limits on its clients over time as expressed in the tables below.

10.1. Wallet Services

10.1.1. Tiers and risk levels

1. Any amounts in virtual assets are denominated in EUR at the time of the transaction.
2. Any increase in limits beyond 100,000 EUR needs to be approved by the MLRO, the Designated Employee or any one Director of the Company after the requesting client has successfully provided the Company with all information and documentation necessary to complete an assessment.
3. Limits can be increased on a case-by-case basis giving due consideration to the type of client profile and risks associated with it. Any increase in Deposit Limits shall be noted in the client profile with the stated reason(s) for approval or rejection.
4. The total amount thresholds are measured in cumulative deposits or withdrawals.

Total Amount Thresholds		**Tier**	**Risk Level**	**Minimum due diligence required**
FIAT	**Virtual Asset**			
Under **2,000 EUR**		Tier A1	**Low**	Simplified Due Diligence (**SDD**) ● Verified Identity document; ● Watchlists screening; ● Political exposure screening; ● Information on SOW/SOF source; ● Self-declaration of PEP status;

				● Verified phone number (SMS verified).
Equal or above **2,000 EUR**		Tier A2	**Medium-Low**	Customer Due Diligence (**CDD**) All SDD fields on prior tier, and: ● Verified Personal Address
Equal or above **10,000 EUR**	Equal or above **20,000 EUR**	Tier A3	**Medium**	Enhanced Due Diligence (**EDD**) (as necessary) All CDD fields on prior tier, and: ● Questionnaire on SOW; ● Document to support SOW/SOF information.
Above **100,000 EUR**		Tier A4	**High**	Enhanced Due Diligence (**EDD**) All EDD fields on prior tier, and: ● Case-by-case assessment and approval.
Table 17 - Due Diligence Tiers and risk levels				

10.1.2. Transaction limits

These maximum limits are globally set for all users, independently of their assigned tier.

Currency	Minimum per day	Maximum per day
EUR	25 EUR	100,000 EUR
BTC	0.002 BTC	10 BTC
ETH	0.055 ETH	300 ETH
BCH	0.02 BCH	100 BCH
USDT	25 USDT	100,000 USDT
USDC	25 USDC	100,000 USDC
Table 18 - Exchange limits		

Currency	Minimum per day	Maximum per day
EUR	50 EUR	10,000 EUR

BTC	0.0007 BTC	None
ETH	0.025 ETH	None
BCH	0.01 BCH	None
USDT	1 USDT	None
USDC	1 USDC	None

Table 19 - Deposit limits (fiat currency: deposit from a bank account; Virtual asset: deposit from an external self-hosted or exchange address)

Currency	Type	Minimum per day	Maximum per day
EUR	FIAT	50 EUR	20,000 EUR
BTC	Virtual asset	0.0007 BTC	2.8 BTC
ETH	Virtual asset	0.025 ETH	90 ETH
BCH	Virtual asset	0.01 BCH	28 BCH
USDT	Virtual asset	50 USDT	20,000 USDT
USDC	Virtual asset	50 USDC	20,000 USDC

Table 20 - Withdrawal limits (fiat currency: withdraw to a bank account; virtual asset: withdraw to an external self-hosted or exchange address)

Total Amount Thresholds	Designated Tier	Risk Level	Minimum Due Diligence Required
Withdrawal of up to **10,000 EUR** per year	Tier B1	**Low**	Initial Business Due Diligence (**IBDD**) ● Email address; ● Country of incorporation; ● Business sector of activity; ● Company's legal name; ● Company's address, including city and zip code; ● Link to a publicly available company website owned under the same company name; ● Yearly gross revenue information; ● Bank information for settlement; ● Business Owner/Representative full name; ● Business Tax identification number; ● Business Proof of Incorporation document.
Withdrawal of more than **10,000 EUR** per year	Tier B2	**Medium**	Full Business Due Diligence (**FBDD**) ● All the above; ● Business Declaration Form; ● Beneficial owner(s) Form(s); ● Bank statement dated within 3 months; ● Identity Document for all individuals with significant control over the business; ● Proof of Address document for all individuals with significant control over the business ● Percentage of ownership for all individuals with significant control over the business
Withdrawal of more than **100,000 EUR** per year	Tier B3	**High**	All the above; additional information if necessary

Table 6 - Settlement Services Thresholds

4. Further documents may be requested after Tier B3 for any transactions of significantly high aggregate volume. The documents need to support the origin of funds of the aforementioned transactions.

Minimum per withdrawal	Maximum per withdrawal
100 EUR	100,000 EUR

Table 25 - Minimum and maximum withdrawal limits for business clients

5. The client may still request a withdrawal below the minimum or above the maximum. However, withdrawals below the minimum will incur extra fees. A withdrawal above the maximum requires manual processing by the FCO after transaction review by the RO and is handled on a case-by-case basis.

11. Risk Assessment

11.1. Business Risk Assessment (BRA)

1. This section contains our current BRA for related risk factors, as well as the method by which the Company has mitigated, controlled or eliminated such risks.
2. The identification of the threats and vulnerabilities one is exposed requires a consideration of the risk areas and risk factors both from a qualitative and a quantitative point of view. Thus, for the purposes of the BRA, it is not sufficient for the subject person to merely draw up an inventory of the threats or vulnerabilities, but also has to consider how numerous these threats or vulnerabilities are.

11.1.1. Business Risk Assessment factors

1. The table below presents some of the quantitative factors considered.

Risk category	Quantitative factors (examples)
Client	● The number of customers within each customer risk type; ● The maturity of the client base (e.g. the duration of existing relationships); ● The volume of business.

Geographical	● The number of subsidiaries or branches within a given jurisdiction; ● The number of clients and/or ultimate beneficial owners from a given jurisdiction; ● The number of transactions to or from a given jurisdiction; ● The number of other factors that expose it to a given jurisdiction.
Service and Transaction	● The number of products, services and transactions; ● The number of customers per each service; ● The volume of transactions per service and client.
Delivery Channel	● The number of distributors and agents; ● The number of client relationships started on a non-face-to-face basis; ● The number of customers introduced through introducers and intermediaries.

Table 26 - Risks and quantitative factors (examples)

2. The Company has to determine the likelihood of any scenario materialising and the possible impact thereof. Likelihood and impact will lead to one's inherent risk, as follows:

- **Risk probability**

The chance of an identified ML/TF risk materialising as part of everyday operations across the industry where the company operates. This can also be interpreted as the vulnerability of each area identified and how likely the area is to be exploited by malicious users. Some risks are therefore more likely to occur than others.

- **Risk impact**

Describes the expected damage to the company and industry should the identified ML/TF materialise without any specifc control measures in place. The potential impact is not the same for all identified risks as some may have a greater impact than others. When determining the impact of an identified risk, consideration has been given to factors such as:

- Potential to facilitate criminal conduct;
- Risk of regulatory fines;
- Risk of legal prosecution;
- Reputational damage to the company and/or the industry as a whole;
- Loss of business as a result of client rejection.

	Impact		
Likelihood	**1**	**2**	**3**
1	1	2	3
2	2	4	6
3	3	6	9

Score	Aggregate Risk
1-2	Low Risk
3-4	Medium Risk
6	High Risk
9	Critical Risk

3. The more complex the activities of the company, the more sophisticated its risk assessment is expected to be. Conversely, whenever a client does not offer complex products, services or transactions, and with limited or no international exposure, the ROs will not require a complex or sophisticated assessment.

4. Over time the Company would be expected to involve a number of functions, where applicable, in the drafting of the BRA. The MLRO, the internal auditor as well as anyone else responsible for monitoring the application of AML/CFT measures, controls, policies and procedures can all contribute to the BRA through their insights and experience.

5. The BRA, revisions thereof, as well as any decision taken in relation thereto, have to be approved by the Board of Directors of the company. It is possible that the Board of Directors may delegate some of its functions to one or more committees (e.g., to the Internal Audit Committee, to the Risk Management Committee, etc.). This may also include the function of adopting and approving the BRA and/or its review and update.

11.2. Client Risk Assessment Matrix

1. The CRA is the methodology for the risk overall assessment of clients. The CRA matrix serves as the guideline for the implemented processes that the RO follows during the assessment of client profile onboarding data.

2. The CRA showcases the rationale for assessing individual clients given a set of criteria, with an associated risk scoring. Clients are assessed on each criteria they match and given a score point for that criteria until a total score is reached. The overall score determines the overall level of minimum due diligence to be applied when onboarding the client.

3. The above does not preclude the client verification to be supplemented with additional checks and verifications, where the employee feels there is need for further investigation which may reveal other factors that increase the risk of the Client and therefore require additional due diligence or monitoring.

4. Full details of client risk assessment can be consulted in the following sheets in annex:

- **Natural Persons**

Appendix A1 - Client Risk Assessment for Natural Persons

- **Business Entities**

Appendix A2 - Client Risk Assessment for Company Entities

11.3 Virtual Asset Risk Assessment

1. The Company performs a risk assessment of all the accepted virtual assets. This assessment reflects the qualitative risk elements for each virtual asset, including its issuer, robustness of underlying network, applicable regulations, degree of decentralization, widespread availability, media perception and other factors.

2. The Company analyzes virtual assets, attributing a final score of “Acceptable” or “Unacceptable”, considering different measures of risk. The Company is only willing to accept virtual assets that obtain an “Acceptable” rating on the risk assessment matrix. Besides the internal review, any virtual assets must also be accepted by all financial and technological partners (eg: settlement providers, screening providers) which have an ongoing relationship.

3. The Company takes a conservative approach to its support of virtual assets, only accepting well-established and reputable virtual assets across the industry. The Company does not accept external requests to support specific virtual assets. Any evaluation and addition to this supported list is done internally and, on a case-by-case basis.

4. The following table summarizes the virtual assets which have been evaluated and obtained an Acceptable risk rating.

Name	Ticker	Observations
Bitcoin	BTC	-
Ethereum	ETH	-
DASH	DASH	PrivateSend feature not supported
Tether	USDT	-
USD Coin	USDC	-
Bitcoin Cash	BCH	-
Elrond	EGLD	-

Table 27 - Accepted virtual assets

11.4. Virtual Asset Transaction Risk Assessment

11.4.1. General Considerations

The company employs on-chain transaction monitoring tools for its virtual asset transactions, by the use of an integrated service provider (Sift). This blockchain analysis tool and analytics service, also known as Know-Your-Transaction (KYT) analyses all incoming and outgoing transactions assessing risk and flagging suspected sources and destination addresses. This tool allows the filtering and blocking of known sources of risk in an automatic way. Transactions from known sources under Sanctions, from Terrorist Finance, Darknet sources and many others are immediately flagged and identified, allowing the company to take appropriate follow-up actions. Moreover, other high-risk sources, such as ransomware, scams, stolen funds, mixers and high risk exchanges are also flagged and identified, allowing the transaction to be blocked or further investigated. This integrated system allows the company to mitigate most of the risks associated with the processing, identification and whitelisting of incoming virtual asset funds.

11.4.2. Transaction blocking Meaning

It is important to note that due to the nature of underlying blockchain transactions and the finality of operations, there is no inherent mechanism to block or reverse a transaction after it has been executed. Therefore, any blocking action related to a virtual asset transaction is effectively done either immediately prior or after the execution of a transaction on the underlying blockchain, depending on the type of transaction (incoming or outgoing, respectively):

- **Outgoing transactions** (from a client to an external address) blocking is understood as preventing a transaction from being executed on the underlying network, after knowing its intended destination

- **Incoming transactions** (from an external address to a client) blocking is understood as preventing the client from moving any received funds upon the funds being received and transaction has been executed on the underlying network.

11.4.3. Usage of Sift

1. All virtual asset transactions go through our blockchain analysis tool, which analyses and alerts the company of all potential incoming and outgoing suspicious activity;
2. Depending on the number of sources which trigger an alert, a risk score will be attributed to the address (ranging from Low to Severe).
3. All alerts are automatically triggered based on the (direct or indirect) sources of funds of the virtual asset addresses from where (or to which) a transfer is being made;
4. Depending on the assigned risk level, an outgoing transaction may be blocked. A risk alert will be triggered requiring manual review of a RO or the MLRO.
5. Depending on the assigned risk level, an incoming transaction will generate an alert associated client account. The account of the client receiving the funds may be blocked. A risk alert will be triggered requiring manual review of a RO or the MLRO.
6. The Company relies on the analysis of the transaction addresses as primary evidence of possible ML/FT in virtual asset transactions. Based on the risk level of the transaction and/or the series of transactions the employee will take the appropriate action in accordance with our Suspicious Transaction Reporting Procedures and unusual transaction guidelines. All transactions shall be recorded in the client profile, including the risk of said transaction.
7. All transactions marked as Severe and High are automatically blocked by the system, and reported to MLRO. Multiple Medium Risk transactions will also trigger an unusual activity report where the employee has reasonable suspicion that there is a risk of ML/FT or the possible emergence of a risky pattern of transactions.

