KYC, AML/CTF and Sanctions Policy

Introduction

This is a short explanation of Ternion OU (Further on – Ternion) KYC, AML/CTF and Sanctions Policy (further on – the Policy), and describes, in general terms, the KYC, AML/CTF and Sanctions compliance Internal Control System (further on – ICS) of Ternion which is fully compliant to Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia (further on – the Law), applicable European Union Regulations, International Sanctions and best practices of AML/CTF industry. This public explanation of the Policy is developed in a describing way for the general public to understand why Ternion is asking certain questions and why Ternion will apply certain actions in certain conditions. Full Policy and ICS procedures are internal confidential documents of Ternion and are not disclosed to third parties (except in cases described in Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia) to prevent circumvention of the ICS and therefore put Ternion at risk to be involved in ML/TF and Sanction breaches.

Ternion, by holding licenses No. FVR000209 (Providing services of exchanging a virtual currency against a fiat currency) and No. FRK000174 (Providing a virtual currency wallet service) is an Obliged Entity in accordance to the Law.

General Provision

According to the Law, Ternion is entitled to ask additional questions and request to submit additional documentation at any point and based on any activity performed by the customer in cooperation with Ternion, if such information is necessary for Ternion to comply with the Law and determine if customer or its actions are related (or possibly could be related) to illicit activity, money laundering, terrorist financing and International Sanctions breach.

By entering into cooperation with Ternion, customer has the obligation to comply with internal regulations of Ternion that are built on the requirements of the Law and other related regulations.

If Ternion has determined that ML/TF or Sanction risk of a customer is too high or there is a suspicion that customer is related to or performs money laundering, terrorist financing, International Sanctions breaching or is/could be related to any other illicit activity or creates any other significant risks, Ternion has the right, at any point and without explanation, to terminate or refuse cooperation with the customer.

All the official correspondence and requests between a customer and Ternion, from customers' perspective, is performed in the Private cabinet of the Exchange (webpage my.ternion.exchange). All the provided information and documentation by the customer is legally binding and is customers' criminal responsibility to be complete and truthful.

Any customer, regardless of the applied risk level, based on certain actions or information, could trigger application of Enhanced Due Diligence that will be performed by Ternion on the customer during which additional questions will be asked and additional information and documents will be asked to submit and it is customers' obligation to submit it in the required time period.

It is customers' responsibility in timely manner to submit to Ternion any information that has changed from previously submitted (for example, changed name of the customer, changed passport, changed address, etc.). If Ternion will determine that sufficient information is lacking or is not submitted in timely manner (for example, new passport as previous has expired), Ternion has the right to restrict customers' activity or even terminate the cooperation with the customer.

It is an obligation of Ternion as Obliged Entity according to the Law in any case when there is a suspicion of ML/TF, International Sanctions breach or any other possible illicit activity to report about such events to the FIU. Conduct of such a report is strictly confidential and will not be disclosed to the customer except cases described in the Law. Ternion, according to the Law, is released from any liability for the losses created to the customer that arises from conducting such a report, even when the customer is proved not to be guilty.

It is important for customers to understand that if no illicit activity was performed or intended to be performed, there are no reasons to be worried that Ternion is asking questions about particular transactions or activity and the best is to fully cooperate, providing necessary answers and documentation as precisely and detailed as possible. Most of the times these are required checks by the Law and ICS rules and if no illicit activity was performed or intended to be performed, then full and honest cooperation will lead to faster investigation and end investigation with positive result for customer as soon as possible.

Onboarding and KYC

KYC (Know-Your-Customer) is a process of identifying and verifying the identity of a customer and assessing the potential AML/CTF (Anti Money Laundering / Counter Terrorist Financing) and Sanction risks that are associated with this customer by conducting business relationship.

By establishing business relationship with Ternion, customer will be required to undergo identification and verification of the natural person who is beneficiary of the registered account. In case of corporate customers, identification and verification will be performed not only on the legal person itself, but also on all the beneficial owners and representatives of this company.

During this so-called Onboarding process, customer will be asked to submit certain information and submit certain documentation, including photos of natural persons that are being identified. It is of utmost importance for customer to submit precise and only truthful information as even a smallest misinformation with illicit purposes will lead to refusal of account opening and this situation, in accordance to the Law, might be reported to the Financial Intelligence Unit of the Republic of Estonia (further on – FIU) as a suspicious activity. All the submitted information is cross-checked and verified in different databases to make sure that submitted documents are real, belongs to the natural person that is the beneficial owner of newly registered account, natural persons that are connected to the registered account are not designated by International Sanctions, Interpol and are not found in different lists of unwanted persons. Lists that Ternion screens against covers most of De jure globally acknowledged countries and their internal lists of persons with criminal background, wanted persons by police, tax avoiders, terrorists, etc., therefore Ternion is able to operate globally.

Ternion is providing full package of services only to those customers that are fully identified and verified according to the requirements of the Republic of Estonia and internal regulations of Ternion.

During the onboarding process or at any later point, according to the Law, Ternion has the right at any point ask customer additional questions and ask to submit additional documentation that could prove customer or its activity is not (or is) related to illicit activity, money laundering, terrorist financing or International Sanctions breach, but customer has the obligation to submit requested information and documentation within the term specified in the request.

If the customer does not submit requested information or documentation to Ternion within the term determined in the request, or Ternion has suspicions or it is acknowledged that submitted information or documentation is forged and does not correspond to the actual situation, or the customer is associated with money laundering, terrorism financing or International Sanctions breach, Ternion is entitled not to enter into business relationship with the customer and not to explain the reasons behind the refusal of cooperation. Moreover, according to the Law, in certain cases these situations will be reported to the FIU.

