Anti-Money Laundering and Combating of Terrorism Financing (AML/CTF) Policy

Card Solutions UAB, Vilnius, Girulių g. 10 Lithuania

Policy about how to prevent money laundering, terrorism financing and sanctions violations.

Place & Date:
12112 Vilnius, 08.03.023

Table of Content

1 Content and purpose

Card Solutions UAB (hereinafter "the Company") qualifies as a Lithuanian financial intermediary pursuant to Art. 2 (3) of the Anti-Money Laundering Act (AMLA).

The Company is committed to assist in the fight against money laundering, financing of terrorism and sanctions violations by operating an effective, risk-based compliance framework. The objective is to manage regulatory and reputational risks actively, to mitigate those and thereby prevent, detect and report money laundering and terrorist financing as well as sanctioned individuals and companies.

This AML/CTF policy defines the principles and guidelines for the prevention of money laundering and terrorist financing as well as dealing with sanctions exposure (AML/CTF) and ensuring the fulfilment of due diligence requirements as defined by the applicable regulatory framework.

2 Scope

The principles and measures, which are defined in this policy, apply to all employees of the Company including the Executive Committee and the Board of Directors. In case the Company maintains one or several subsidiaries, the principles of this policy are also applicable for those subsidiaries under consolidated supervision.

The Company is committed to the principle of "three lines of defense". Employees with direct customer contact act as the first line of defense ensuring that the customer relationship is compliant with regulatory requirements. The AML Officer, as part of the second line, advises the first line, monitors and reports on AML/CTF and the auditor, as the third line, reviews the work of the AML Officer.

3 Regulatory basis

The following regulatory requirements apply as the basis for this policy:

- Federal Act on Combating Money Laundering and Terrorist Financing (AMLA) and the Ordinances on Combating Money Laundering and Terrorist Financing (AMLO).

In addition, the statutes of the Company, organizational regulations and other policies of the Company apply.

4 Definitions and abbreviations

The terms as listed beneath shall have the following meanings:

AML Officer	External or internal person ensuring the implementation of the AML/CTF framework within the Company
AML/CTF	Anti-money laundering, counter terrorism financing and prevention of sanctions violation
Assets	All items of value such as Virtual Assets, FIAT currencies, shares and investment products
Beneficial Owner	Each person who is the ultimate, effective economic owner of the Assets involved in the relationship
Board of Directors (BoD)	All members of the Board of Directors together. The body which bears the overall responsibility for the Company.
Cash transactions	All (physical and non-physical) transfer of Assets, in particular the exchange of money, cryptocurrencies, precious metals, traveler's checks and the like, which are not part of a permanent business relationship
Compliance	Ensuring adherence to legal, regulatory and internal provisions as well as the observance of customary market standards and code of conduct.
Contracting Partner	A customer who has a business relationship with the Company based on a contract for using its services and products
Controlling Person	Individual who exercises control over a legal person either as shareholder, managing director or otherwise
Cryptocurrency	Any Virtual Asset which is classified as payment token
Executive Committee (EXCO)	All members of the Executive Committee together. The body which implements and executes the Company's strategy.
FATF	Financial Action Task Force, sub-organization of the OECD responsible for setting international standards on the fight against money laundering
FIAT	Any money declared by a government to be legal tender
High-risk Business Relationships	Business relationships with increased AML/CTF risks

High-risk Country	Countries with increased money laundering risks
High-risk Business Sector	Business sectors with increased money laundering risks
KYC file	Know your customer file. The file containing all relevant background information about a customer.
MROS	Money Laundering Reporting Office
MRZ	Machine-readable zone, part of an identification document
Permanent business relationship	Business relationship which is not limited to the performance of one-off financial activities
Politically Exposed Person (PEP)	Individual or related person who is or has been entrusted with prominent public functions in politics, governments, military, justice or in state corporations as well as in intergovernmental organizations or international sports associations
Relationship / transaction with increased risk	Relationship or transaction, which fulfils the criteria for being classified as with increased risk (also called high-risk relationship & high-risk transaction)
SECO	The Lithuanian state secretariat for economic affairs
SRO	Self-regulatory organization the Company is required to become a member of
TAN	Transaction number, a one-time password used for verification
Travel Rule	The FATF Recommendation 16 on wire transfers requests virtual asset service providers (VASP) to exchange originator and beneficiary identifying information with counterparties during transmittals.
VASP	Virtual Asset Service Provider
Virtual Assets	Any assets in form of token that are based on decentralized technology including utility, payment and asset token

5 Customer review

5.1 Principles

5.1.1 Prohibited Assets and business relationships

The Company does not accept Assets if the Company knows or is aware of indications that these assets are the proceeds of criminal activities or qualified tax evasion, even if the respective crime or offense was committed abroad.