11.4.4. Risk Rules determined by Sift

1. The following rules pertaining risk are pre-determined by Sift and cannot be lowered by the company. Should the company wish to adjust a particular risk alert the matter must be raised directly with Sift representatives.
2. The table below presents the applicable categories and corresponding risk levels (Sift always uses fiat denomination amounts in US Dollars).

Category	Exposure Type	Direction	Minimum (USD)	Max (USD)	Risk level
Child Abuse Material	Direct or Indirect	Sending or Receiving	$0	-	Severe
Sanctions	Direct or Indirect	Sending or Receiving	$0	-	Severe
Terrorist Financing	Direct or Indirect	Sending or Receiving	$0	-	Severe
Darknet Market	Direct	Sending or Receiving	$100	-	High
	Indirect	Sending or Receiving	$500	-	High
	Indirect	Sending or Receiving	$100	$500	Medium
	Direct	Sending or Receiving	$10	$100	Medium
Ransomware	Direct	Receiving	$100	-	High
	Indirect	Receiving	$500	-	High
	Indirect	Receiving	$100	$500	Medium
	Direct	Receiving	$10	$100	Medium
	Direct	Sending	$500	-	Medium
Scam	Direct	Receiving	$100	-	High
	Indirect	Receiving	$500	-	High
	Indirect	Receiving	$100	$500	Medium
	Direct	Receiving	$10	$100	Medium

	Direct	Sending	$500	-	Medium
Stolen Funds	Direct or Indirect	Receiving	$0	-	High
	Direct	Sending	$500	-	Medium
Gambling	Indirect	Sending or Receiving	$1,000	-	Medium
	Direct	Sending or Receiving	$500	-	Medium
High Risk Exchange	Direct	Sending or Receiving	$500	-	Medium
Mixing	Indirect	Sending or Receiving	$1,000	-	Medium
	Direct	Sending or Receiving	$500	-	Medium
P2P Exchange	Indirect	Sending or Receiving	$1,000	-	Medium
	Direct	Sending or Receiving	$500	-	Medium

Table 29 - Categories and risks associated

12. Post-onboarding Client Profile Review

12.1. Periodic Client Information Refresh

1. The Company will do its utmost to keep its client profile information elements updated. This is important to ensure that any subsequent review of profile assessment is correct.

- For individual clients, the most pressing elements to keep updated are the identification and residence information/documents.

- For business, the most pressing elements to keep updated are the status of the business entity, particularly its cessation, insolvency, change of primary activity and change of ownership.

2. All clients are subjected to the following procedures:
   - Periodically reminded to keep their profile information up-to-date, and their responsibility of informing us of any changes;
   - Periodically asked if any of their profile information changes, and if so, to take action and update their profile information (either in dashboard or through a CSA).
3. In regard to expired or soon to be expired identity documents, if an individual client:
   - Has an identity document expiring in the next 90 days, he will be contacted to submit an up-to-date identity document;
   - Has an expired document as part of its information profile, its account is suspended, until such document is submitted and accepted.

12.2. Periodic Client Risk Profile Review

1. The Company will periodically review the profiles of its clients, to make sure that their risk assessment is still within acceptable limits. Depending on the client's current level of risk, the system will set up an automatic schedule to review the client information and transactions, to ascertain if it needs risk updating, based on the client's activity and behaviour.

2. If any such cases are detected, the MLRO will be notified to review the profile in question to ascertain the actions to take and verify if the client's relationship remains within the risk threshold of the Company.

3. For individual clients who are confirmed PEPs, a manual profile review is also periodically performed by MLRO or RO. Additionally, the MRLO can also, and its own discretion, carry out a re-screening on any client, as deemed necessary.

4. The Company's periodic review schedule for natural persons (individuals) and business entities is described below in Table 26 and 27, respectively.

PEP status	Client Risk	Review Period	Review Type
Non-PEP	Low risk	Every 24 months	● Automatically performed by the system. System informs the MLRO or RO of the need of manual review; ● Ad-hoc.
	Medium risk	Every 24 months	● Automatically performed by the system.

			System informs the MLRO or RO of the need of manual review; ● Ad-hoc.
	High risk	Every 12 months	● Automatically performed by the system. System informs the MLRO or RO of the need of manual review; ● Ad-hoc.
PEP	High risk	Every 12 months	● Manually performed by the MLRO or RO.

Table 30 - Clients and corresponding periodic reviews - individuals

Client Risk	Review Period	Review Type
Low Risk	Every 36 months	Manually performed by the MLRO or RO
Medium Risk	Every 24 months	Manually performed by the MLRO or RO
High Risk	Every 12 months	Manually performed by the MLRO or RO

Table 31 - Clients and corresponding periodic reviews - business entities

12.3. Client Requests to Close Account

1. After onboarding, a client may at any time request to close the account. After receiving this request by the client, the Company will proceed to confirm with the client the closure of the account and instruct the client to settle any remaining funds and/or pending transactions.
2. After all transactions are settled, the Client will be notified of the closure of the account. This does not mean that the client's records are deleted, as outlined in the Record Keeping Policy section. The client also has the right to keep a copy of his records before the business relationship ceases.
3. There are, however, instances, as outlined in the Suspicious Transaction Reporting Policy section, where due to FIU order or ongoing investigation, the client request to close the account may not be granted.

12.4. Account closure due of client death or incapacitation

1. In the eventuality an individual client (natural person) dies or becomes incapacitated, the legal heir or guardian (incumbent person) should notify the Company of this eventuality, under the prescribed legal period.

2. The incumbent person will be able to close the account and receive any funds in the account before its closure. The account will be closed at the end of the process and cannot be kept open and re-assigned to the incumbent person as a new client.

3. The Company will require at least the following documents from the incumbent person in order to confirm a client's death or incapacitation:

- Client's Identity document;
- Incumbent person's Identity document;
- Proof of address of the incumbent person;
- The client's death certificate or incapacitation issued by a recognized government entity (the document must be certified and apostilled by a legal notary or equivalent and must be sent both digitally and by registered post);
- The Client's will or equivalent legal document attesting the incumbent person as the sole designated heir or legal guardian (the document must be certified and apostilled by a legal notary or equivalent and must be sent both digitally and by registered post).

4. If the designated person is not the sole designated heir, a document granting the incumbent person the legal right to the account's funds as inheritance, signed by all designated heirs or issued by a court of law must be sent.

5. After the documents are received and accepted as valid, the incumbent person will be contacted for scheduling a video call with an RO, ensuring the incumbent person's request validity. The whole process shall be heavily scrutinized to avoid any false claims.

13. Document Acceptance Policies

13.1. General guidelines

1. As part of our acceptance guidelines, any submitted documents to be manually reviewed must be in a language that the RO is able to read and therefore verify. Currently the only universally accepted language is English, with others supported at the ROs sole discretion.

2. If in an unaccepted language, the document must be accompanied by an official English translation.

3. Moreover, there are certain documents that we refuse to accept, such as:

- Any document that contains an expired validity date;
- Any document that cannot be reasonably be verified as authentic;
- Any official documents in a foreign language and without an official translation that cannot be analysed by the RO;
- Any document that shows inconsistencies with other received documents for the same client;
- Any document exhibiting evidence of tampering or forgery.

4. Any document showcasing inconsistencies or signs of tampering will raise the level of scrutiny of the client to the highest, and may result in other proactive actions, such as refusal of service, account termination, filing of an STR or others.

13.2. Business Entity Incorporation Document

1. The following is a list of examples of accepted documents typically to be asked to corporate clients when it comes to proof of their business incorporation. This document has multiple purposes such as:

- to demonstrate that the business entity exists and is duly registered under a specific geography;
- to prove the entity purpose and stated activities;
- to present basic entity details (e.g. name, incorporation number, tax ID, VAT ID);
- to corroborate self-declared business data at onboarding.

2. The specific document(s) are dependent on the type of incorporated entity, with various degrees of complexity, as showcased on the table below.

Type of Entity	**Examples of Accepted Documents**
Limited Companies	A certificate of Incorporation or equivalent
Limited Liability Partnerships	
Public Traded Companies	
Partnerships	One of the following: • A recent business bank statement (dated within the last 3 months) • A business utility bill (dated within the last 3 months) • An invoice from a supplier (dated within the last 3 months); • A tax authority correspondence (dated within the last 12 months); • Business premises rates bill (dated within the last 12 months). *The document must contain at least the partner's names on it, the business address and the trading name (if applicable).
Sole Trader	All of the following documents: • One of the following documents as proof of identity document of the Sole Trader: o National Identity Card o Driver License o Passport • One of the following documents showcasing the Sole Trader's business/operating address: o A recent business bank statement (dated within the last 3months); o A business utility bill (dated within the last 3 months); o An invoice from a supplier (dated within the last 3 months);

	○ Official tax authority correspondence (dated within the last 12 months); ○ Business premises utility bill (dated within the last 12 months). Any of the documents must clearly showcase the full name of the SoleTrader and match the identity document name • A photo of the Sole Trader holding their proof of identity document
Charities **Community Organisations**	All the constitution documents confirming: • What the charity organization has been setup to do; • Who are the appointed Board and Committee members; • Who are the Key Officials (Chairperson / Treasurer / Secretary).
Table 32 - Accepted documents for type of company	

3. Depending on the jurisdiction of the incorporated business, the RO may request the business incorporation document or any other to be provided with a certification by a legal notary with apostille.

13.2.1. Document verification

1. The proof of the business incorporation is manually verified by the RO and/or the MLRO.
2. After the document is submitted, it is crucial to verify that the document corresponds to a registered and active company. Due to the different national systems used around the world, there is no single unified system to accurately verify an entity. Instead, the RO must first ascertain the country of incorporation of the entity, then search the available public national company registry for the matching number.
3. Most incorporation documents nowadays contain links and information that facilitates the verification on their respective national registry.

13.2.2. Documents we do not accept

We do not accept the following as incorporation documents:

- any documents not issued by an official entity or governmental body;
- provisional incorporation documentation that does not include a clearly assigned registration number or tax identification number.

13.3. Individual Identification Documents

Identification Documents	
Acceptance Notes	**Examples of Accepted Documents**
Must showcase the client's: ● Full name ● Date of birth ● Recognizable picture ● Nationality Must have a visible: ● Issue date ● Expiration date	● Passport ● Driving license ● National identity card (can also be used as evidence of address if it includes this field) ● Residence permit card (can also be used as evidence of address if it includes this field)

Table 33 - Examples of accepted IDs

13.3.1. Document verification

The verification of an Identification Document can be automated by use of a third-party identity verification platform, manually by an RO or a combination of both.

13.3.2. Documents we do not accept

We do not accept the following documents as IDs:

- Provisional or temporary documentation;
- Printouts of documents;
- Photo of a screen/screenshot;
- Any document with an expiry date within the upcoming 90 days (counting from date of first receival);
- National insurance cards;
- Birth certificates;
- Work ID Cards;
- Student ID Cards;
- Any documents in foreign languages with only non-roman characters.

13.4. Individual Proof of Address Document

Proof of Address (POA)	
Acceptance Notes	**Examples of Accepted Documents**
Must be an original document received at the client's residence. Must showcase the client's ● Name ● Address, including city, country, zip or post code	● Utility bill (eg: gas, electric, satellite television, phone bill) issued within the last 90 days; ● National identity card (only if it includes address as a field); ● Official mail correspondence from any local, municipal or federal government entity or tax authority (issued within the last 90 days);

Must have a recognizable: ● Issue date ● Name of issuer ● Address of issuer ● Contact of issuer	● ~~Electoral card or registration document confirming electoral~~ jurisdiction; ● Rent contract or tenancy agreement for the current year; ● Lawyer or Notary letter confirming recent house purchase or land registry confirmation of address (issued within the last 90 days); ● Statement issued by a Bank or Credit Union (dated within the last 90 days); ● Statement issued by a recognized financial institution or entity carrying out relevant financial business in the EU (issued within the last 90 days).

