

Guidelines on the Prevention of Money Laundering and Terrorism and Proliferation Financing and on Ensuring the Compliance with the Restrictions imposed by Sanctions in the Currency Cash Exchange Sector

To promote common understanding of the capital companies, having received Latvijas Banka's licence to perform currency cash exchange (hereinafter, capital companies), regarding their compliance with the requirements for the identification of suspicious transactions stipulated in the "Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing" (hereinafter, the Law), the Law on International Sanctions and National Sanctions of the Republic of Latvia (hereinafter, the Sanctions Law) and Latvijas Banka's Regulation No. 176 "Requirements for the Prevention of Money Laundering and Terrorism and Proliferation Financing and Sanctions Risk Management upon the Purchase and Sale of Cash in Foreign Currencies" of 16 July 2019, the Licensing Committee of Latvijas Banka has identified indications that may raise suspicions of money laundering, terrorism or proliferation financing, non-compliance with the restrictions imposed by sanctions or an attempt thereof when carrying out currency cash exchange transactions.

Money laundering refers to activities where proceeds of crime are channelled through the financial system so as to create an impression that they have come from legitimate sources.

Terrorism financing refers to collecting or transferring financial or any other assets, obtained by any means, directly or indirectly, with the intention of using them or in the knowledge that they will, in full or in part, be used for terrorist activities.

Proliferation financing refers to a set of activities aimed at concealing the origin of the funds and their end-user as well as the true nature of the transaction in order to finance the proliferation of weapons of mass destruction, inter alia obtain the necessary know-how and auxiliary materials.

In order to ensure the compliance with the restrictions imposed by sanctions, capital companies are obliged to identify the subjects of sanctions and to prevent non-compliance with the restrictions imposed on a person subject to sanctions, inter alia refuse to provide financial services to such persons, e.g. refuse to execute currency cash exchange transactions with such persons or persons acting in the name or on behalf of such persons. At the same time, circumvention of the imposed sanctions, inter alia by using other persons as a cover, shall be considered to be a criminal offence and shall also be established in the context of the prevention of money laundering.

I Proceeds of crime

According to the Criminal Law, proceeds of crime (criminally acquired property) are assets that have come into the ownership or possession of a person as a direct or indirect result of a criminal offence.

In addition to the proceeds of crime stipulated in the Criminal Law, funds owned or directly or indirectly controlled by the following persons shall also be deemed proceeds of crime:

- a person who is included on any list of persons suspected of being involved in terrorist activity or production, storage, transportation, use or distribution of weapons of mass destruction, compiled by states or international organisations stipulated by the Cabinet of Ministers;
- a person who is included on the list of subjects of sanctions drawn up by the Cabinet of Ministers on the basis of the Sanctions Law with a view to combatting the involvement in terrorist activity or production, storage, transportation, use or distribution of weapons of mass destruction;
- a person on whom bodies performing operational activities, pre-trial investigating institutions, the Office of the Prosecutor or a court have information which forms sufficient basis for suspecting this person of committing a criminal offence related to terrorism or participation therein.

According to the Law, the Financial Intelligence Unit of Latvia (hereinafter, the FIU) shall compile the information on the respective persons and publish it on the website <http://sankcijas.fid.gov.lv/>. The sanctions of the United Nations, those of the European Union as well as the national sanctions of the Republic of Latvia are listed on this website.

II Money laundering

Money laundering usually has three stages:

- the placement stage where cash or its equivalent is introduced into the financial system;
- the layering stage where several complex financial transactions are carried out to obscure the origin of funds;
- the integration stage where the funds are integrated back into the economy from what seem to be legitimate sources.

Such a simplified approach does not cover all money laundering techniques: depending on circumstances, one of the usual stages could also be omitted. Currency cash exchange is most likely to be part of the layering stage to disguise the origin of funds.