The Company does not start a business relationship with any person that is knowingly connected to money laundering, financing of terrorism or listed on a sanctions list. Prohibited are in particular business relationships with persons for which it is known or reasonably suspected that they are involved in criminal or terrorist activities or support criminal or terrorist organizations.

The Company does not open or maintain any business relationships with banks that have no physical presence in the place of incorporation (fictive banks or shell banks).

Neither a business relationship with a person active in a "non-serviced" business sector nor with a person domiciled in a "non-serviced" country will be opened nor a transaction to such a country will be executed or from such a country accepted (as outlined in Appendices).

5.1.2 General business restrictions

The Company does not accept, exchange, deliver, hold or provide any physical cash (bills or coins) or any other physical items of value.

The Company does not accept deposits from the public. However, the company reserves the right to make use of the EUR 1m sandbox threshold and/or the 60 days settlement period. In case the Company makes use of the EUR 1m sandbox threshold, the respective regulatory requirements as outlined are met. Every customer affected is informed and expressly accepts prior to the Company accepts the customers deposits:

- That the deposits are not covered by the Lithuanian depositor protection

The Company is not entering into a business relationship with

- an association
- a foundation
- an insurance wrapper or similar structures
- Escrow structures
- Politically exposed people (PEP)

When onboarding individuals, only a natural person owning beneficially her-/himself the assets involved in the relationship is accepted.

The following services are not offered:

- Pseudonym and numbered mandates
- Joint mandates

The Company only accepts permanent business relationships.

5.2 Establishing a business relationship

Business relationships are commenced based on the provisions in the Regulations by following the process as outlined beneath.

5.2.1 Identification principles

The Company identifies its customers

- in person
- by correspondence

If the identification cannot be performed in line with the requirements outlined beneath or cannot be completed because of quality issues, the identification is stopped and either repeated or cancelled.

The Company documents the identification process.

5.2.2 Identification of natural person

The following process applies for natural persons identified **in person**:

1. The customer provides the relevant personal data as outlined in "Documentation requirements (KYC)".
2. The customer presents an identification document the Company takes a copy from declaring to have taken the copy from original by dating and signing the copy.
3. The customer completes a written declaration (Form A) confirming the identity of the beneficial owner of the Assets to be brought into the relationship.

The following process applies for natural persons identified **by correspondence**:

1. The customer provides the relevant personal data as outlined in "Documentation requirements (KYC)".
2. The customer provides a certified copy of his/her identification document.
3. The customer sends a copy of a utility bill as proof of domicile address. The Company ensures that the address correspond with the address provided.
4. The customer completes a written declaration (Form A) confirming the identity of the Beneficial Owner of the Assets to be brought into the relationship.

5.2.3 Identification of legal entities

The following process applies for legal entity identification:

1. The customer provides a certified extract from the commercial register of the respective country ***or***
The customer provides a certificate of incorporation in original or as a certified copy if the company was founded within the last 12 months or a certificate of good standing in original or as a certified copy if not
or
The Company prints or downloads an extract from the commercial register or from a trustworthy private database, marks it as printed or downloaded and adds date and signature.

2. The natural person(s) opening the business relationship is (are) identified like a natural person. The Company ensures that the person(s) is (are) entitled to act on behalf of the legal entity.
3. The customer completes a written declaration (Form K) confirming the identity of the Controlling Person of the legal entity or, in case of a domiciliary company, completes a written declaration (Form A) confirming the identity of the Beneficial Owner of the Assets to be brought into the relationship. Both can be done via TAN method.
4. The Identity of the Controlling Person(s) of the legal entity (Form K) or of the Beneficial Owner(s) of the Assets (Form A) is (are) verified.
5. Other signatories are disclosed by the customer and taken on file.

If the customer is a **trust**, the trustee provides either a certified extract from the commercial register of the respective country or a copy of the trust deed or other equivalent document. The trustee is identified following the process of identification of a natural person or legal entities. The trustee completes a written declaration (Form T) confirming the declaration of the trust, the settlor, the protector and the beneficiaries. In case of a revocable trust, the person who can revoke the trust is to be declared.

5.2.4 Documentation requirements (KYC)

For any **natural person** as customer, the following information is to be collected and documented in a customer profile:

- Family name and first name
- Date of birth
- Nationality/ies
- Domicile address (street, city and country)
- Business sector of activity
- Place/s of business activity/ies
- Financial circumstances (declaration of income and total wealth)
- The intended use of the assets involved in the business relationship
- Nature (currency) and amount of the assets involved
- Source of the assets involved (source of funds)

For any **legal person** as customer, the following information is to be collected and documented in a customer profile:

- Company name
- Domicile address
- Business activity/ies
- Place/s of business activity/ies
- Financial circumstances (turnover)
- The intended use of the assets involved
- Nature and amount of the assets involved
- Source of the assets involved (source of funds)

The information provided is reviewed with regards to plausibility. Should the information appear contradictory or implausible, the Contracting Partner is contacted for clarification. If clarifications are not successful, in case of a relationship with increased risks and if indications for money laundering, terrorism financing or sanction violation occur, the AML Officer is approached. The AML Officer undertakes an enhanced due diligence and, if indications remain, starts an investigation.