Table 34 - Examples of accepted Proof of Address

13.4.1. Document verification

The POA is manually verified by the RO and/or the MLRO.

13.4.2. Exceptional Circumstances

1. There may be circumstances where people are unable to provide documentation proving their place of residence. In such cases we can obtain alternate sources of documentation following a clarification on the reasons why the client is unable to provide the standard documentation.
2. The documentation to be obtained should naturally reflect the appropriate risk posed by the Client's Account and the strength of the document in providing its verification. A note to this effect must be entered into the person's file. Examples include the following:

- when a client only has a temporary address and has no permanent residential address elsewhere, such as seasonal workers, a letter from a director or manager of the employer confirming the residence at a stated address and indicating the expected duration of employment would be sufficient;
- when a client resides on a yacht, the client's residential address may be verified by obtaining documentation relating to the chartering of the yacht and berthing agreements;

- when the client is residing in a nursing home or similar residential care institution, the subject person may verify the client's residential address by obtaining a letter from the director or manager of the home/institution confirming the client's residential address;
- when the client is homeless or a member of the travelling community, subject persons must gather sufficient information and, where available, documentation on the client's situation and frequent whereabouts;
- when the client is a student or part of the academic staff, and is residing in a university, college or any other institutional residence, the subject person may verify the client's residential address by obtaining a letter from the director or senior official of the university, college or institution confirming the client's residential address.

13.4.3. Documents we do not accept

We do not accept the following documents as POAs:

- printouts of documents;
- Photo of a screen/screenshot;
- any payee form detailing the person's cessation of employment;
- any documents in foreign languages with only non-roman characters.

13.5. Individual Source of Wealth and Source of Funds Document

1. While what specifically constitutes a SOW or SOF document is not specifically stated in law, the Company establishes as a good practice to detail some accepted documents for each type.
2. The following is a list of examples of accepted documents typically to be asked to individual clients when it comes to SOW and SOF, depending on the answers received.

Type of SOF/SOW	Description	Examples of Accepted Documents
Asset Finance	Lending that enables you to release cash from value in the assets you already own.	● Copy of loan agreement; ● Letter from solicitor; ● Bank statement which clearly states where the funds originated.
Company Profits	Financial benefit achieved when the amount of revenue gained from a business activity exceeds the expenses, costs and taxes needed to sustain the activity.	● Company financial statements; ● Bank statement which clearly states where the funds originated.

Company Sale	Funds received following the sale of a company.	● Proof of ownership and sale of the company, including values; ● Company minutes or written confirmation of sale.
Crowdfunding	The practice of funding a project or venture by raising many small amounts of money from many people, typically via the internet.	● Details on the source used to crowdfund, including custodian details and record keeping on the investors.
Gift	Property, money or assets transferred from one person to another while receiving nothing less than fair market value in return.	● Solicitor approval of gift; ● Details on the gifter and evidence of how they acquired their wealth.
Inheritance	All or part of a person's estate/ assets given to an heir or beneficiary.	● Copy of the will; ● Letter from solicitor; ● Bank statement which clearly states where the funds originated.
Initial Public Offering (IPO)	The process by which a private company can go public by sale of its stocks to the general public.	● Details of the stock exchange the company floated on, including a public URL to evidence its availability; ● Document showcasing regulatory flings and underwriters; ● Bank statement which clearly states where the funds originated.
Initial Coin Offering (ICO)	Virtual asset equivalent of an IPO (see above). They act as fundraisers, with a company looking to create a new coin, app, or service.	● Details of the completed KYC procedure on investors, including contract with certified KYC provider; ● Details of the AML policy; ● Details on the custody of funds (legal and/or technical); ● An URL which evidences availability of the virtual asset for each investor.
Invoice Finance	Short-term borrowing that is extended by a lender to its business customers based on unpaid invoices.	● Copy of the loan agreement; ● Letter from your solicitor; ● Bank statement which clearly states where the funds originated.
Loan	Property, money or material goods given from one party to another in exchange for future repayment of the principal amount along with interest or other financial charges.	● Loan contract; ● Bank statement which clearly states where the funds originated.

Maturing Investments	Assets received from previous investments.	● Portfolio account statement; ● Bank statement which clearly states

		where the funds originated.
Pension	Money received from a pension. Usually a lump sum or regular payment.	● Certificate of pension annual payment, showing values ● Tax office document ● Letter from former employer or pension provider Bank statement which clearly states where the funds originated
Peer to peer lending (P2P)	A way for people to lend money to individuals or businesses. The lender receives interest at a higher rate than a savings account.	● Loan agreement or contract; ● Letter from solicitor / representative; ● Bank statement which clearly states where the funds originated.
Property Sale	Funds received from the sale of a property. This may be a second home or profits from moving home.	● Proof of ownership and sale of the property, with stated values; ● Property deed; ● Letter from solicitor; ● Bank statement which clearly states where the funds originated.
Salary	Payment(s) made by an employer to an employee, typically on a monthly basis.	● Statement of annual pay from employer, showing values; ● Wage slips; ● Bank statement which clearly states where the funds originated.
Virtual asset	Virtual assets owned under a public blockchain, in either self-custody or under exchange custody.	● Sift KYT rating clear (automatically obtained); ● Declaration of ownership of source address (if self-custody as source).

Table 35 - Examples of accepted SOF/SOW documents

13.5.1. Document verification

The verification of a SOF and SOW document is manually performed by a RO.

13.5.2. Documents we do not accept

We do not accept as SOW-SOF any document stating a different name as primary beneficiary.

14. Jurisdiction Acceptance Policy

The Company restricts the clients based on their jurisdiction.

14.1. Applicability by client type

This jurisdiction concept applies differently whether the client is a natural person or a business entity, specifically:

- The jurisdiction of acquired residence and acquired nationality for natural persons (for further details on this is established, refer to the details on the Establishing Jurisdiction for natural persons section);
- The jurisdiction of incorporation for business entities.
  Furthermore, the company also chooses to apply restrictions if the business entity itself declares to do businesses or otherwise serves clients in a non-reputable jurisdiction.

14.2. General considerations and framework

1. The Company, in evaluating jurisdictions, has referred to the FATF public documents on high-risk and non-cooperative jurisdictions, as well as the European Commission legal acts identifying high-risk third countries, United Nations list of countries sanctioned or embargoed and the US (OFAC) sanctions' list.
2. The Company has incorporated the jurisdictional lists in its CRA, and has categorized these jurisdictional lists into Non-serviced, High Risk, Medium Risk and Low Risk.
3. The Company shall pay special attention to business relationships and transactions with clients from high-risk jurisdictions and whenever the transactions involved have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall be examined.
4. The Company does not accept, do business or in any way serves clients in Non-serviced jurisdictions.
5. Non serviced can be further segmented into:
   - Non-Reputable

These jurisdictions bear unacceptable risk due to external factors. Typically related to their international standing (e.g. Sanctions, Financial non-compliance).

- Business-adverse

These jurisdictions bear too much of a risk due to internal factors. Typically related to their associated regulatory requirements and/or uncertainty to properly service.

Risk	Description
Non-serviced	• Jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply; • Jurisdictions which have been sanctioned by the EU or listed by the EU Commission • Jurisdictions that the Company considered too high risk for doing business in; • Jurisdictions not supported by payment providers. ***In this category no business is carried out.***
High Risk	● Jurisdictions that have had strategic AML/CFT deficiencies in the past and that have been recognized by the EU and other relevant international bodies as achieved significant progress and not possessing unmitigated systemic risks; ● Jurisdictions with no strategic AML/CFT deficiencies but with a negative perception in the international financial community; ● Jurisdictions that the Company considers especially risky for its businesses. ***In this category enhanced due diligence applies.***
Medium Risk	● All jurisdictions not explicitly considered as **Non-serviced**, **High Risk** or **Low Risk** ***In this category the standard due diligence process applies, and can be escalated to enhanced due diligence.***
Low Risk	● Jurisdictions which could be considered as low-risk are those which have strong institutional adherence and proven commitment to AML/CTF standards; ● Reputable jurisdictions, EU Member States and EEA countries. ***In this category the simplified due diligence process applies.***

Table 36 - Jurisdictions by risk and descriptions

6. The Company, when dealing with natural persons established or linked to high-risk jurisdictions, will apply proportionate EDD measures accordingly. A connection to these jurisdictions may take various forms.

7. A business relationship shall be considered to be connected to a high-risk jurisdiction if the Client, the beneficial owner, the SOW/SOF, the residence, or the business/economic activity are situated in or originate from such a jurisdiction. However, not every form of connection to a high-risk jurisdiction shall give rise to the requirement to apply EDD. By way of example, where a business relationship involves a client who is a citizen of a non-reputable jurisdiction but does not reside in such jurisdiction and the business/economic activity and/or the SOW/SOF involved are not in any way connected to such jurisdiction, the requirement to apply EDD does not arise.

8. The Company, when establishing business relationships or acting in the course of a business relationship with a natural person established in a non-reputable jurisdiction, in respect of which there has been an international call for countermeasures (i.e. FATF Category 1 jurisdictions), shall notify the FIU of this occurrence.

14.3. Non-serviced jurisdiction sources

The Company regularly refers to the various international authorities such as the EU, OFAC, FATF and the UN in order to update the jurisdiction table. Sanctioned and High-Risk Jurisdictions were considered according to latest sanctions and risk country lists and are outlined in the table below:

- US OFAC sanctions as of 14-12-2020
- EU sanctions as of 23-12-2020
- EU Commission high-risk third countries as of 07-05-2020

Country	Sanctioned & Embargoed			High Risk	Unrecognized or Disputed territory
	UN	EU	US	EU Commission	
Afghanistan	●			●	
Barbados				●	
Bahamas				●	
Belarus		●	●		
Bosnia & Herzegovina		●			
Botswana				●	
Burundi		●			
Cambodia				●	
Central African Republic			●		
Congo D.R.	●	●	●		

Cuba			●		

Eritrea	●				
Ghana				●	
Guinea		●			
Guinea-Bissau	●	●			
Haiti		●			
Iran	●	●	●	●	
Iraq	●		●	●	
Lebanon	●		●		
Libya (aka: Libyan Arab Jamahiriya)	●	●	●		
Jamaica				●	
Maldives		●			
Mali	●				
Mauritius				●	
Mongolia				●	
Myanmar		●		●	
Nicaragua				●	
Democratic People's Republic of Korea (aka: North Korea)	●	●	●	●	
Pakistan				●	
Panama				●	
Russia		●			
Samoa				●	

Somalia	●		●		
South Sudan	●	●	●		

Sudan	●	●	●		
Syria		●	●	●	
Trinidad and Tobago				●	
Tunisia		●		●	
Ukraine		●	●		
Venezuela		●	●		
Western Sahara					●
Yemen			●	●	
Zimbabwe		●	●	●	

Table 37 - List of sources of high risk, sanctioned or embargoed jurisdictions

14.4. Jurisdictions segmented by Risk

13.4.1. Individual Clients

The following table summarizes all the jurisdictions and their assigned risk. It applies to individual clients.

Jurisdictions		Risk
Afghanistan, Bahamas, Barbados, Belarus, Botswana, Cambodia, Central African Republic, Congo DR, Cuba, Democratic People's Republic of Korea, Ghana, Iran, Iraq, Jamaica, Libya, Mauritania, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Russia, Somalia, South Sudan, Sudan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Venezuela, Western Sahara, Yemen, Zimbabwe.	***Non-Reputable***	Non-serviced
Cook Islands, Côte d'Ivoire, Guam, United States of America, United States Minor Outlying Islands, Kosovo.	***Business-adverse***	

Algeria, Angola, Anguilla, Antigua And Barbuda, Aruba, Bangladesh, Bosnia & Herzegovina, Belize, Benin, Bermuda, Burundi, Cayman Islands, Cameroon, Chad, Colombia, Comoros, Equatorial Guinea, Eritrea, Gabon, Gambia, Guinea, Guinea-Bissau, Haiti, Honduras, Kiribati, Kyrgyzstan, Lebanon, Lesotho, Liberia, Madagascar, Maldives, Mali, Marshall Islands, Martinique, Mayotte, Montserrat, Morocco, Mozambique, Nauru, Nigeria, Norfolk Island, Palau, Papua New Guinea, Paraguay, Rwanda, Samoa, Serbia, Sierra Leone, Solomon Islands, Suriname, Swaziland, Tajikistan, Timor-Leste, Togo, Tunisia, Turkmenistan, Turks And Caicos Islands, Tuvalu, Ukraine, Uzbekistan, Zambia	**High**
All jurisdictions not included in any of the other classifications. **For Example:** Brazil, China, India, Mexico, Saudi Arabia, South Africa, Turkey.	**Medium**
Andorra, Australia, Canada, Israel, Japan, New Zealand, Singapore, Gibraltar, United Arab Emirates, South Korea, United Kingdom, EU Member States and countries in the EEA.	**Low**

Table 38 - List of supported and non-supported jurisdictions for individual clients, segmented by risk

14.4.1. Business Clients

The following table summarizes all the jurisdictions and their assigned risk. It applies to business clients.