Ternion is entitled at any moment to change or additionally introduce new requirements for customers' identification and verification unilaterally at its discretion without customers' consent and prior notification. If necessary, Ternion takes measures to insure the receipt of additional identification information from the customer, as well as from publicly available reliable and independent resources and from other information sources that is provided to Ternion by different vendors.

Customer risk

Right after the Onboarding, if customer identification and verification was successful, Ternion, based on criteria described in internal documentation of ICS (a strictly confidential methodology), determines customer risk level (risk in terms of ML/TF and International Sanctions). Customer risk level is a dynamic parameter that changes based on changes in data or requirements. It is constantly calculated during the whole time of cooperation between Ternion and the customer.

If a customer will pass Onboarding (Identification and Verification) process successfully, but Ternion will calculate a risk level that is too high to continue the cooperation, Ternion will refuse the cooperation with the customer. The same principle applies to continuing the cooperation – if due to changed circumstances customer risk level becomes too high, Ternion will terminate the cooperation with particular customer.

All of the Ternion customer base is divided into risk groups where each risk group is applied with certain additional supervision requirements. If the risk group of the customer increases or is at certain high level already from the beginning of the cooperation, Ternion might ask such customer additional information and documentation on the source of the funds, particular fund flow, further destination of the funds, the reasons behind a certain activity, partners of the customer, etc. Customers have obligation to fully answer the questions and submit all the requested documentation within determined time.

Ternion, for customers with higher risk level, could apply additional cooperation requirements or restrictions to mitigate existing risks. Therefore, as certain restrictions could be applied (individually),

such customers might encounter with delays of order and transaction execution or receive requests before or after execution of transaction or orders.

Customer risk group also impacts when and how often Ternion will apply Due Diligence and Enhanced Due Diligence on the customer.

Ternion is required by the Law to identify and apply additional supervision requirements to Politically Exposed Persons (PEPs), family member of a PEP or a close associate of a PEP. Information on definition of mentioned persons can be found in the Law.

Ongoing customer monitoring

According to the Law, other related regulations and best practices, Ternion will perform ongoing customer monitoring during all the period of the cooperation between customer and Ternion.

Ongoing customer monitoring, depending on the customer risk level and other internal criteria, will include at least, but not limited to:

a) Monitoring of customers' transactions in all currencies based on pre-set scenarios and known information about customer and its economic activity;
b) Updating information available on the customer and making sure relevant data and documentation is up to date and truthful;
c) Identification of the source and origin of the funds used in transactions as well as destination of the funds;
d) Performing regular Due-diligences and Enhanced Due-diligences based on risk levels and other criteria;
e) Identifying potentially suspicious activity based on unusual patterns found manually and automatically using scenarios;
f) Evaluating involved jurisdictions in customers' activity;
g) Regular screening of all customers against changes in screening lists.

As a result of ongoing customer monitoring process, Ternion will ask customers additional questions and ask to submit additional documentation. This can result in delay of transactions and orders if customers will not submit requested information in timely manner or information will not be complete or truthful.

Transaction monitoring

Transaction monitoring is divided into two parts – online transaction monitoring and post-factum transaction monitoring. Online transaction monitoring is performed in real-time and is screening transactions against different lists and stops payments based on particular criteria. Post-factum transaction monitoring screens payments based on certain patterns and criteria that can not be determined in real-time.

Ternion will check all of customers' transaction as incoming, as outgoing in all available currencies and do analysis of currency combinations to determine suspicious transactions.

Ternion is using latest technological developments and most up-to-date intelligence covering virtual currency transactions, determining risk levels of transactions, determining illicit funds and illicit activities like purchases in “Dark-Web” and terrorist financing that is possible to determine due to technological development of block-chain technology.

Ternion will stop execution of certain transactions and ask questions to the customer regarding the transaction and will execute transaction only after all of the questions are answered in full and no suspicions of illicit activity will be present. Ternion has the right also to block account and freeze the funds of the customer in case of suspicious activity and keep the account and funds frozen until customer has answered on all of the questions and submitted required documents that proves customer to be innocent.

If Ternion will determine particular transaction as suspicious or unwelcome based on internal regulations, but there is no need to report such transaction to the FIU, transaction could be refused and returned to the originator. Possibly this scenario could lead to additional questions to the customer, applying restrictions to customers’ activity or even termination of business relationship between Ternion and the customer.

Third party fiat currency deposits and withdrawals are forbidden, therefore, any attempt to perform such activity (for example, deposit fiat currency funds from other persons bank account) will result in questions to customer and/or termination of cooperation with customer.

International Sanctions

Ternion, as Obliged Entity, must comply to the International Sanctions Act of the Republic of Estonia as well as Regulations of European Union and sanctions of United Nations. Ternion is intended to comply also with partner countries Sanction Acts, for example, OFAC sanctions of United States of America and others.

International Sanctions compliance is implemented in Ternion at all levels of ICS and it is not limited to only name screening, but compliance to sanctions is ensured in their full scope.

Ternion Onboarding process ensures that no person that is designated or could possibly create sanction risk can become a customer of Ternion. If Ternion customers will try to breach International Sanctions ar become designated persons during cooperation, it will be noticed during cooperation and live transaction performance using sophisticated technological solutions, available intelligence, automated scenarios and performed manual due-diligences.

Attempts to breach International Sanctions will result in serious consequences and freezing of the funds of involved customers.

Related documentation and regulation

For customers to fully understand requirements of AML/CTF and International Sanctions, Ternion advises customers to get acquainted with the following regulations and best practices:

1) Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia: https://www.riigiteataja.ee/en/eli/517112017003/consolide

2) International Sanctions Act of the Republic of Estonia: https://www.riigiteataja.ee/en/eli/503072014002/consolide

3) A review of EU implemented sanctions: https://sanctionsmap.eu/#/main

4) The FATF Recommendations: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html