The AML Officer defines a sample size for standard risk relationship without any such indications and performs spot checks on the relationship opening documents after being onboarded.

5.2.5 Exposure check

Any customer including any person involved is matched with relevant PEP- and sanctions-lists. The minimum requirements are EU sanctions and US sanctions (OFAC list).

- In case of a person listed on a sanctions list, the opening of a relationship is denied
- In case of indications for money laundering, terrorism financing or sanctions violation, the opening of a relationship is denied

In case of a negative exposure as listed above or any other negative exposure, the AML Officer is approached immediately for further investigation and to clarify whether a reporting duty as outlined in "Reporting & documentation" is given.

In order to perform sanctions, PEP and negative exposure checks, the Company cooperates with an established tool provider fulfilling Lithuanian standards.

5.2.6 Risk classification and acceptance

The Company assigns, based on the risk scoring as outlined beneath, every business relationship to one of the following categories:

- Risk category 1 (score 0 - 1) Standard risk business relationship
- Risk category 2 (score ≥ 2) Business relationship with increased risks (high-risk business relationship)

If the risk score is ≥ 2 the business relationship is classified as a business relationship with increased risks (high risk business relationship).

The Company uses the following risk criteria based on the assessment of the risks inherent to the Company's business case with scoring:

- Domicile or residence of the Contracting Party, the Controlling Person or the Beneficial Owner (for scoring of countries see Appendix)
- Place of the business activities of the Contracting Party or the Beneficial Owner (for scoring of countries see Appendix)
- Sector of business activities of the Contracting Party or the Beneficial Owner (for scoring of business sectors see Appendix)
- Complexity of structures, particularly if using several domiciliary companies or a domiciliary company with fiduciary shareholders in a non-transparent jurisdiction (scoring: non-complex: 0 / complex: 1)
- Frequent transactions carrying an increased risk (scoring: no frequent high-risk transactions: 0 / frequent high-risk transactions 1)
- Total amount of wealth of the Contracting Party, if an individual or a domiciliary company, is > 10 Mio. EUR or equivalent (scoring: <10 Mio. EUR: 0 / >10 Mio. EUR: 1)

In case one criterium has several answers (such as several sectors of business activities), the one with the highest risk exposure prevails. In case several persons are involved in the relationship, the one with the highest risk exposure prevails.

A business relationship is in any case classified as high-risk (score: 2) if:

- any Politically Exposed Person is involved in the business relationship
- the domicile or residence of the Contracting Party, the Controlling Person or the Beneficial Owner is located in a country that is on the following two lists of FATF: "high-risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring". (if not restricted see Appendix)
- an investigation because of money laundering, terrorism financing or sanctions violation was conducted by the Company (irrespective of the outcome)

- the Company considers the business relationship as high-risk due to any other reason based on a risk assessment by the EXCO or the AML Officer

In case a business relationship is classified as high-risk, enhanced due diligence is undertaken by the AML Officer before onboarding is completed. If during its lifecycle, a business relationship is re-classified as high-risk, enhanced due diligence is undertaken without delay.

Depending on the circumstances, enhanced due diligence may include (not exclusively)

- the collection of information from the Contracting Partner
- the consultation of reliable publicly accessible sources and databases
- information from trustworthy individuals or authorities

The AML Officer assesses the results of the enhanced due diligence with a view to plausibility. If necessary, the AML Officer clarifies the background of the relationship, requests further documents or starts an investigation. The result of the clarification is documented in such way that a third party can easily understand the economic background and purpose of the business relationship.

An EXCO member decides on the acceptance of any new business relationship with increased risks. The decision on the acceptance or decline of a business relationship is documented.

The Company does not use the following risk criteria:

- Nationality of the Contracting Party or the Beneficial Owner (see Appendix)
  A person's nationality does not provide great confidence about a potential money laundering/terrorism financing risk in particular considering the global economy the Company is operating in.
- Lack of personal contact to the Contracting Party and the Beneficial Owner
  Since the Company's focus is not on identification in person and if considering the shift towards a digital economy, missing personal contact is not considered as a supportive risk factor.
- Nature of requested goods or services
  The Company offers a very limited range of services that are of an equivalent exposure. Therefore, the nature of services requested is not a supportive risk factor.
- The amount of assets introduced
  Since the business case of the Company also includes investment in a highly volatile asset class, the amount of assets introduced may lead to constant changes of the risk level of the customer and is therefore not a supportive risk factor.
- Amount of inflowing and outflowing assets
  Due to the nature of the Company's business activity, a high frequency of in- and outflows is expected. Therefore, this criterium does not provide any additional confidence.
- Country of origin or destination of frequent payments
  Since the token economy operates globally as well as the country of origin and destination of token transfers remain often in transparent, this risk factor does not provide great support.