Jurisdictions		Risk
Afghanistan, Antarctica, Bahamas, Barbados, Belarus, Botswana, Bouvet Island, Cambodia, Central African Republic, Congo, Cuba, Democratic People's Republic Of Korea (DPRK), Ghana, Iran, Iraq, Jamaica, Libya, Mauritania, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Russian Federation, Somalia, South Sudan, Sudan, Syria, Trinidad and Tobago, Uganda,, United States Virgin Islands, Vanuatu, Venezuela, Western Sahara, Yemen, Zimbabwe	***Non-Reputable***	**Non-serviced**
Cook Islands, Côte d'Ivoire, Guam, United States of America, United States Minor Outlying Islands, Kosovo.	***Business-adverse***	

Algeria, Angola, Belarus, Bosnia & Herzegovina, Belize, Benin, Bermuda, British Indian Ocean Territory, British Virgin Islands, Burundi, Cayman Islands, Cameroon, Chad, Colombia, Comoros, Eritrea, Gabon, Gambia, Guinea, Guinea-Bissau, Haiti, Honduras, Kosovo, Lebanon, Liberia, Maldives, Mali, Martinique, Mayotte, Morocco, Northern Mariana Islands, Rwanda, Samoa, Serbia, Sierra Leone, Solomon Islands, Tunisia, Ukraine.	**High**
Andorra, Australia, Canada, Israel, Japan, New Zealand, Singapore, Gibraltar, United Arab Emirates, South Korea, United Kingdom, EU Member States and countries in the EEA.	**Low**

Table 39 - List of supported and non-supported jurisdictions for business clients, segmented by risk

15. Sanction screening

15.1. Business clients

1. The company will screen its business clients for any possible applied Sanctions.
2. The company screens against all the following publicly available lists:
   - EU - European Union financial sanction list https://data.europa.eu/euodp/data/dataset/consolidated-list-of-persons-groups-and-entities - subject-to-eu-fnancial-sanctions-fsma
   - US-OFAC Consolidated sanction list https://sanctionssearch.ofac.treas.gov/
   - United Nations Security Council Consolidated list https://www.un.org/securitycouncil/content/un-sc-consolidated-list
   - UK - HMT Financial sanction list https://www.gov.uk/government/publications/fnancial-sanctions-consolidated-list-of-target s/consolidated-list-of-targets
   - CH - SECO Sanction List https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen/suche_sanktionsadressaten.html
3. The company will not do business and will refuse to onboard any entity with a positive match in any of the aforementioned lists.

15.2. Individual clients

1. The company will screen its individual clients for any possible applied Sanctions.
2. The screening of individual clients is performed at the onboarding stage by the third-party verification provider (Onfido).
3. The list of databases that the verification provider searches against are publicly available here: https://documentation.onfdo.com/watchlists/

16. Business Sector Acceptance Policy

1. The Company restricts its business clients based on their stated sector and business activities.
2. It goes without saying that the company will not accept clients who are conducting any type of illegal activity in their respective jurisdictions.
3. Each activity is classified in terms of risk for the Company. Certain activities constitute unacceptable levels of risk and are classified as non-serviced.
4. It should be noted that certain activities may be restricted or require a license in their respective jurisdictions of operation. This does not impede their acceptance by the Company but may constitute an additional factor of risk.
5. The table below outlines the various sectors and activities segmented by risk.

Sector	Activity	Risk
Agriculture & Forestry	Services involving the Primary Sector ● Wood production & forestry ● Plants & Gardening ● Animal breeding ● Hunting ● Fishing ● Other	**Low**
	● Any services that harvest or exploit natural resources in an overly extractive way	**Non-serviced**
Art & Antiques	Services dealing with the trade of valuable Art and Antiques ● Art dealing ● Antiques dealing ● Auction ● Exhibition or Museum	**High**

Commodities	Services dealing with the trade of physical commodities ● Commodity mining ● Commodity processing ● Commodity trading (non-precious metals) ● Precious Metal trading ● Precious Metal mining	**High**
Consulting	Consulting services of different natures ● Legal consulting ● Recruiting & Staffing ● Personal coach or Trainer ● Software & IT consulting ● Software development services ● Strategy & Management consulting ● Marketing & PR ● Other	**Medium**
Education & Research	Services dealing with education, learning and research ● Educational services ● Tutoring ● Research & Development ● Other	**Low**
Energy & Environment	Services dealing with production of energy, recycling and waste ● Energy production & storage ● Environmental care ● Infrastructure management ● Waste management ● Recycling ● Other	**Low**
	● Any services dealing with nuclear energy or nuclear materials	**Non-serviced**
Finance (non-regulated)	Non-regulated Financial Services ● Escrow or Custodial agent ● Financial Advisory ● Financial Analysis ● Financial Auditing ● Relationship Management	**Medium**
	● Sales of currency by non-financial institutions	**Non-serviced**
Finance (regulated)	Regulated Financial Services, excluding the ones related to virtual assets ● Asset Management	**High**

	• Asset Trading	

	• Bank • Exchange • Financial intermediary • Money services business • Investment Fund • Insurance services • Reinsurance	
	• Bankruptcy attorneys or entities engaged in debt collection; • Credit protection services; • Credit counseling or repair agencies.	**Non-serviced**

Finance (virtual asset related)	Regulated Financial Services, related to virtual assets
	• Virtual asset miner
	• Virtual Asset Service Provider (VASP)
	  ○ Custodial wallet provider
	  ○ Exchange
	• DLT infrastructure provider
	• Coin sales
		High

Gambling	Services dealing with betting of money or convertible virtual assets • Casino • Online-gambling • Sport-related betting • E-sports betting	**High**
Sports	Services dealing with physical or virtual sport activities (not involving betting) • Physical sport • E-sports • Sport events organisation • Sports agents • International sports organisation	**Medium**
Real Estate Development	Services dealing with the planning, construction or sale of real estate • Building architecture & planning • Construction • Real estate sales • Brokerage or intermediation	**Medium**
Real Estate Management	Services dealing with the management, maintenance or administration of real estate • House maintenance & security • Rental services • Property management	**Low**

Medical Care	Services dealing with medical care or prescribed by physician ● Emergency services ● Medical care services	**Medium**
	● Production, Sale and Distribution of prescription drugs and medicines	**Low**
Health & Well-being	Services dealing with health (non-medical) and general well-being ● Non-medical treatment ● Physiotherapy ● Mental therapy ● Childcare ● Elderly care ● Cosmetics ● Health accessories ● Body care products ● Other	**Low**
	● Services that produce, sell or distribute of legal but non-prescription recreational drugs	**High**
	● Services that produce, sell or distribute controversial non-prescription substances of any kind for which the regulatory status is not specifcally clear or of otherwise dubious nature	**Non-serviced**
Manufactured Goods	Producers or sellers of manufactured goods ● Food & beverages (excluding alcohol) ● Alcoholic beverages ● Tobacco ● Clothing & textile ● Pulp, paper or wood products ● Metal & stone (non-precious) ● Chemicals ● Machinery ● Medical equipment ● Luxury goods (except Art & Antiques) ● Furniture & Household items ● Rubber & plastic ● Prints ● Glass / ceramics / clay ● Items for children ● Electronics & IT hardware ● Watches ● Automobiles or parts ● Other	**Low**
Entertainment	Provision of services related to multimedia, entertainment or Information Technology	**Low**

	• Graphic Design • Gaming • Event organisation • Content creation (non-broadcast) • Publishing • Performative arts • Other	
Mass Media	• Media streaming (Photography / video / flm / radio) • Telecommunication • Social media publication • Journalism (non-accredited)	**Low**
	• Journalism (accredited)	**Medium**
	• State media publication	**High**
	• Any media promoting or containing incitement to hate, violence, harmful or inappropriate content (as determined by their respective jurisdiction laws)	**Non-serviced**
Military & Arms	Services involving military equipment and weapons • Military industry • Military infrastructure • Weapon manufacturing	**Non-serviced**
Non Governmental	Non-governmental or religious institutions • Non-profit organization • Charity organizations • Religious organisation • Intergovernmental organisation	**High**
Political	Political institutions, groups or ofcial government bodies • Political party or organization • Government administration • Executive authority • Judicial authority • Legislative body	**High**
	• Any group or political body promoting hate or violence	**Non-serviced**
Security Services	• Private security • Personal protection services	**Medium**
Sex industry	• Pornography video distribution & streaming services • Services that employ or contract sex industry workers • Escort services	**Non-serviced**

Retail Distribution	Services dealing with retail distribution of goods	**Low**

	• Food & beverages distribution • Retail commerce • Shopping Centre	
	• E-commerce distributor • Import/Export business	**Medium**
	• Fuel stations & dispensers	**Non-serviced**
Tourism & Accommodation	Services dealing with leisure travelling and tourism • Airfare booking • Hotel & accommodation • Restaurant & Cafe • Catering • Travel or Tourism agency • Other	**Low**
Transport & Logistics	Services dealing with transportation and storage of cargo and materials • Shipping • Air freight • Land freight • Warehousing & storage • Coordination & planning • Other	**Low**
Any	• Services that may, by association, negatively impact the reputation of the company; • Services that resort to forced labour or child labour (even if deeemed legal in their respective industries or jurisdictions); • Shell Companies; • Institutions known to deal with Shell Companies.	**Non-serviced**

Table 40 - List of sectors by risk

17. Transaction Monitoring Policy

17.1. Scrutiny of Transactions

1. Transaction monitoring involves scrutinizing transactions undertaken in the course of a business relationship to ensure these are consistent with the Company's knowledge of the client's risk profile.

2. An unusual transaction should serve as a red flag or a trigger event, whereby the Company would need to assess the situation in question and establish whether:

- the transaction is suspicious enough to warrant further investigation;
- the transaction is suspicious enough to be reported to the FIU;
- the business relationship remains within the risk appetite of the Company.

3. It is also possible that there may be material changes in the activity carried out by the client, in which case the Client Risk Assessment will be updated, the client screened, and if necessary, further client due diligence information will be carried out.

17.2 Transaction Monitoring

1. Currently, the Company performs the corresponding systems and alerts as indicated in the table below.
2. The Company's automated systems currently maintain an audit trail of all transactions to, from and within the platform. Transactions are monitored in two ways:
   - Pre-Transaction Monitoring: in real time, where transactions or activities are reviewed as they take place or prior to their finalization.
   - Post-Transaction Monitoring: after the event, where transactions and patterns are reviewed after their execution.
3. In most instances the FCO, with access to the transaction list and execution infrastructure will also be involved. Monitoring systems and alerts are presented in the tables below.

Pre-Transaction	Method of Alert	Method of Control
FIAT deposit to client account (wallet and card services only)	● The FCO monitors incoming transfers and approves allocation to the client balance; ● Any unusual transaction triggers analysis and the RO is notified for further investigation; ● The list of transactions will be disclosed in the Back Office Tool.	● The FCO can block any transactions through the banking service provider platform; ● The RO and MLRO can suspend client account activity through the Back Office tools.
FIAT withdrawal to client account	● The FCO monitors accounts for requests for withdrawal to accounts; ● List of Transactions will be disclosed in the Back Office Tool.	

Virtual asset deposit to client account	● The system triggers a Sift KYT alert for any transactions which have been blocked due to Severe or High Risk; ● The list of Transactions will be disclosed in the Back Office Tool.	● Automatically blocked by the system if detected by Sift KYT as Severe of High Risk. Follow-up analysis and resolution requires intervention of the RO or MLRO; ● The RO and MLRO can block individual transactions in Sift KYT; ● The RO and MLRO can suspend client account activity through the Back Office tools.
Virtual asset withdrawal to external address	● The system triggers a Sift KYT alert for any transactions which have been blocked due to Severe or High Risk; ● List of Transactions will be disclosed in the Back Office Tool.	