According to the Latvian National money laundering/terrorism financing risk assessment report, the level of threat to the currency cash exchange sector of being used in money laundering has been assessed as medium-high. In money laundering schemes, currency cash exchange requires no special planning, knowledge or expertise and is easily accessible. Hence, currency cash exchange can be used for money laundering in the following ways:

- by converting the currency obtained as income abroad from smuggling or selling excise goods;
- by converting less liquid currency, obtained as a result of non-identified criminal offences, to euro and US dollars which are internationally accepted currencies, including in Latvia;
- by converting the funds obtained as a result of non-identified criminal offences to high-denomination banknotes to facilitate the storage and transportation of the proceeds of crime;

- where criminal organisations and individual criminals gain influence in capital companies by purchasing their shares, becoming representatives of executive bodies or holding offices which may be used for money laundering and terrorism or proliferation financing.

III Terrorism financing

Unlike the funds used in money laundering, those used for terrorism financing may be originating from lawful sources. Therefore, it is also necessary to pay closer attention to the purpose and nature of a transaction, any additional information available in relation to that transaction as well as the potential future use of the funds.

Terrorism financing activities can be divided into three main stages: 1) obtaining, collecting and accumulating the funds; 2) transferring or shipping the funds to the end-user; 3) using the funds to purchase materials or reward terrorists.

The level of threat to the currency cash exchange sector of being used in terrorism financing has been assessed as medium-high. In terrorism financing schemes in Latvia, currency cash exchange is most likely to be employed at the second stage, i.e. when preparing for a transfer of funds to the end-user or intermediary or when carrying out such a transfer. The level of threat is mainly dependent on the share of anonymous transactions and the fact that currency cash exchange requires no special planning, knowledge or expertise and is easily accessible. Hence, the currency cash exchange can be used for terrorism financing in the following ways:

- by converting the funds to US dollars which is an internationally accepted currency and allows the execution of payments in any country, including in countries with high terrorist activity; US dollars are usually transported to conflict areas to finance terrorist activities;
- by converting the funds to another currency in high-denomination banknotes to facilitate the storage of funds and their transportation to conflict areas to finance terrorist activities;
- by converting the funds to the national currencies of the countries neighbouring those with high risk of terrorism financing.

IV Proliferation financing

Funds for proliferation financing can come from various sources, e.g. from a country subject to sanctions, directly or indirectly, from a company supporting proliferation or from proceeds of crime. In order to successfully purchase weapons of mass destruction, inter alia carry out their transportation and any other activities, it is necessary to hide or obscure the origin of funds irrespective of their source by involving e.g. shell companies, agents and other intermediaries, so as to distance the beneficial owner involved in the transaction from the transaction as much as possible.

At the stage of obscuring the origin of funds, currency cash exchange may also be used as an element or instrument in a particular transaction to ensure additional anonymity by using cash.

V Identification of the beneficial owner within the framework of customer due diligence

According to the Law, the beneficial owner is a natural person who is the owner of the customer – legal person – or who controls the customer, or on whose behalf, for whose benefit or in whose interests business relationship is being established or an individual transaction is being executed, and it is at least:

- as regards legal persons – a natural person who owns, in the form of direct or indirect shareholding, more than 25 per cent of the capital shares or voting stock of the legal person or who directly or indirectly controls it;
- as regards legal arrangements – a natural person who owns or in whose interests a legal arrangement has been established or operates, or who directly or indirectly exercises control over it, inter alia who is the founder, proxy or supervisor (manager) of such legal arrangement.

The Law lays down an obligation for capital companies to obtain information on the beneficial owners of their customers. When identifying the beneficial owner, the following information shall be obtained:

- personal identity information;
- information about the nationality and country of residence of the natural person;
- information about the type of control exercised by the natural person over the customer:
 - i. in case of a legal entity: information about the amount of the legal entity's capital shares or stock controlled by the natural person;
 - ii. in case of a legal arrangement: information about its mechanism of governance and the natural person's role in its operation.

A capital company can identify the beneficial owner of the customer in at least one of the following ways:

- by obtaining a statement, approved by the customer, on the beneficial owner;
- by using information or documents from the information systems of the Republic of Latvia or a foreign country (e.g. the information published in the database of the State Revenue Service, the Enterprise Register of the Republic of Latvia, the State Unified Computerised Land Register and other sources), documenting the used source of information and the information obtained from it;
- by identifying the beneficial owner of the customer independently, where it is impossible to obtain the information in any other way.