5.2.7 Rejection or termination of a business relationship

The rejection or the termination of the business relationship is mandatory if:

- the Company had been misled by the Contracting Partner during the identification process
- the Company received a false statement about the Beneficial Owner or the Controlling Person of the Assets to be involved in the business relationship
- doubts about the information provided by the Contracting Partner persist even after repeating the identification of the Contracting Partner, the Beneficial Owner or the Controlling Person

In case of a non-cooperative Contracting Partner, the AML Officer is notified immediately. Generally, in case of a continuously non-cooperative Contracting Partner, the business relationship shall be terminated. The AML Officer recommends the closing of the business relationship to the EXCO if the deficiencies occurred cannot be solved otherwise and a termination appears to be appropriate. An EXCO member takes the final decision.

If there is suspicion for money laundering or terrorism financing, the AML Officer performs an investigation. In such cases, the business relationship must neither be terminated during the investigation nor if the conditions for a reporting as outlined in “Reporting & documentation” are fulfilled.

5.3 Monitoring

5.3.1 Monitoring principles

The profile of the Contracting Partner is kept up-to-date and changes to the customer’s data are recorded on an ongoing basis. In addition, profiles are reviewed regularly depending on the respective risk level.

All employees and external service provider performing AML relevant tasks like an internal employee have the duty to inform the AML Officer if money laundering, financing of terrorism or sanctions violation is suspected or if there is awareness of any activity and/or transaction which indicates such exposure. The same duty applies in case of circumstances that may lead to legal or reputational risks for the Company.

5.3.2 Regular update

Business relationships are periodically updated in line with their level of risk.

Risk category 1	bi-annually (every 2 years)
Risk category 2	annually

Business relationships classified as high-risk are in addition at least annually reviewed by the AML Officer. The continuation of the business relationship is subject to an EXCO Member approval.

The Company repeats the procedure of identification if doubts arise during the business relationship as to whether the information given concerning the identity of the Contracting Partner is accurate or, in case of a natural person as Contracting Partner, whether the Contracting Partner is identical with the Beneficial Owner and these doubts cannot be eliminated by means of usual enquiries.

5.3.3 People monitoring

Throughout the duration of the business relationship, crosschecks on the Contracting Partner, the Controlling Person and the Beneficial Owner against the PEP- and sanctions list are undertaken.

If a Contracting Partner is identified as negatively exposed, the business relationship is passed on for review to the AML Officer and re-classified as high-risk. The AML Officer undertakes enhanced due diligence on the background of the customer. In case of an indication for money laundering, terrorism financing or sanctions violation, the AML Officer starts an investigation.

5.3.4 Transaction monitoring

These rules apply for FIAT as well as Virtual Assets transactions.

The Company classifies every transaction as either a standard or a high-risk transaction. A transaction is considered as high-risk if at least one of the following criteria is met:

For individuals:

1. Threshold single transaction individuals
   - Risk category 1 EUR 250'000 (or equivalent)
   - Risk category 2 EUR 100'000 (or equivalent)

   Several transactions at the same business day are considered as a single transaction.

2. Threshold multiple transaction individuals
   - Risk category 1 turnover of EUR 500'000 (or equivalent) in one calendar month
   - Risk category 2 turnover of EUR 250'000 (or equivalent) in one calendar month

For legal entities:

3. Threshold single transaction legal entities
   - Risk category 1 EUR 1'500'000 (or equivalent)
   - Risk category 2 EUR 500'000 (or equivalent)

   Several transactions at the same business day are considered as a single transaction.

4. Threshold multiple transaction legal entities
   - Risk category 1 turnover of EUR 2'000'000 (or equivalent) in one calendar month
   - Risk category 2 turnover of EUR 750'000 (or equivalent) in one calendar month

The minimum number of transactions to trigger the multiple transaction threshold are two. In case a bunch of transactions reach together the threshold for multiple transaction monitoring, the calculation of the limit for further transactions starts from zero.

5. Country of origin

All transactions performed by a customer domiciled in a country that is on the following two lists of FATF: "high-risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring". (if not restricted see Appendix)

The following transactions are always deemed to carry an increased risk (to the extend relevant for the business case of the Company):

- Transactions in cases where, at the beginning of a business relationship, assets equivalent to a value of EUR 100’000 are physically introduced, whether in one payment or split into several payments
- Money and asset transfers in one or split into several transactions which appear connected reach or exceed the amount of EUR 5’000 if no permanent business relationship is associated with these transactions.
- Payments from or to a country which is considered "high-risk" or non-cooperative by the FATF and for which the FATF demands a higher level of due diligence (see Appendix)

The Company has an effective process in place to monitor transactions in order to facilitate the detection of high-risk transactions. It operates an electronic monitoring system. Hits generated by this system are to be analyzed and commented by the first line of defense and reviewed by the AML Officer.