Table 41 - Pre-transaction monitoring - methods of alert and control

Post-Transaction	Method of Alert	Method of Control
All internal exchanges of currency	● No specific alert set, as transactions are always performed within the system; ● List of Transactions will be disclosed in the Back Office Tool.	● The RO and MLRO can suspend client account activity through the Back Office tools.
Card withdrawals (wallet and card services only)	● No specific alert set, as active monitoring is performed by the card service provider; ● List of Transactions will be disclosed in the Back Office Tool.	● RO and MLRO can block accounts through the Back Office tools; ● FCO can block accounts through the card third-party provider.
Card usage (wallet and card services only)		

Table 42- Post-transaction monitoring - methods of alert and control

17.3 Risk Factors and Triggers

1. The following table includes a non-exhaustive list of factors and triggers and the corresponding automated systems applied to detect unusual transactions.

Factors and Triggers	Risk mitigation mechanisms
A significant change in the client's account balance, volume or frequency of transaction	● All transactions are registered; ● Any client that reaches the maximum transaction limit established for their profile will require further due diligence to raise the limit; ● Clients will be unable to use their account to move any balance or assets until approved for the next profile limit.
A significant change in the Client's account balance, volume or frequency of requested withdraws	
Mismatch between the client's risk profile and value and/or level of transactions	
Unusually large FIAT transactions on the Client's account (wallet and card services only)	● All transactions are registered; ● Individual client's bank deposits are restricted in the maximum amount allowed (hard limits) and cannot be increased; ● Individual client's bank withdraw requests are manual and subject to manual FCO scrutiny; ● Bank deposit requests are subject to further scrutiny from the destination banking institution.
Immediate repetitive deposit and withdrawal in rapid succession of FIAT on the individual client's account (wallet and card services only)	
Carrying out of several transactions in rapid succession within the system, such as the purchase and immediate resale of virtual assets (wallet and card services only).	● Only applicable to Individual Clients. Not applicable to Business Clients; ● Sale and purchase of virtual assets within the platform is not restricted. However, withdrawals and deposits out of the platform are subject to scrutiny.
A change in the geographical destination or origin of a FIAT transaction related to an business client	● Business clients are not allowed to deposit FIAT; ● Business clients are only allowed to perform bank withdrawals to a single bank account under their company name; ● Destination bank account is not easily changed. This information can only be entered once at onboarding and it requires a support request ticket

	to change.

A change in the geographical destination or origin of a FIAT transaction (wallet and card services only)	• All transactions are registered; • Individual clients are only allowed to perform bank withdrawals to a bank account under their name; • Deposits and withdrawals are subject to the Approval of the FCO - if there is a request being made to a jurisdiction that is not in the SEPA region we will receive an Alert.
Mismatch between stated jurisdictional connections as determined at client onboarding and the client activity	
Any incoming or outgoing virtual asset transactions by clients (wallet and card services only)	• All virtual asset deposits and withdrawals are subject to the scrutiny of Sift KYT; • Any transactions flagged as High Risk are blocked and require the approval of an RO for processing; • Any transactions flagged as Severe are blocked and require further investigation by an RO.
Attempts by clients to obfuscate the movement, source or destination of funds, such as by using digital currency mixers/tumblers (wallet and card services only)	
Table 43 - Risk and triggers and corresponding risk mitigation mechanisms	

2. The above listed detection rules implemented by the Company's automated systems will be tested and fine-tuned by the Company and MLRO on an annual basis to ensure that whilst transactions and patterns are actually being detected, they are not generating too many false positives. Similarly, the above detection rules may need to be updated to reflect changing trends.

3. These factors are especially important when one considers the express obligation imposed on the company to examine the purpose and background of complex and unusually large transactions, and unusual patterns of transactions that do not have any apparent economic or lawful purpose. However, in this case, one must bear in mind the amounts involved in the transactions. Should these amounts be unusually large, even if they may be within the normal pattern of transactions carried out by the client, the company may still perform diligence to understand the purpose and nature of such transactions.

17.4 Actions once an alert is received

1. When assessing unusual transactions, the RO may request from the client information and documentation on one or more of the following information:

- the SOF pertaining to the transaction;
- any new operational activities;
- any significant relevant changes (such as a change in occupation for individual clients or change of business activities for business clients);
- any other information or documentation that the company deems reasonably necessary to be satisfied that the funds are derived from legitimate sources.

2. The level of information/documentation to be obtained should allow the RO to come to a reasonable conclusion on the legitimacy of the transaction, but should not be excessive, disproportionate or irrelevant, and the requests should make sense in the context of the transaction and the client.

3. Where notwithstanding the information and/or documentation received, the RO is not satisfied with the explanations provided or has doubts as to the veracity of the information or documentation provided, the RO will consider whether there are sufficient grounds to file a STR. The MLRO should similarly consider fling a STR when the client displays an unreasonable reluctance to cooperate.

4. The MLRO may also determine that despite receiving such alerts the nature of such transactions would not constitute a risk of ML/FT and consequently may determine that a STR is not necessary. Through the initial phases of the company, it is very likely that many false positives will be triggered as part of the calibration process of such systems. In the case of any such alert and the decision not to pursue a STR, the RO or MLRO will make a note to such effect in the Client's profile.

18. Suspicious Transaction Reporting Procedures

18.1. Internal Reporting

1. These procedures detail steps to be followed when the RO knows or suspects, or there are grounds to suspect, that a person or a transaction is connected to ML/FT.

2. Internal reports can be submitted in writing directly to the MLRO, using a standard template *(see Appendix D for Internal Suspicious Transaction Report Form)*, and should contain all relevant information and documentation available to assist the MLRO in making a determination. The RO may be appointed to assist the MLRO or delegated as MLRO in conducting further investigation or authorised to take decisions on behalf of the MLRO.

3. Additional internal reports may have to be made following the submission of an initial report as the designated employee may notice further transactions or activities that give rise to knowledge or suspicion of ML/FT. These too need to be reported to the MLRO.

4. As part of our automated ongoing monitoring systems, the company makes use of software solutions to identify transactions or patterns of transactions which are unusual or exceed a given threshold (either global or client-specific). Any generated reports are transmitted automatically to the MLRO for evaluation.

5. The MLRO must evaluate internal report received and determine whether or not the information contained in the report:

- Does give rise to a knowledge or suspicion of ML/FT;
- Whether further information is necessary to reach a reasonable determination.

6. If more information is required to reach a determination, the MLRO must collect and consider any additional information and/or documentation deemed relevant to make an appropriate determination. Failure to diligently consider all relevant information available may lead to vital information being overlooked and the knowledge or suspicion not being disclosed to the FIU.

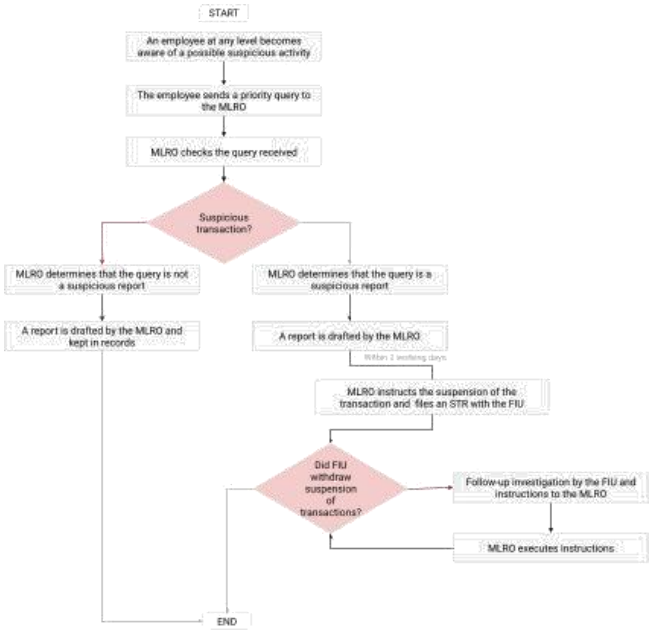
7. If, after careful deliberation, the MLRO concludes that an internal report does not substantially give rise to the suspicion of ML/FT, the MLRO does not need to file a report with or otherwise inform the FIU. In this case, the MLRO must keep a written record of the internal report received, the assessment carried out, the outcome and the reasons why the report was not submitted to the FIU.

8. The final decision to file or not to file an STR must always be made by the MLRO. This does not mean that the MLRO should alone undertake such determination. In reaching a determination on whether an internal report gives rise to knowledge or suspicion of ML/FT, the MLRO can seek assistance, including from internal or external advisors.

9. Independently of the persons involved in the decision process by the MLRO, the decision process should be done discreetly. Communication among persons involved in the decision process should be done on a need-to-know basis and in a manner that does not disclose any information leading to the identification of the subject of the STR or associated client information. Consideration should be taken regarding any non-disclosure obligations that involved persons have to adhere to. It is therefore recommended that a careful stance is adopted when circulating any information internally to avoid risks of leakages and disclosures, which would place the company in breach of its non-disclosure obligations.

18.1.1. Internal Reporting Process

Below you will find the process flow used whenever there is a possible suspicion of ML/FT.



18.2 External Reporting - STR

1. After evaluating that a suspicious transaction and all the associated information, the MLRO can file a STR with the FIU whenever is determined that the company knows, suspects or has reasonable grounds to suspect that:

- a transaction may be related to ML/FT;
- a person may have been, is, or may be connected with ML/FT;
- ML/FT has been, is being, or may be committed or attempted.

2. Whenever there is a suspicion that a transaction may be connected to ML/TF the FIU should be notified via https://www.fu.ee/en/notify-us.

3. The MLRO must file a STR with the FIU no later than the deadline prescribed by the FIU for such reporting. If the FIU does not establish a deadline, the MLRO should file the STR no longer than 2 (two) business days after conclusively identifying the activity as ML/TF.

4. If the external report originated from an internally submitted report by an employee, the MLRO must not disclose the name of the employee who made the internal report to the FIU.

5. The Company is obligated only to file an STRs with the FIU and with no other foreign supervisory authority. This does not preclude however that the company provides follow-up assistance to any foreign supervisory authority, if explicitly requested by the FIU or under the scope of a MLAT.

6. The STR is to be submitted to the FIU through electronic means, using the designated FIU website, identification credentials and template. When preparing an STR, the MLRO should refer to the FIU template, completing the necessary fields accordingly.

7. The MLRO will then follow instructions (if any) received from the FIU.

8. The MLRO will communicate to the FIU the information resulting from the monitoring and the FIU may use that information for the purpose of carrying out its analysis and reporting functions.

18.3 Restrictions on STR Information Disclosure

1. The Company is generally prohibited from disclosing specific information to any external person or entity (with the exception of the ones specifically mentioned below). This restriction applies even to the client and any of its own associated data. Such information includes that:

- An STR has been submitted with the FIU;
- Any client information associated with an STR or that led to the filling of the STR;
- The FIU demanded information within the context of an ML/FT analysis;
- Information has been or may be transmitted to the FIU within the context of an ML/FT analysis (i.e. including considerations of making an STR);
- An ML/FT analysis or investigation on a client has been, is being or may be carried out by the FIU or by a law enforcement agency, respectively.

2. Under this context, the term 'external party' includes any person who does not constitute part of the Company. This includes any person to whom the company may have outsourced any of its functions or processes.

3. When dealing with a Client who is the subject of an ongoing investigation, the RO must still retain the necessary contact with a client and should enquire, in a tactful manner, on the background to one or more transactions or to activity that appears to be inconsistent with the Client's normal pattern of activity. While this is a prudent practice and forms an integral part of the enhanced due diligence measures, such enquiries would not in themselves give rise to client suspicion that an investigation is ongoing.

4. The prohibition from information disclosure is not applicable when submitting or sharing information with:

- Competent supervisory authorities;
- Law enforcement agencies;

- Courts of law;
- Financial provider institutions that have themselves AML/CFT obligations and have a binding contract with the Company, with due obligation of information sharing;
- Branches, parent organizations and subsidiaries of the company;
- Any external party who is a legal or an obliged entity with a mandate to carry out diligence on behalf of the Company under the scope of an investigation. Examples include notaries, enforcement officers, auditors, attorneys or other legal service providers, providers of advisory services in the field of accounting or taxation;

5. It is absolutely paramount that any disclosure to an external party is consented by the MLRO and the company's legal advisor after having done a full inquiry on the legality of such a disclosure.