Where a capital company has employed all possible means of identifying the beneficial owner and has established that it is impossible to identify any natural person that would correspond to the clarification of the term "beneficial owner" provided for in the Law and any doubts that the legal person may have another beneficial owner have been ruled out, the capital company, by appropriately justifying and documenting the activities carried out to identify the beneficial owner of the customer, can establish that the beneficial owner of the legal person is the person holding a position in the highest management body of the legal person.

Based on the risk assessment, a capital company shall take the necessary measures to verify whether the identified beneficial owner is the actual beneficial owner of the customer.

When verifying the beneficial owner, the capital company shall take into account the potential risk factors which may point to the provision of incorrect information. For instance, the capital company shall verify whether the profile of the identified beneficial owner is consistent with that of an individual able to manage a business or be its beneficial owner, since individuals with no fixed addresses or individuals from non-cooperative jurisdictions for the purposes of exchanging legal information with the Republic of Latvia may also be indicated as beneficial owners.

The capital company should note that individuals attempting to launder money are seeking to obscure their activities under the cover of various natural and legal persons or legal arrangements, e.g. by establishing non-profit charity foundations, associations and endowments.

VI Identification of suspicious transactions and their reporting

To ensure effective prevention of money laundering and terrorism and proliferation financing, a capital company shall have an ongoing obligation to assess each discussed, planned, submitted, initiated, postponed, executed or confirmed transaction with regard to its possible association with money laundering and terrorism and proliferation financing, and to immediately report each such suspicious transaction to the FIU.

With regard to its internal control system, a capital company shall lay down and document the following:

- procedure for identification of suspicious transactions;
- procedure under which the capital company reports suspicious transactions to the FIU;

Upon identification of a suspicious transaction, it shall be reported to the FIU immediately in electronic form via the FIU's website <https://goaml.fid.gov.lv>

Explanatory notes on the submission of reports, including their technical schemes and various classifiers are also available on the FIU's website <https://www.fid.gov.lv> (the section "E-reporting"). In addition to the above, the FIU informs the users registered on the website <https://goaml.fid.gov.lv>, on a regular basis, about the latest developments, inter alia the latest typologies.

A capital company shall have no right to disclose the fact of reporting; therefore, the circulation of documents shall be organised so as to ensure that the information is not disclosed to the customer and third parties, inter alia, the employees of the capital company who do not need the information to perform their work duties.

The procedure for identification of suspicious transactions establishes signs and indications which may give rise to suspicion with respect to a transaction, as well as lays down the analysis and due diligence processes for the examination of the circumstances of the transaction, inter alia the previous transactions, the customer and any other information necessary to verify the suspiciousness of a transaction.

Reporting a suspicious transaction shall not exempt a capital company from submitting a threshold declaration. In the same way, submitting a threshold declaration shall not

exempt a capital company from the obligation to assess each discussed, planned, submitted, initiated, postponed, executed or confirmed transaction with regard to its possible association with money laundering and terrorism and proliferation financing.

VII Threshold declarations

According to the Law and the Cabinet of Ministers regulations adopted on the basis of the said Law, the subjects of the Law are obliged to submit threshold declarations to the FIU. Threshold declarations shall be submitted via the FIU's website <https://goaml.fid.gov.lv> once a week on the transactions executed in the respective period.

Threshold declarations shall be submitted on any transaction whose amount corresponds to the threshold amount stipulated by the respective Cabinet of Ministers regulations. Threshold declarations require no transaction analysis, and they shall include only a limited amount of information. As indicated in the previous section, the submission of a threshold declaration shall not exempt a capital company from the obligation to identify suspicious transactions and report them to the FIU. Thus, it is possible that a capital company reports one transaction to the FIU twice, i.e. when submitting a threshold declaration and when reporting a suspicious transaction.

VIII Refraining from executing a suspicious transaction

Given that currency exchange is a service that is normally executed immediately, a capital company shall refrain from providing the service to a customer where there are reasonable grounds to suspect that the transaction is related to money laundering or terrorism and proliferation financing. A capital company shall immediately report such cases to the FIU as suspicious transactions.