Depending on the type of business activities conducted, the following questions are of particular relevance:

- the reason for the transaction
- the origin of the Assets
- the connection of the transactions with the Contracting Partner’s business activity
- the reason for significant deviations from the type, volume or frequency of transactions that would be usual in the context of the business relationship
- the reason for significant deviations from the type, volume or frequency of transactions that would be usual in comparable business relationships

The AML Officer reviews the comment and either approves, rejects and ask for further clarification or start an investigation in case of indication for money laundering, terrorism financing or sanction violation.

5.3.5 Transaction monitoring Virtual Assets (additional requirements)

In case of crypto transactions with external wallets only:

a) Travel Rule

In- and outflows in Virtual Assets performed from or to an external wallet are permitted if the customer of the Company is identical with the person controlling the external wallet by having access to the wallet. The Company verifies this requirement by using technical means as follows:

- Providing an external wallet to the credentials presented by the customer of the Company during the on-boarding process ***or***
- Obtaining a print-screen of the external wallet ***or***
- Verifying access of the customer of the Company to the external wallet presented by a transfer of a small amount (so called Satoshi test) and getting proof of receive by the customer ***or***
- Verifying access of the customer of the Company to the external wallet presented by sending a message (such as a password) to the wallet of the customer and getting proof of receive by the customer ***or***
- Obtaining a digital signature verification for both single and multi-signature (MultiSig) wallets

After successful proof of control, the wallet is assigned to the customers’ profile and can be used for in- and out-going payments in Virtual Assets.

If an incoming transaction is not originating from a verified wallet of the customer, proof of control must be provided immediately. Otherwise, the Company initiates an investigation for suspicious transactions.

In case the customer uses an external wallet hosted by a third party, the provider of hosted wallets submits the name, account number and address of the respective wallet holder as well as the name and account number of the beneficial owner so that the Company is able to provide full identification.

The proof of control will be regularly repeated according to the following rules:

- For business relationship with risk category 1: after 18 months
- For business relationship with risk category 2: after 12 months
- In case of doubt that the customer still has control over the wallet

For inter-VASP transactions, the Company may make use of a travel rule protocol such as the TRP or the OpenVASP protocol in order to receive identifying information about the person receiving or sending the Virtual Assets from or to the customer.

6 Reporting & documentation

The Company informs its supervising regulator immediately about any report made to authorities.

6.1 Duty to notify MROS

Based on art. 9 para 1 AMLA, a duty to notify the Money Laundering Reporting Office Switzerland MROS is given, if the Company knows or has reasonable grounds to suspect that Assets involved in the business relationship

- are connected to an offence in terms of art. 260ter no. 1 or 305bis Lithuanian criminal code (SCC)
- are the proceeds of a criminal act or of a qualified tax offence according to art. 305bis no. 1bis SCC)
- are subject to the power of disposal of a criminal organization or serve the financing of terrorism (art. 260^{quinquies} paragraph 1 SCC)

In case of such indication, the AML Officer has to be informed immediately. The circumstances and the background of the case will be analyzed by the AML Officer. After the review, the AML Officer informs the Executive Committee and presents an assessment as well as a recommendation. The Executive Committee decides on any notification based on the recommendation of the AML Officer. The decision is documented. The necessary notifications are made by the AML Officer subsequent to the respective decision of the Executive Committee.

The Company immediately notifies MROS if it terminates negotiations aimed at establishing a business relationship because of a reasonable suspicion as defined above.

The Company immediately notifies MROS if the Company knows or has reason to assume that the data passed on by FINMA or the supervising regulator is relating to a person or organization corresponds to the data of a

Contracting Party, a Controlling Person, a Beneficial Owner of the assets or an authorized signatory in a business relationship or transaction. In this case the Company immediately freezes the Assets entrusted to it and related to the report.

In connection with reports according to article 9 AMLA, the Company freezes the Assets entrusted to it and related to the report as soon as the MROS informs the Company about forwarding the report to theprosecution authorities. The Company keeps the Assets frozen until it receives an order from the competent prosecution authority, but at the most for five working days from the date at which the MROS informs the Company about forwarding the notification to the prosecution authorities respectively from the date at whichthe AML Officer notified the MROS.

The Company is prohibited from informing the Contracting Partner affected or third parties of the notification.

6.2 Right to notify MROS

If the Company does not have reasonable grounds for suspecting money laundering activity or financing of terrorism, but has indication suggesting that Assets are derived from criminal activities or legal funds are misused for criminal purposes, the Company is entitled to take one of the following actions:

- to notify the MROS based on the right to notify
- to continue the business relationship under increased control (re-classification as high-risk business relationship)
- to terminate the business relationship

6.3 Sanctions reporting

In case of a potential reporting duty to SECO based on a sanction list finding, the AML Officer summarizes the situation and presents it to the Executive Committee including a recommendation. The decision of the Executive Committee and the reasons behind is documented.