18.4 Suspension of a Transaction or an account after STR submission

1. Where there is a suspicion or knowledge that ML/TF or related criminal activity is being committed, the corresponding transactions should be suspended and the FIU informed with transaction related information.
2. The transactions in question may still be processed whereas its immediate suspension would reasonably:
   - cause considerable harm, delay or hinder an ongoing or future investigation;
   - impede investigating or identifying the recipient under investigation;
   - cause the client to become aware of a possible STR filling or investigation;
   - be impossible due to underlying technical restrictions outside of the scope of the company (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 reversibility, such as blockchain-based systems).

In those instances, the transaction will be carried and the client will continue to be serviced. A report will be submitted to the FIU thereafter, providing the reasons why the FIU was not so informed before the transaction was executed;

3. The FIU may order the suspension of a transaction or impose restrictions for a set period of time.
4. A transaction may be subsequently performed with written consent of the FIU.
5. An order from FIU regarding an already suspended transaction will prevail over any legal or contractual obligation to which binds the company and the client.

18.5 Suspension of a Client account after STR submission

1. Where there is a suspicion or knowledge that ML/TF or related criminal activity is being committed and an STR is fled, the company must also decide whether or not to continue a relationship with the client who is the subject of the STR. This is a decision that the MLRO must take, depending on the specific circumstances, including the number of STRs associated with the client.
2. The Company must not automatically report to the FIU every transaction carried out by the client after the STR has been fled, unless the FIU specifically requests this to be done.
3. The Company must continue the relationship and not suspend the client account if the suspension would reasonably:

- cause considerable harm, delay or hinder an ongoing or future investigation;
- impede investigating or identifying the recipient under investigation;
- cause the client to become aware of a possible STR filings or investigation.

If a follow-up request regarding the client is received from the FIU, the company should hold discussions with the FIU prior to the suspension of the account, in order to ensure that the steps taken by the company do not hinder or undermine the analysis or any subsequent investigation.

19. Post-suspension Asset Freezing Policy

1. In certain instances, such as after fling of an STR or ongoing client investigation, the company may have been required to:

- Suspend specific client transactions, but still allow client activity;
- Suspend the Client's account , restricting the client from performing any actions (including login) inhibiting the processing of any further transactions.

2. In such cases, the Client's assets will be frozen, until one the following circumstances occurs:

- The FIU instructs the company to allow the Client's account or transaction to be unsuspended;
- The period specified by the FIU request suspension expires, and the FIU does not extend nor does it object the unsuspension;
- A court order instructs the company to allow the Client's account or transaction to be unsuspended

3. In cases where the Company is able to proceed with an un-suspension of a transaction or Client's account after the respective suspension period expires, and the FIU does not oppose its execution, it is up to the discretion of the company's MLRO to proceed with the un-suspension. In this instance

the Company may also decide to terminate the relationship after any pending transactions are carried out.

4. The Company may only proceed with the execution of a transaction that has been opposed by the FIU once the respective suspension period expires. This obligation not to execute a transaction opposed by the FIU prevails over any legal or contractual obligation to which the subject person may be subject.

19.1. Conflict of instructions

In cases where the Company is able to proceed with an un-suspension of a transaction or Client's account after the respective suspension period expires, the FIU can still oppose or extend the suspension period. However, if a court order is issued by a competent court and served to the Company while a transaction is suspended and said order contradicts the FIU instructions, then the Company will be bound by the court order. Thus, in this instance it will not follow the instructions prescribed by the FIU.

19.2 Custody of frozen funds

1. At the request of the Public Prosecutor, the court may determine the freezing of funds, values or assets subject to the applied suspension measure, if it is shown that they are from or are related to the practice of criminal activities or to the financing of terrorism and there is a danger of being dispersed in the legitimate economy.

2. If the Company is instructed to freeze the funds associated with a specific transaction, they will be kept in this state, until a decision otherwise.

3. If the cause of the assets being frozen is the result of an enforcement action directed towards a client, the Company may impose a custody fee to offset its ongoing costs of custody. This fee will be charged for the continuous custody and safekeeping of the funds (including transfers, technical support and maintenance), until a decision is made by the relevant authorities. Any applicable fee will be deducted from the user account on a recurring basis, from the total funds under custody. If the funds frozen are in the form of virtual assets, the Company reserves the right to apply special provisions to secure the integrity and security of the aforementioned funds, namely to secure the funds in a segregated cold-wallet.

5. In the advent of a change, fork or external event that mandates pressing technical changes to maintain the integrity and safeguard of the funds, the Company will duly undertake such measures to the best of its ability. Any such costs will be deducted from the frozen amount;

5. In the advent of a technical protocol split / fragmentation (eg: "hard-fork"), any newly created assets are considered property of the Company, and not under freezing.
6. Due to the nature of virtual assets, transfers may incur at a fixed or variable protocol fee, which lies outside of the Company control. Any such transfer fees will be deducted from the frozen fund amount in question.
7. The company also acknowledges that the many underlying technical aspects of the virtual asset protocols are outside of its control, and cannot be mitigated against due to the nature of such technical protocols (e.g. volatility). These events may lead to a loss of assets while under long-term custody, with no fault borne by the Company.

20. Information Sharing Restrictions

Due to its obligations as a regulated entity, the Company has restrictions on the data that can be shared both internally and with third party entities outside of the organisation. These policies are to include policies and procedures on data protection and are to regulate the sharing of information within the Company, even when any subsidiaries or branches are to be established outside the EEA. This would include policies and procedures regulating the sharing of client private information, and any information associated with their client profile, such as information on a STR or suspicious activity.

20.1 Subsidiaries of the Company

1.. The Company must always ensure that any policies and procedures meet its AML/CFT obligations, even if the jurisdiction of the subsidiary enforces less stringent rules.
2. In situations where the subsidiary's local law restricts or impedes it to fulfill its duties, the subsidiary must follow local laws and regulations, but must inform its parent organization that the Company policies and procedures being applied may not be in line with the policies of the parent Company.

20.2 Sharing and Use of Information

1. Policies and procedures on data protection and the sharing information for AML/CFT purposes must be applied across the Company. An exception is made in this regard to entities delegated with the implementation of AML/CFT policies and procedures.
2. Even if the delegated entities would have no grounds to receive this information (as they

themselves do not have any AML/CFT obligations), the sharing of such information can still be allowed if they are delegated with the implementation of the Company's AML/CFT policies and procedures.
3. Other than the mentioned above, sharing of information would be dependent on:

- the information having been collected by the Company;
- the delegated company having in place proper AML/CFT policies and procedures;
- the application of the delegated company's AML/CFT policies and procedures being under the supervision of the Company.

4. When sharing information for AML/CFT purposes, the Company must bear in mind its non-disclosure obligation regarding Suspicious Transaction Reporting and associated procedures.

20.3 Prohibition to Share Information

1. These policies and procedures impose restrictions on all the Company's employees on the sharing of information. The Company is precluded from disclosing to any third parties that information has been demanded by the FIU or that information has been or may be transmitted to the FIU. This includes internal sharing with members of the Company and its employees not involved in AML-related duties.

2. Any member or employee of the Company is therefore prohibited from disclosing information to a third party or to any member of the Company (other than the employees mandated to accompany the case), such as:

- information on an STR that has, is or will be fled with the FIU;
- information demanded by the FIU within the context of a suspected case of ML/FT;
- information that has been or may be transmitted to the FIU within the context of an ML/FT analysis (i.e. including considerations of making an STR);
- information on an ML/FT analysis or investigation that has been, is being or will be carried out by the FIU or by a law enforcement agency.

21. Reporting Obligations to Providers

22.1 General obligations

1. As part of our obligations towards certain financial providers who are themselves subject to AML/CTF policies (such as banking providers, credit/debit card service providers, exchange providers), we are required to report, disclose and share some elements of our CDD information.
2. Financial providers may require periodic reporting of certain clients classified as High Risk, such as PEPs upon their onboarding, as well as some general metrics indicative of client and business risk.

21.2 Obligation to share Client onboarding data

1. The service provider has the right to request any client onboarding data. This only applies for clients who use the provider's services. This is typically shared upon request, from an inbound compliance request. The Company should return within (4) four business days of the request.
2. Although the deadline described above applies to the service provider currently established (Contis), the mechanisms for sharing data depends on each specific provider.

21.3 Information Sharing Restrictions

1. Despite our obligations to service providers, we are precluded from sharing any Suspicious Transaction Reporting information or data involving ongoing FIU investigations. Despite the fact that we are to share information concerning STRs to the card service provider (e.g. number of STR issues in a specific month), we are restricted by the FIU from sharing any private data information.
2. No person in the Company is permitted to send any details of an STR or anything related to a case of knowledge or suspicion of ML/FT to the card provider or any other person within the Company group with the exception of top management on an absolutely need to know basis.

21.4 Right of Audit

1. The service provider may audit the data sharing process and mechanisms, by giving at least one (1) week's notice, this is in addition to any scheduled audit under contracted terms.
2. Access to any relevant records to be audited must be given to the provider's designated point of contact, as well as for any reasonable assistance required to complete the audit.

21.5 Card Provider Reporting Obligations

1. As part of our obligations towards our card service provider (Contis) we are required to share our CDD with them on a regular basis as well as on the occurrence of certain trigger events. In the following subsections you may find the relevant obligations we ought to perform as well as how we are tackling it.
2. This type of record sharing of client information only applies to individuals clients who are eligible, have or had associated card services provided by Contis. It does not apply to our own clients who are not serviced by the card service provider but may be serviced in other business contexts by the Company.
3. The card service card provider requires us to obtain a series of information and documentation to aid us and then maintain good CDD records on our clients. For further details on what is expected in terms of CDD kindly refer to Customer Due Diligence - Individual Identification Document and Individual Source of Wealth and Source of Funds Documentation Policy sections.
4. Details on the treatment of PEPs can also be found in the PEP Acceptance Policy section.

21.5.1. Obligations to notify of new Clients who are PEPs

1. In cases where an individual client is a confirmed PEP and has successfully been accepted as a client, the card provider must be notified on the same business day.
2. The client information shall be sent by email from the designated and recognized compliance domain email address to a pre-shared card provider email address.

Period of reporting	Reporting medium	Sender	Receiver
Upon request	Summary email, with client details shared via online secure channel	compliance@Blockrhino.com	peps@contis.com

Table 44 - Reporting notifications details

New PEP Notification - Template
Dear Sir/Madam, *Following our reporting duties, we hereby inform you that we have a user confirmed as a PEP, whose file is included in the link below.* *Please let us know if you have any questions or need further clarifications.*

Best regards *Account Compliance*

Table 45 - PEP Reporting notification - email template

21.5.2. Monthly Reporting Obligations

The first business day of each month the Company is required to confirm certain information pertaining to its clients and activities during the preceding month (if any):

- the total number of submitted SARs for clients;
- the total number of submitted SARs for clients during the preceding month which may be linked to fiat transactions that took place on the card provider platform;
- the total number of clients declined due to money laundering concerns;
- the total number of confirmed PEP clients;
- the total number of false positive PEP clients;
- the total number of enforcement actions and/or court orders received which are linked to clients, even if the transactions included in the court order are not linked to provider platform transactions.

2. It should be noted that if any reported figures differ from the provider's records, this may result in audits taking place more frequently and other punitive measures. If necessary, the service provider compliance department is available to provide the necessary assistance required to comply with an enforcement action or court order.

21.5.3. Procedure to execute

The summarized information shall be sent by email from the designated and recognized compliance domain email address to a pre-shared card provider email address. Any associated client data will be sent to the corresponding Compliance department to a protected repository.

Period of reporting	Date of Reporting	Reporting medium	Sender	Receiver
Monthly	First business day of each month	Summary email, with client details shared via online Secure channel	compliance@Blockrhino.com	compliance.queries@primetrust.com

Table 46 - Monthly reporting notification details

21.6 Settlement Provider Reporting Obligations

1. As part of our obligations towards our settlement providers (financial providers, banks or equivalent) we are required to share our CDD with them upon request, as well as on the occurrence of certain trigger events. Incoming requests for individual clients are received by email, from a designated and recognized compliance domain email address (compliance.queries@primetrust.com).
2. These requests are typically received at the provider risk when an individual user withdraws or deposits more than a certain threshold amount in their account, by bank transfer.
3. A strict deadline for reply is included in the received email, typically from (three) 3 to (four) 4 business days and should be sent to the same sender email address. Failure to reply upon the mandated deadline results in account-wide restrictions for the provider account, affecting transactions for all users.
4. The RO and/or MLRO must collect available information regarding the client onboarding information from records, namely:
   - general client profile information;
   - Identity document;
   - Proof of Address;
   - an image showing the client's face;
   - SOF document or information for the specified transaction(s).
5. The image showing the client's face can be extracted from the client's onboarding liveness verification video. Information regarding the client profile can be extracted from the Back Office tool, filling the information fields of the template below on the email body.
6. Note that details can be added, depending on the type of SOF information or document provided.