If a capital company executes a currency cash exchange transaction where the transaction is completed some time after the receipt of the payment, in addition to the obligation to identify and report suspicious transactions and in conformity with the requirements of the Law, the capital company shall also lay down a procedure in its internal control system for refraining from executing a transaction where there are reasonable grounds to suspect that the transaction is related to money laundering or terrorism financing. A capital company shall, without delay but no later than on the following business day, report to the FIU that it has refrained from executing such a transaction.

- In such cases, the FIU shall assess the received report within five or, where necessary, eight business days. Within this time period, the capital company shall receive an order from the FIU:
- to discontinue refraining from executing the transaction or
- to freeze the funds where there are reasonable grounds to suspect that a criminal offence is being committed or has been committed, including money laundering, terrorism or proliferation financing or an attempt thereof.

Where refraining from executing a transaction or refusing to execute a transaction may alert the customer so that he/she can attempt to avoid liability, the execution of the

transaction is permitted. At the same time, the capital company shall, without delay but no later than on the following business day, report the suspicious transaction to the FIU.

IX Typologies of possible criminal offences

Within the meaning of the prevention of money laundering, typologies are the most common types and mechanisms of money laundering. Since criminals use innovative money laundering methods, certain typologies may differ depending on the region where and the particular time period when they are used, i.e. non-current typologies may become current and vice-versa. New market mechanisms are always subject to high risk, since supervisory mechanisms for preventing money laundering are not always developed for such markets.

The current typologies of criminal offences are as follows (non-exhaustive list):

- evasion of taxes and payments equivalent thereto;
- fraud in e-environment;
- fraud related to non-bank loans;
- financial pyramid scheme;
- unregistered or unlicensed commercial activity;
- fraud related to receiving public financing;
- criminal offence involving a politically exposed person;
- criminal offence while performing duties of a public official;
- corrupt practices;
- use of counterfeit documents;
- fraud in insolvency proceedings;
- other types of fraud;
- terrorism financing;
- financing of the production, storage, transportation, use and distribution (proliferation) of weapons of mass destruction;
- laundering of money of unknown origin.

X Suspicious transaction indications (risk identifiers)

In addition to typologies, indications (risk identifiers) may be determined to identify or help to identify suspicious transactions.

Latvijas Banka has identified and draws the capital companies' attention to the following most common indications of suspicious currency cash exchange transactions and their risk identifiers:

- customer identification problems (the customer is unwilling to provide the identification data or provides minimal or fictitious information, or information that is difficult to verify, or there are reasonable grounds to suspect that the personal identification document is a counterfeit);
- the customer is nervous for no apparent reason;
- the customer is accompanied by other persons observing him/her;
- the customer brings money which he/she has not counted;
- the customer is asking about the threshold for identification and due diligence or their procedures;

- the customer performs several similar low-value transactions below the threshold from which a capital company initiates customer due diligence, suggesting that this is done deliberately to avoid potential identification;
- several customers perform consecutive similar transactions below the threshold from which a capital company initiates customer due diligence, suggesting that this is done deliberately to avoid potential identification;
- the customer performs transactions in several currency exchange offices within a short period of time;
- the customer performs a large-value transaction with rarely used currencies;
- the customer performs a complex transaction (i.e. the transaction has no clear economic or legal purpose), including the exchange of currencies;
- the customer performs a transaction that is atypical of this customer, i.e. a transaction that is unusually large for this customer;
- the customer performs a transaction that is atypical of his/her residence or destination country;
- the origin of the funds used in the transaction is unclear;
- the customer performs a transaction, and its value is inconsistent with the customer's financial situation;
- the transaction is related to another suspicious transaction which has already been reported by the capital company to the FIU;
- there are reasonable grounds to suspect that a counterfeit document has been used in the transaction;
- high-denomination banknotes have been used in the transaction;
- the banknote denominations are atypical of the customer;
- the banknote packaging is atypical of the customer.