6.4 Documentation and data storage

The company creates and organizes their documentation in a manner allowing a competent third party at any time to make reliable conclusions regarding compliance with the legal and regulatory obligations concerning AML/CTF.

Documents and records are created and stored in a manner allowing the Company to respond to any requests for information and seizure by competent authorities within the period of time required. The company maintains an up to date AML file for each contracting party containing all information of fundamental significance to the establishment of facts with regard to an AMLA-relevant business relationship as well as a list of acquisition and information of relationship closed. Each individual transaction is at any time constructible.

The Company holds physical paper or electronic copies of all significant documents. Documents and reports are stored in a secure place (inaccessible to unauthorized third parties) in Switzerland.
The following requirements are applicable:

- Possibility to print out the necessary information on paper if requested
- The server used is located in Lithuania
- All data is accessible to the Company at all times
  The requirements pursuant to Arts. 9 and 10 of the Lithuanian Accounts Ordinance concerning permitteddata medium as well as data review and migration apply in addition. All customer related data are stored in an unchangeable form as a regular backup.

The Company retains documentation for a period of ten years following the end of the business relationship or the conclusion of the transaction.

Documents which are of fundamental significance for the establishment of facts concerning a business relationship and which are not written in one of the official languages of Lithuanian or in English are translated into English or into one of the official languages of Lithuanian by an appropriately qualified and approved translator.

7 Third parties

The Company might engage third parties for the fulfilment of duties of due diligence or otherwise work with third parties as cooperation partners such as external service providers or business partners.
The responsibility for being compliant with the duties carried out remains with the Company and the duty to report and the duty to freeze assets as well as the decision about acceptance or termination of a business relationship cannot be delegated to a third party.

When engaging third parties, the following conditions are met:

- Evaluation and careful selection of the appointed person and guarantee of the person for proper business conduct
- Instruction of the person with regards to its responsibilities by concluding of a written agreement with the appointed person or company
- Control of the person whether the appointed person is complying with the duties of due diligence

The Company ensures that any third parties to whom due diligence tasks were delegated to, do not themselves delegate those tasks further to any other person or company.

8 Responsibilities

Generally, all employees including the BoD as well as the EXCO are responsible for following and being compliant with all applicable external and internal provisions and are requested to immediately report any breaches to the AML Officer.

External service providers are also to be bound to a comparable level of compliance.

8.1 Board of Directors

The BoD bears the overall responsibility concerning the risks in the Company and supervises the Company's activities in this regard. The implementation of risk mitigating measures may be delegated to the EXCO. A member of the BoD is designated as the person responsible for overseeing the implementation of the regulatory framework for Compliance.

In particular, the duties of the BoD are:

- Sets up an appropriate company structure that enables and ensures compliance with relevant AML/CTF regulations
- Approves this policy
- Establishes, records and approves the general principles relating to AML/CTF
- Ensures that the AML Officer as well as any other person assigned to implement AML/CTF tasks, receive all relevant data and information in a complete, correct and timely manner
- Ensures that all employees are aware of the AML Officer and are informed when and what shall be reported to the AML Officer
- Ensures that the AML Officer has sufficient resources to effectively carry out its responsibilities including competent personnel and technological equipment
- Evaluates and approves the annual AML Officer report and takes correcting measures in case of weaknesses and deficiencies

8.2 Executive Committee

The EXCO performs all corporate management tasks that are not assigned to the BoD or have been delegated by the BoD to the EXCO. The EXCO holds the responsibility that the Company's business activities are performed in a compliant manner. This duty cannot be delegated to a third party.

In particular, the duties of the EXCO are:

- Implements this policy
- Appoints one or several persons who has/have the skills, experience and expertise to serve as AML Officer, ensures deputization if required and determines and controls the responsibilities and duties of the AML Officer based on the requirements as outlined in this policy
- Decides on the acceptance, continuing and termination of business relationships
- Decides about MROS, SECO and FINMA notifications based on the recommendation of the AML Officer
- Grants the AML Officer unrestricted access to the EXCO and the BoD
- Performs all reporting duties towards the regulator as well as towards customers
- Supervises all third parties to whom task of the Company have been delegated to

8.3 First line support

The Company maintains a first line support that prepares customer related tasks in order be reviewed by the AML Officer. The tasks are in particular

- Ensuring that the onboarding process was performed in a complete and correct manner

- Double check the data entered by the customer and verify data if needed (such as address on utility bill, sender information of the bank transfer, face comparison where needed)
- Requests additional information from the customer where required
- Performs KYC reviews
- Further tasks in coordination with the AML Officer

8.4 AML Officer

The AML Officer serves as the anti-money laundering, counter terrorism financing and sanctions competence centre. The AML Officer supports and advises the Company in the implementation of this policy without overtaking the responsibility for correct implementation by the Company.