Period of reporting	Reporting medium	Sender	Receiver
Upon request	Summary email, With client details shared via online secure channel	compliance@Blockrhino.com	<Same address as received>

Table 47 - Reporting response details

Dear Sir/Madam

Please find below the collected due diligence information for the client: *Client email: <USER_EMAIL>* *Phone: <PHONE_NUMBER>* *Legal name: <USER_NAME>* *Birth date: <BIRTH_DATE>* *Birth place: <BIRTH PLACE>* *Occupation: <OCCUPATION>* *Politically exposed person: <No/Yes>* *Source of wealth: <USER_OCCUPATION>* *Source of funds: <STATED_SOURCE_OF_FUNDS>* *Countries of Wealth: <COUNTRIES_OF_WEALTH>* *Funds or wealth from a fagged country: <No/Yes>* *Purpose of the account: <ACCOUNT_PURPOSE>* *Address: <USER_ADDRESS>* *ID document: <STATUS>* *POA document: <STATUS>* *Client ID and selfie and source of funds are attached as an encrypted .zip fle.* *Best regards* *Account Compliance*
Table 48 - Reporting response - email template

22. Law Enforcement Cooperation & Information Requests

1. As part of its duties and as per applicable law and Company policy, the Company is required to cooperate with supervisory and law enforcement authorities in preventing money laundering and terrorist financing, thereby communicating information available to the Company and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation.

2. We comply with Law Enforcement requests for information where it pertains to specific preservation orders and fund freezing. We will not and do not voluntarily disclose non-public information to a requesting party. In accordance with EU and national privacy law, the Company will only disclose non-public user information in response to a legitimate and an enforceable subpoena,

court order or search warrant from a body that has jurisdiction to compel the Company to disclose that information.

3. In cases where the requesting law enforcement agency is from outside of the European Union, procedures under the MLAT may apply.

22.1. General Guidelines for Requests

1. When law enforcement agencies request non-public information (such as a client's personal or financial information), we will not share this information unless an enforceable court order, subpoena or search warrant has been issued, received and validated as legitimate.
2. We will notify affected clients if we believe we are legally required to provide their personal or financial information to a law enforcement agency, unless we are prohibited by law from doing so.
3. When law enforcement agencies request information about a client, we cannot and will not provide information about anyone with whom we don't have an established business relationship.(e.g. one of our Client's customers). We consider this information to be in the possession, control and custody of the Client, who is the controller and processor of such information. If law enforcement agencies request this information, such requests for information should be directed to the relevant Client and not us.
4. Only information specifically requested and clearly outlined in an enforceable court order, subpoena or search warrant will be disclosed.
5. This policy does not constitute legal advice or a promise or guarantee that we will respond to any requests for information in a specific way, timeframe or at all. All legal requests for information are evaluated on a case-by-case basis. We reserve the right to change this policy or these guidelines in our sole discretion at any time.
6. When requesting the confirmation of the existence of data on our platform the law enforcement agency must be very specific about what information it is looking to obtain as we may not be able to respond to vague, ambiguous or blanket requests. Certain identifiers may be helpful in determining whether we currently retain the requested information.

22.2 Submitting a Request

1. All legal requests must be submitted by email to compliance@Blockrhino.com from an email address originating from a recognized government or enforcement authority domain.
2. To aid the expeditious review of information requests, law enforcement officers must include at least the following information in their request:

- name of the law enforcement authority;
- proof that the officer is authorized to request the information (proof of authority) and current position within the law enforcement organization;

- proof of identification of the requesting officer within the law enforcement organization (e.g. photo or other official ID which includes badge number, internal ID number);
- email address from a government domain;
- contact information (email address, phone number) from the governmental organization;
- the name of the legal entity that the request is addressed to;
- details of the request, including:
    - the subpoena/court order identification number in the subject line;
    - instructions on how we should authenticate the subpoena as valid (e.g. call-back procedure);
    - any public blockchain addresses, transaction IDs or identifiers. They must be either plain text, excel (.xlsx) or comma-separated file (.csv) formats (images or PDFs are not accepted);
    - a reasonable deadline for a reply to the request;
    - an official and enforceable court order, subpoena or search warrant;
    - the reason for the requested information (e,g. possible crimes in question);
    - MLAT request for cross-border law enforcement (if applicable).

3. Please do note that failure to include all the mandatory information stated above may result in delayed response times and/or no response.

23. Record Keeping Policy

23.1 Records retained

1. The retention of records is not only intended to show that the Company has complied with its obligations at law but also to assist the FIU, relevant supervisory authorities and law enforcement agencies in the prevention, detection, analysis or investigation of possible ML/FT.

2. The Company has to retain records of all client relationships it enters into and of any transaction carried out, be it an occasional transaction or a transaction that takes place within the context of a continued business relationship. These records are to include any documentation and information produced or obtained in complying with our AML/CFT policies and procedures.

3. The Company is committed in keeping the following records:

- all CDD documents and associated information (including replies to questionnaires);
- transaction documentation and information and other accounts and details in relation to the business transactions whether international or domestic;
- internal reports made to the MLRO;

- external reports in relation to ML/FT, particularly STRs;
- reports issued by the Company to the FIU;
- a record for the reasons for not forwarding an internal report to the FIU;
- a record of AML/CFT training provided;
- a record of any outsourcing agreements;
- the AML Policies and Procedures;
- records of the actions taken to adopt and implement the risk-based approach.

4. The above records shall be of good quality, clearly legible and kept in electronic form.

5. If required by the FIU, an annual compliance report is to be completed by the MLRO, reviewed internally by the Board of Directors, signed by all parties concerned and submitted to the FIU within the required submission period.

23.2 Period of Retention

The date of commencement of this time period depends on the type of records to be retained as set out in the table below.

Record Type	Duration	Start Date
Data and Documents of Client Due Diligence	Eight (8) years	Starting from the date on which the business relationship is terminated, or the last client transaction is carried out.
Data and Documents involving the client relationship, including transactions and client activity	Eight (8) years	Starting from the date on which the business relationship is terminated, or the last client transaction is carried out.
Suspicious Transaction Report	Eight (8) years	Starting from the date the STR was submitted to the FIU.

Internal Reports to the MLRO	Five (5) years	Starting from the date the MLRO reaches the determination not to make a disclosure to the FIU.
Training Records	Five (5) years	Starting from the date the training was concluded.
Employee Screening Records	Variable	Retained until the employment relationship ceases.
Outsourcing Contracts	Five (5) years	Starting from the date of termination of contracted service.
Other Records and Contracts	Five (5) years	Starting from their date of signing or approval.
Table 49 - Periods of retention by record type		

23.3 Record Keeping & Data Protection

1. The Company will inform a customer that the collection of personal data is necessary to comply with its AML/CFT obligations and that any such personal data will be used only for AML/CFT purposes (other than where the Company is subject to additional obligations which require it to process the same data). The Company must ensure that any such data is actually used only for the said purposes and should restrict access thereto accordingly.
2. While these policies do not impose restrictions on a client to access and modify their own data in terms of the applicable laws (e.g. GDPR), they impose constraints that supersede the right of the client to have access to certain parts of their own profile information. This applies to all information pertaining that cannot be shared with the user by law without FIU consent, including analysis or investigation into possible cases of ML/FT, internal data for a submitted STR, ongoing investigations, law enforcement requests, court orders.
3. In line with the prohibition to share information upon STRs, , the client will not be informed of these record's existence as part of their client profile, and will be denied access to these records if specifically requested. The only exceptions to this is if a court order, law enforcement or FIU order mandates this access.
4. Once the eight (8) year retention period expires, the Company will assess the necessity of retaining client data held in terms of its AML/CFT obligations for longer periods. The Company will

then consider any applicable data protection requirements and whether there exists a justification to hold onto the client records for a longer period, whether full or partial form.

5. May the Company decide on the deletion of client data after the retention period, it must do so in a secure manner, so as to safeguard the client's privacy, guaranteeing that the client data is permanently deleted and cannot be reconstructed by a third party.

23.4 Retrieval of Records and Indexing

1. The Company is required to maintain efficient record-keeping procedures that enable it to retrieve and/or grant access to information in a timely manner when so requested by the relevant authorities acting in accordance with the applicable laws.
2. When requests for information are made by the FIU, the Company must ensure that we are able to reply to these enquiries in a timely manner, by not later than five (5) working days from when the demand is made. It should be noted that the FIU may impose a shorter response time for replies to requests for information.
3. The Company may make representations justifying why the requested information cannot be submitted within the requested response time imposed. However, the FIU will always have the final word.
4. To facilitate the retrieval of records and to assist in any compliance monitoring activity conducted by the FIU or other relevant supervisory authorities, the Company will maintain an Index listing all current business relationships in accordance with the requirements of the Implementing Procedures. Such Index must be maintained at all times and be ready for retrieval in a physical or electronic form by the FIU.
5. A similar list should also be maintained for any occasional transactions carried out over the previous eight (8) years and any business relationships that were terminated over the same period of time. Until such time as a more efficient system will be available the aforementioned index shall be used.

24. Training Policy

24.1 General Awareness of AML Topics

The Company is required to take appropriate and proportionate measures for the following purposes:

- ensure that employees are aware of relevant AML/CFT legislation and data protection requirements, and the applicable offences and penalties resulting from breaches of the same, as well as of the Company's AML/CFT measures, policies, controls and procedures;
- provide training in relation to the recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering or the funding of terrorism.

2. The Company has set its training programme, including the content and frequency of any training or awareness raising sessions, on the basis of the risks identified through the Company's Business Risk Assessment Matrix, the specific roles of the employees being trained, and any relevant developments including legislative changes, development of new products or services and new markets targeted by the Company. In all cases, new employees must be made aware of their responsibilities and those of the Company upon their employment or engagement.

3. Awareness and training will be provided to employees whose duties include the handling of relevant financial business, irrespective of their level of seniority. This includes:

- Directors;
- Senior management;
- MLRO and designated employee(s);
- Compliance Officer;
- Reviewing Officer;
- Customer Support Officers;
- all employees of the Company who are involved in activities which fall within the definition of relevant financial business.

4. The Company is required to maintain records of the training provided in order to monitor which employees have received training, how frequently, and the nature of training provided. In line with record keeping requirements, training records are to include:

- the date on which training was delivered;
- the nature of the training;
- the names of the employees who received training;
- a copy of any training materials provided.

24.2 Specific AML Training

1. All employees that engage in Compliance-related tasks must have completed specific minimum training in relation to:

- AML/CTF in an international context
- AML/CTF applied to blockchain transactions
- GDPR (e.g. data privacy)

2. The Company uses third party course materials and online courses from the Association of Certified Anti-Money Laundering Specialists to provide the training. Minimum training must be initiated within one (1) month of a new employee with Compliance functions joining the Company.

3. The following certifications, but not limited to, are considered to fulfill the requirements for required initial training (if they have been renewed and are in good standing for the current period):

- The Association of Certified Anti-Money Laundering Specialists (CAMS) as Certified Anti-Money Laundering Specialist

or from

- The International Compliance Association (ICA) as Anti-Money Laundering Expert

4. If the employee already has achieved and maintains one of the two above certifications, he/she is exempted from completing basic training upon starting his compliance-related functions.

25. Use of Outsourced Systems

25.1 Meaning of Outsourcing

1. Outsourcing means that the Company would not implement certain measures and procedures itself, but rather delegate its implementation to another entity. For the avoidance of doubt, the acquisition of software or access to commercial databases to assist in, or facilitate, the carrying out of AML/CFT obligations without any data or information belonging to the subject person being submitted to and processed by a third party is not considered outsourcing.

2. Outsourcing is to be distinguished from the possibility of having external persons exercising the delegated duties of its own CDD measures.

3. The Company's responsibility for AML/CFT can never be delegated as a whole. As a consequence the Company must effectively monitor how service provider(s) carry out the outsourced AML/CFT measures and procedures and ensure that these are being carried out as required by law and in accordance with its own policies and procedures.

4. The Company should ensure that it has a contingency plan in place in the eventuality of a sudden termination of the outsourcing arrangement. This plan must ensure that the Company can continue to meet its AML/CFT obligations. In the absence of a contingency plan with a suitable replacement service to meet its AML/CFT obligations, the Company could also choose to temporarily halt its activities.