Indications of suspicious currency cash exchange transactions and their risk identifiers may imply that the customer operates with funds derived from an illegal source or having an illegal purpose of use, i.e. one of the typologies of criminal offences might apply to the customer or the funds involved in the transaction.

Therefore, the obligation to perform customer due diligence to obtain the information on the customer and the funds involved in the transaction is of great importance.

Considering that cash circulation is associated with higher money laundering risk, the legislator has established that a capital company is obliged to perform customer due diligence upon executing each currency cash exchange transaction where the amount of the transaction or the total amount of several seemingly related transactions exceeds 1500 euro.

The threshold amount stipulated by the Law whereby a capital company is obliged to perform customer due diligence constitutes an obstacle for persons who may be interested in using capital companies for the purposes associated with money laundering or terrorism and proliferation financing; therefore, the aggregate risk of capital companies being involved in money laundering or terrorism and proliferation financing activities is not particularly high. However, the risk is still relevant, and it is

the process of customer due diligence and supervision of the transactions executed by customers (provided that it is implemented in a targeted manner to prevent the risks of money laundering or terrorism and proliferation financing) that helps capital companies not to get involved in illegal activities.

XI Compliance with the Sanctions Law

In Latvia, the Sanctions Law is binding on all persons, including capital companies. The purpose of the Law is to ensure peace, security and justice in line with Latvia's international obligations and national interests by implementing the international sanctions and establishing the national sanctions.

As already mentioned in the previous sections, according to the requirements of the Law, the funds owned or directly or indirectly controlled by a person included in one of the lists of subjects of sanctions compiled by states or international organisations stipulated by the Cabinet of Ministers or drawn up by the Cabinet of Ministers on the basis of the Sanctions Law with a view to combatting the involvement in terrorist activity or production, storage, transportation, use or distribution of weapons of mass destruction, shall be deemed the proceeds of crime. Essentially, such persons are subject to both the requirements of the Law and those of the Sanctions Law. At the same time, it should be taken into account that the Sanctions Law covers a much wider range of sanctions and, thus, persons subject to sanctions. It is therefore important to be aware of the different procedures that may be applied to the persons subject to sanctions.

Even though the Sanctions Law stipulates various possible restrictions, the primary obligation of capital companies is to identify and comply with the financial restrictions established with regard to the subject of sanctions. Upon identifying such restrictions, a capital company is obliged to ensure the following:

- deny access to funds and financial instruments to the subject of sanctions;
- refuse to provide the financial services specified in the international or national sanctions to the subject of sanctions;
- where a capital company manages the funds of the customer, freeze all funds and financial instruments owned, managed or controlled by the subject of sanctions.

To ensure compliance with the Sanctions Law, the updated list of sanctions shall be checked before executing a transaction. When cooperating with a legal person or arrangement, it is also important to identify its beneficial owners, since its beneficial owner may be sanctioned even if the legal person or arrangement itself is not subject to any sanctions; consequently, the sanctions most likely also apply to the legal person or arrangement.

In addition to the above, capital companies are also obliged to observe targeted sanctions which do not apply to a particular person but rather a particular sector or activity, e.g. restrictions on providing tourism services in Crimea or restrictions on exports of various products to countries outside the European Union.

Useful links:

Useful information and methodological materials on the prevention of money laundering and terrorism financing: <https://www.fid.gov.lv/en>

International organisation (FATF): <http://www.fatf-gafi.org/>

High-risk jurisdictions

When assessing the risk of the customer, the risk level of the customer's jurisdiction shall be taken into account. Information on the high-risk jurisdictions identified by the FATF and the EU is available on the FIU's website: [Augsta riska valstis | Finanšu izlūkošanas dienests \(fid.gov.lv\)](#)

Basel AML Index: <https://www.baselgovernance.org/basel-aml-index>

Corruption Perceptions Index: <https://www.transparency.org/en/cpi>

Explanation of the "grey list" and jurisdictions included therein:

<https://lvportals.lv/skaidrojumi/313364-kas-ir-pelekais-saraksts-un-kadas-valstis-taja-ieklaudas-2020>