The tasks of the AML Officer are in particular:

- Supports and advises employees and the EXCO with regards to the implementation of anti-money laundering, counter terrorism financing and sanction-related regulation
- Proposes regular amendments to this policy
- Creates and updates the AML/CTF activity plan
- Prepares and updates regularly the Company's AML/CTF risk assessment for the attention of the EXCO and the BoD
- Arranges for additional enhanced due diligence on high-risk business relationships
- Performs investigation in case of indication for money laundering, terrorism financing or sanctions violation
- Controls regularly the high-risk business relationship review
- Advises the EXCO to open, keep, report or to terminate a business relationship in case of high-risk or any other exposure
- Reviews regularly the criteria for high-risk business relationships and transactions
- Reviews the transaction monitoring performed by the first line of defense
- Coordinates and controls employee trainings on AML/CTF
- Monitors relevant regulatory changes in the areas of AML/CTF
- Supports the audit when reviewing the Company's activities in the areas of AML/CTF and implements feedback if any
- Directly liaise with and support of authorities in case of requests or investigations performed by authorities in the area of AML/CTF

The AML Officer role contains at least one senior executive with specific knowledge of the Company's exposure in the areas of AML/CTF and with sufficient seniority to identify the respective risks, adequately address them, take decisions and advocate for them.

The AML Officer has the resources, expertise, and access to all relevant information necessary to perform its duties appropriately and efficiently. The AML Officer reports directly to the EXCO on all AML/CTF related matters as well has a direct reporting line to the BoD.

The AML Officer shall in particular have the following rights:

- Entitlement to issue internal guidelines for AML/CTF matters

- Unimpeded access to all stored records at all times
- Reclassification of any customer relationship to a relationship with increased risks if appearing as appropriate
- Freezing assets if appearing as appropriate

9 Internal reporting

9.1 Ordinary reporting

The AML Officer reports to the Executive Committee on a semi-annually basis. In addition, an annual report forthe attention of the Executive Committee as well as to the Board of Directors is created.

9.2 Extraordinary reporting

All employees, as soon as they become aware of any breach of duties based on this policy, have the obligation to promptly inform their responsible superior (Executive Committee Member) or contact the AML Officer about the issue directly. Such reports are to be treated confidential and may also be made anonymously.

The Executive Committee Member immediately informs the AML Officer in case of significant changes of regulatory risks or violations of this policy in their area of responsibility.

10 Training

The AML Officer coordinates employee trainings regarding anti-money laundering and prevention of financing of terrorism as well as sanctions.

The AML Officer defines the functions within the Company, that are considered as exposed because of a close contact to Contracting Partner as well as their Assets with regards to the Regulations. For these functions, an annual training focused on anti-money laundering and counter terrorism financing as well as sanctions is undertaken.

The basic AML training for employees working in the AML sector takes place within 12 months after admission or joining the Company. After completion of the basic training, repetitions in form of advanced trainings shall take place every two years.

11 Exception to policy

The Company may decide to deviate from a provision outlined in this policy if:

- the provision is not a mandatory requirement according to Regulations ***and***
- the deviation does not expose the Company to disproportional risks

In order to deviate from a provision of this policy, a written preapproval of the AML Officer as well as of an Executive Committee Member is required. The approval has to be documented and the exception will be included in the regular reporting.

12 Updates of this policy

This policy shall be updated as often as required by the circumstances including when needed to reflect changes in applicable external regulation, sanctions and FATF opinions. The AML Officer proactively assists in the regulatory watch and necessary adjustments to the policy including to its appendices.

Appendices

The following appendices are integral part of this policy. They do not need an approval from the Executive Committee and can be adjusted by the AML Officer.

Appendix 1 Country Risk Categories
Appendix 2 Business sector Risk Categories
Appendix 3 Permissible and non-permissible FATF member states

Appendix 1 Country Risk Categories [last update: 02/2023]

For country risk categories the following lists are consulted:

- FATF lists “High Risk Jurisdictions subject to a Call for Action” and “Jurisdictions under Increased Monitoring”
- High-risk countries list (based on SECO sanctioned countries and best practice standards)

Customers with **domicile** or with current **business activity** in one of the following countries are excluded from the service of the Company. These countries are declared as **«non-serviced»** countries.