25.2 General Requirements

1. Any outsourcing with a third party must be regulated by written agreement, where the terms and conditions set by both parties are clearly stated.

2. There must be specific requirements to be met for the outsourcing to be permissible. Prior to acquisition or making use of any external software or system in an AML/CFT context, the Company must always assess the system and evaluate the capabilities of the software (such as what types of documents the system is able to screen for authentication, whether the system allows for the retention of documents uploaded) to ensure that the requirements are satisfied.

3. Prior to outsourcing the General Outsourced Activities to a third party, the Company undertakes some procedures, such as the following:

- performing an assessment of any potential ML/FT risk due to the proposed outsourcing;
- maintaining a written record of the assessment;
- assessing the perceived risk;
- ensuring the outsourcing does not negatively prejudice the subject person's ability to comply with its obligations at law;
- ensuring the outsourcing will not impede the effective supervision of the Company by the FIU;
- ensuring the third party has the necessary resources, qualifications, skills and authorisations (if required) at its disposal to effectively carry out the measures and procedures it is to perform on behalf of the Company;
- ensuring the manner in which the third party proposes to implement the outsourced activities on behalf of the Company is in line with all applicable legal requirements and the Company's own policies and procedures;
- ensuring the third party is in good standing, there being no adverse information in its regard;
- ensuring the third party is located and operating from an EU Member State or another reputable jurisdiction with adequate data privacy laws;
- ensuring the third party is not subject to any obligation that would lead to a breach of any data protection, professional secrecy, confidentiality or non-disclosure obligation to which the Company has to adhere.

4. The Company is expected to be able to demonstrate a clear understanding of relevant aspects of the system, namely the kind of scenarios, typologies, detection and rules applied, how the system is compatible with the products or services the subject person offers, and how it can be adjusted to match different profiles or adapt to changes in the client relationship, among others.

5. Regardless of the systems and methods adopted to carry out transaction monitoring, the Company should carry out periodic tests and reviews to assess the effectiveness of the system and should moreover be able to demonstrate a good understanding of their mode of operation.

25.2.1 Automated Systems employed in Client Screening

1. If the Company chooses to employ automated systems to verify client information documents and identity data during onboarding, there are certain requirements that must be met. This applies specifically to the verification of the Identity document that the individual client submits, the liveness check (e.g. ensuring that a real person is submitting the document through the online channel) and the cross-check between all the information submitted.

General safeguards
● The electronic system used to record the document has to record associated client data to ensure that the same natural person is the one submitting the document; ● The electronic system has to automatically record the date and time of the scanning of the document; ● The electronic system has to have safeguards so as not to allow any of the data referred to in the previous two points to be altered, amended or tampered with.
Visual Checks
● The system must be able to compare automatically the facial features on the ID with a separate photograph or a video clip taken by the client, with a high degree of certainty; ● The system must have the capability of comparing the images and determining that the person represented in both photographic images is one and the same, with a high degree of certainty.
Authentication Checks
The system must have the capability of automatically verifying the authenticity and validity of the identification document submitted by performing a number of checks, such as: ● Verifying the security features (such as holograms) of that particular Identity document are in place; ● Reading and validating the Machine-Readable Zone (MRZ) code; ● Examining the document's lamination for anti-tampering; ● Examining the document's layout and features (such as font, typeface and colour) to ensure that these match the respective document's standard.
PEP Screening
● The system must be able to compare the individual client's name and nationality data from the Identity document against lists of known PEPs;

● The system should generate an acceptable rate of false positives.
Sanction Screening
● The system must be able to compare the individual client's name and nationality data from the Identity document against lists of known persons under sanctions; ● The system should generate an acceptable rate of false positives.
Adverse Media Screening
● The system must be able to compare the individual client's name and nationality data from the Identity document against results of adverse online media.
Record Keeping
● All electronic copies of the Identity documents, photographs or videos submitted by the clients must be retained; ● The system must have measures in place to ensure that these records cannot be altered or tampered with.

Table 50 - Automated systems in client screening

25.2.2 Automated Systems employed in Monitoring of Blockchain Transactions

If the Company chooses to employ automated systems to monitor certain types of blockchain-based transactions, there are certain requirements that must be met. This is specifically relevant, as this type of monitoring cannot be reasonably done by a human operator and applies specifically to the risk verification of incoming and outgoing transactions.

Automated Monitoring Systems
● System must generate reports demonstrating the reasons why an alert was raised and which rules or parameters were considered; ● System must be reconfigurable with relative ease and efficiency to cater for changes, new trends and typologies; ● System should have functionalities to learn from previous false positives and fine-tune its future operation; ● System must maintain an audit trail of the alerts raised.

Table 51 - Automated monitoring systems

25.3 Responsibility for Updating Data

1. When making use of a third-party software or platform, the Company should consider who is to be responsible to ensure that information, data and documentation is kept updated. Should this component not be part of the service acquired through the use of this software or platform, the Company must ensure that it carries out itself the necessary on-going monitoring to adhere to its obligations. In addition, even when any such updating is carried out by the service provider itself, the subject person has to ensure that it is informed whenever a client refuses to update the information, data and documentation held through the software or on the platform.
2. In all instances, the Company should not only be in a position to access the information, data and documentation used for verification purposes at all times but must also be in a position to retain copies thereof following termination of the outsourcing agreement.

Appendices

Appendix A1-Client Risk Assessment for Natural Persons

Client Risk Assessment for Natural Persons

Client ML/TF & PF Risk Scoring for Personal Customers

Risk Parameters	Risk Levels	Risk Level Score
Customer nationality	High Risk Country	7
	Medium Risk Country	4
	Low Risk Country	1
Customer Address/ domicile	High Risk Country	7
	Medium Risk Country	4
	Low Risk Country	1
Customer Type	Reputation/Crime- Major Offence	7
	Reputation/Crime- Minor Offence	4
	Reputation/Crime-No Offense	1
Product Type	High Risk Product	7
	Medium Risk Product	4
	Low Risk Product	1
Anticipated Account Activity	Deposits over 5,000/month	7
	Deposits less than 2,000/month but more than 5,000/month	4
	Deposits less than 2,000/month	1
PEP Screening	PEP status	Automatic High-Risk Account
	No PEP status	1
Source of Funds/Wealth	High Risk Country or Business source	7
	Medium Risk Country or Business source	4
	Low Risk Country or Business source	1
Total Risk Calculation		

Risk Assigned:
_____

Legend

Total Risk Calculation	Client Assigned Risk

Score between 7 and 20	Low
Score between 20 and 32	Medium
Score above 32 or PEP Status	High

Appendix A2-Client Risk Assessment for Company Entities

Client Risk Assessment for Company Entities

Client ML/TF & PF Risk Scoring for Business Customers

Risk Parameters	Risk Levels	Risk Level Score
Country of the Business	High Risk Country	7
	Medium Risk Country	4
	Low Risk Country	1
Business Type	Reputation/Crime- Major Offence	7
	Reputation/Crime- Minor Offence	4
	Reputation/Crime-No Offense	1
Product Type	High Risk Product	7
	Medium Risk Product	4
	Low Risk Product	1
Anticipated Account Activity	Deposits over 5,000/month	7
	Deposits less than 2,000/month but more than 5,000/month	4
	Deposits less than 2,000/month	1
PEP Screening (UBO, directors, shareholders, signatories)	PEP status	Automatic High-Risk Account
	No PEP status	1
Source of Funds	High Risk Country or Business source	7
	Medium Risk Country or Business source	4
	Low Risk Country or Business source	1
Total Risk Calculation		

Risk Assigned: _____

Legend

Total Risk Calculation	Client Assigned Risk
Score between 8 and 20*	Low
Score between 20 and 34	Medium
Score above 34 or PEP Status	High

*Some business types are automatically considered low risk. See Section 4.5.b in the AML Policies and Procedures Manual for list of very low risk entities

Appendix B-Declaration form for Business Entity

Business Declaration Form

Name of Business: _____

Entity Incorporation/ Registration Number: _____

Country of incorporation/Registration: _____

Address: _____

Company Telephone No. _____

Company Email address: _____

Name of Person Completing Declaration Form: _____ Position Held in the Company:_____

Contact No. of Person Completing Declaration Form:_____

Email address of Person Completing Declaration Form: _____

Is the person identified above responsible for day-to-day management and policy decision making, including but not limited to financial management and decisions? Yes ☐ No ☐

If No, provide the name and telephone number of the person who has this authority:

Nature of Business (Specify all Services and Products):_____

Years the Company has been in business: _____

Number of Employees: _____

Size of Business: Small ☐ Medium ☐ Large ☐

Geographic Reach of Business: Local ☐ Regional ☐ Multinational ☐

If you have ticked Regional or Multinational above, please specify the jurisdiction in which you company operates: _____

Type of ownership: Sole ☐ Partnership ☐ Other ☐ (Specify): _____

I/We acknowledge and confirm that the information provided above is true and correct to the best of my/our knowledge and belief. In case any of the above specified information is found to be false or untrue or misleading or misrepresenting, I/We am/are aware that I/We may liable for it.

Name: _____
Signature: _____
Date (MM/DD/YYYY): _____

Appendix C- Beneficial Ownership Declaration Form

Beneficial Ownership Declaration Form

The regulations of the EU require that the beneficial owners of all companies be known by the financial institutions providing products and/or services. In light of these requirements, please complete the below form with the correct information.

All individuals who are ultimately entitled to control or exercise the control of 20% or more of the voting rights of the company, either directly or indirectly through their beneficial ownership of an underlying corporate shareholder, should be regarded as Principal Shareholders/Beneficial Owners of the Company.

Section A: Company Details
Company Name:
Entity Incorporation/ Registration Number:
Country of incorporation/Registration:

Section B: Ultimate Beneficial Owner/s Details
The details of natural persons who are the ultimate beneficial owners who directly and/or indirectly hold = > 20% ownership in the Company or who exercise control over the company are as follows:

No	First Name	Middle Name	Last Name	Number of shares owned	% of Holding in the Company	Date of Birth (MM/DD/YYYY)	Nationality	Company Title / Occupation	Residential Address and Country of Residence
1									
2									
3									
4									
5									
6									
7									

Please note that you are required to provide the following for all listed beneficial owners:

- Valid Picture ID
- Proof of Address e.g. bank statement, utility bill no older than 3 months

Section C: PEP & Reputation Status for Ultimate Beneficial owner/s

With respect to each of the above listed individuals, please confirm the following:

Politically Exposed Person (PEP) Declaration - Tick as appropriate

1. Have any of the above-listed beneficial owner/s currently hold/have held/are being considered for a position as a Political Exposed Person (see explanation of PEP below)?

A PEP is a current or former senior official in the executive, legislative, administrative, military or judicial branches of a government, whether elected or appointed, or paid or not; or a senior official of a major political party; or a senior executive of a government-owned or government funded corporation, institution or charity. A PEP also includes the "close associates" and "immediate family members" of a PEP. A close associate is a person (i) who is widely and publicly known to have a close association with a PEP, or (ii) who is actually known by the business to be a close associate of the PEP, even if the association is not widely known. The immediate family members of a PEP include, for example, spouses, domestic partners, parents, siblings, children, step-children, the spouses of children, and a spouse's parents and siblings.

Yes ☐ No ☐

If yes, please provide details below.

.....
.....
.....

2. Have any of the above-listed beneficial owner/s ever been convicted of a felony or any other serious crime in the country where the services will be rendered or in any other country (other than traffic violations)? Are there any legal proceedings of this nature pending?

Yes ☐ No ☐

If yes, please provide details below.

.....
.....
.....

I/We acknowledge and confirm that the information provided above is true and correct to the best of my/our knowledge and belief. In case any of the above specified information is found to be false or untrue or misleading or misrepresenting, I/We am/are aware that I/We may liable for it.

Name: _____
Signature:_____

Date (MM/DD/YYYY):_____

Appendix D- Internal Suspicious Transaction Report

Internal Suspicious Transaction Report

Reported by	Function	Date:

Reported To (Name of CO)

Date of Transaction/Activity:	
Reference information (attach copy of instruction and/or relevant information if available)	
Name of Client	

I consider the above transaction to be suspicious for the following reasons:

_____
_____

Signed_____

Name of Reviewer:	Date Reviewed:

I have reviewed the above transaction and I consider that the transaction is/is not suspicious for the following reasons:

_____
_____
_____

Signed _____

Position _____