- Albania (2)
- Barbados (2)
- Belarus (2)
- Burkina Faso (2)
- Burundi (2)
- Cambodia (2)
- Central African Republic (2)
- Congo, Democratic Rep. (2)
- Democratic People's Republic of Korea (DPRK) (2)
- Guinea (2)
- Guinea Bissau (2)
- Haiti (2)
- Iran (2)
- Iraq (2)
- Jamaica (2)
- Jordan (2)
- Lebanon (2)
- Libya (2)
- Mali (2)
- Morocco (2)
- Mozambique (2)
- Myanmar (2)
- Nicaragua (2)
- Nigeria (2)
- Philippines (2)
- Russia (2)
- Senegal (2)
- Somalia (2)
- Sudan, Republic of South (2)
- Sudan (2)
- Syria (2)
- Tanzania (2)
- Uganda (2)
- Venezuela (2)
- Yemen (2)
- Zimbabwe (2)

Thereof countries accepted by the company and classified as high-risk (scoring: 2):

- Cayman Islands (2)
- Gibraltar (2)
- Panama (2)
- South Africa (2)
- Turkey (2)
- United Arab Emirates (2)

The following countries are classified as high-risk countries (scoring: 1):

- Afghanistan (1)
- Algeria (1)
- Angola (1)
- Anguilla (1)
- Antigua & Barbuda (1)
- Aruba (cfr NL) (1)
- Azerbaijan (1)
- Bahamas (1)
- Bahrain (1)
- Bangladesh (1)
- Belize (1)
- Benin (1)
- Bermuda (1)
- Bolivia (1)
- Bosnia and Herzegovina (1)
- Botswana (1)
- British Virgin Islands (1)
- Cameroon (1)
- Chad (1)
- China (1)
- Colombia (1)
- Comoros (1)
- Congo, Republic of (1)
- Côte d'Ivoire (1)
- Cuba (1)
- Curacao (cfr NL) (1)
- Cyprus (1)
- Delaware (1)
- Djibouti (1)
- Dominica (1)
- Dominican Republic (1)
- Ecuador (1)
- Equatorial Guinea (1)
- Eritrea (1)
- Ethiopia (1)
- Fiji (1)
- Gabon (1)
- Gambia (1)
- Ghana (1)
- Grenada (1)
- Guernsey (1)
- Guyana (1)
- Honduras (1)
- Hong Kong (1)
- Ireland (1)
- Isle of Men (1)
- Jersey (1)
- Kazakhstan (1)
- Kenya (1)
- Kiribati (1)
- Kosovo (1)
- Kyrgyzstan (1)
- Laos (1)
- Lesotho (1)
- Liberia (1)
- Macao (1)
- Madagascar (1)
- Maldives (1)
- Malta (1)
- Marshall Islands (1)
- Mauritania (1)
- Mauritius (1)
- Mexico (1)
- Miami (1)
- Micronesia (1)
- Monaco (1)
- Montserrat (1)
- Nauru (1)
- Nepal (1)
- Niue (1)
- Pakistan (1)
- Palau (1)
- Papua New Guinea (1)
- Paraguay (1)
- Peru (1)

- Puerto Rico (1)
- Rwanda (1)
- Saint Kitts and Nevis (1)
- Saint Lucia (1)
- Saint Vincent and the Grenadines (1)
- Sao Tome and Principe (1)
- Seychelles (1)
- Sierra Leone (1)
- Singapore (1)
- Solomon Islands (1)
- Suriname (1)
- Swaziland (1)
- Tajikistan (1)
- Timor-Leste (1)
- Togo (1)
- Tonga (1)
- Trinidad and Tobago (1)
- Turkmenistan (1)
- Turks & Caicos Islands (1)
- Tuvalu (1)
- Ukraine (1)
- Uzbekistan (1)
- Vanuatu (1)
- Viet Nam (1)
- Zambia (1)

Appendix 2 Business Sector Risk Categories [last update: 12/2022]

Customers active in one of the following business sectors are excluded from the service of the Company. These activities are declared as «non-serviced» business sectors.

- Military & arms (1)
- Exotic animals (1)

An activity or business qualifies as a high-risk if the respective sector of business activity involves (scoring 1):

- Adult Entertainment industry (1)
- Art & antiques (1)
- Charity, NGO & non-profit organizations (1)
- Commodities (1)
- Foreign exchanges (non-professional) (1)
- Gambling & sports (1)
- Money transfer agents (1)
- Politics & public administration (1)
- Precious stones & metals (1)

Where unclear, the AML Officer supports in determining whether a certain activity is deemed as high-risk.

Appendix 3 **Permissible FATF Member States for bank transfers in case of online identification** [last update: 02/2023]

- Australia
- Austria
- Belgium
- Brazil
- Canada
- France
- Germany
- Greece
- Hong Kong (China)
- Ireland
- Israel
- Italy
- Japan
- Korea (South)
- Luxembourg
- Malaysia
- Netherlands
- New Zealand
- Norway
- Portugal
- Saudi Arabia
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom
- USA

<u>Non-permissible</u> FATF Member States for bank transfer in case of online identification
[last update: 12/2022]

- Argentina
- Denmark
- China
- Finland
- Iceland
- India
- Mexico