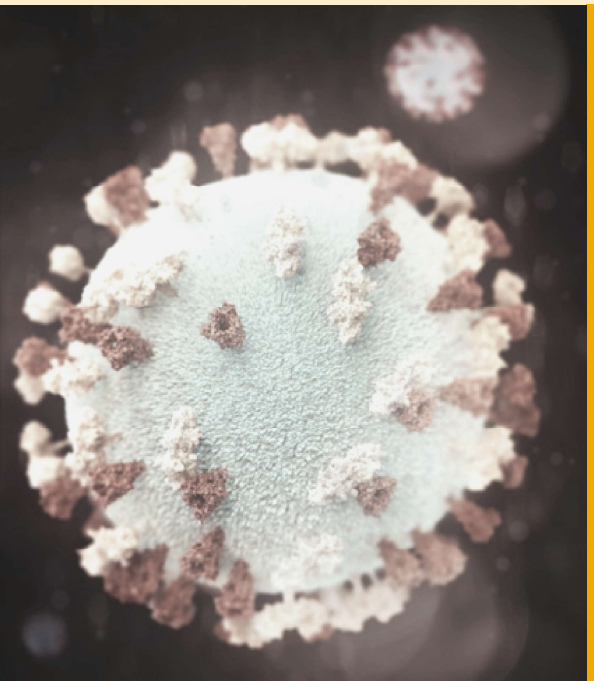
Financial Intelligence Unit

INFORMATIVE MATERIAL

MONEY LAUNDERING AND TERRORISM FINANCING RISKS CAUSED BY COVID-19



MAY 2020

INTRODUCTION

Covid-19, hereinafter – Covid, pandemic is a global crisis where everyone, including the financial sector, needs to respond quickly and effectively to established constraints and market conditions, which can also have a significant impact on the implementation of measures regarding anti-money laundering, hereinafter – ML, and counter terrorism financing, hereinafter - TF. During the Covid crisis, measures to prevent ML and TF remain a high priority, in order to mitigate the use of Latvian financial and non-financial sector for ML and TF activities.

In this material, the Financial Intelligence Unit of Latvia has compiled up-to-date information and trends on the ML and TF risks caused by the Covid crisis and the state of emergency, uniting information provided by international organizations, incl. information published by the Financial Action Task Force (FATF), cooperation partners and analogous foreign institutions, as well as information held by the Financial Intelligence Unit of Latvia. It should be noted that the global health and economic crisis is currently in its initial phase, therefore the identification of specific ML and TF trends and typologies is also at an early stage. In this material, the ML and TF risk profile is based on the following general assumptions:

- Governments, legal and natural persons are increasingly turning to online systems to enable remote work and social interaction.
- Activity of businesses that are classified as non-essential is limited as well as provision of on-site client services is restricted, therefore both essential and non-essential business are seeing increased online sales.
- In order to reduce the negative impact of the state emergency and Covid restrictive measures on the development of the Latvian economy, a number of support measures have been implemented in various areas.

- The Latvian government has determined sectors where the financial situation has significantly deteriorated due to the spread of Covid* as well as procedure by which the measures specified in the regulatory framework and special support mechanisms for the representatives of the sector affected by the crisis are applicable.**

- The Covid pandemic has driven significant demand for medical supplies, such as personal protective equipment and medicine and a national and global shortage of such goods can be identified due to the overwhelming demand.

- Banks and financial institutions remain in operation with some offering more limited services and restricting provision of on-site services.

- The closure of many businesses and other restrictions on trade and travel has led to mass unemployment, restructuration of state resources and a general economic recession that will impact the financial and social behaviour of businesses and individuals.

*Regulations Regarding the Sectors where the Financial Situation has Significantly Deteriorated due to the Spread of COVID-19. Available: https://likumi.lv/ta/en/en/id/313428-regulations-regarding-the-sectors where-the-financial-situation-has-significantly-deteriorated-due-to-the-spread-of-covid-19

**The Law on Measures for the Prevention and Suppression of Threat to the State and Its Consequences Due to the Spread of COVID-19. Available: https://likumi.lv/ta/en/en/id/313373-on-measures-for-the-prevention-and-suppression-of-threat-to-the-state-and-its-consequences-due-to-the-spread-of-covid-19

04

ML RISKS

The Covid pandemic has led to significant demand for medical supplies for Covid prevention. Due to the significant demand shortage of such products has been identified, as well as inadequate price and often critically low quality of delivered or offered goods. In the view of the previously mentioned, the government, in response to the Covid pandemic and its consequences, has decided to reduce the regulatory requirements in the field of public procurement, i.e. the regulation stipulates that certain entities - state capital companies, inpatient medical treatment institutions and other services and institutions are allowed not to apply the requirements specified in the Public Procurement Law when purchasing goods and services necessary for the restriction of Covid.*

In addition to the above mentioned facilitations, the government has also provided variety of other support measures, incl. social assistance and tax relief initiatives, downtime benefits and others.

Although described support mechanisms have been implemented to mitigate and address the consequences of the Covid crisis, they may create new ML opportunities.

Based on the ML risks identified by international experts and the Financial Intelligence Unit of Latvia in the context of the Covid crisis, as well as the suspicious transaction reports received, predicate offenses have been identified significantly more frequently than stand-alone ML cases.

Cabinet of Ministers Regulation No. 103 "Regarding Declaration of the Emergency Situation". Available: https://likumi.lv/ta/en/en/id/313191-regarding-declaration-of-the-emergency-situation

1.1. Fraud

Information published by the FATF, information available to the Financial Intelligence Unit of Latvia, as well as received suspicious transactions reports indicate that criminals have attempted to profit from the Covid pandemic through increased fraudulent activities. The primary fraudulent activities include:

1.1.1. Impersonation of officials.

In such cases, criminals contact individuals (email or telephone) and impersonate government officials with the intent of obtaining personal banking information or cash, using the support mechanisms implemented by the government as a justification.

1.1.2. Counterfeiting, including essential goods (such as medical supplies and medicines).

Given the high demand, there is a significant increase in online scams involving certain medical supplies, personal protective equipment and pharmaceutical products. In such cases, the suspects claim to be employees of businesses, charities, and international organisations offering medical supplies and requesting prepayment, however, the goods are never delivered or the quality of goods delivered is critically low.

1.1.3. Fundraising for fake charities.

Information published by international experts confirms an increase in fundraising scams. In such cases, criminals posing as international organisations or charities circulate e-mails requesting donations for campaigns to eliminate consequences caused by Covid. Recipients of these emails are then directed to provide credit card information or make payments through the suspect's secure digital wallet.

1.1.4. Intentionally driving a legal person to insolvency.

Taking into account the support mechanisms introduced by the government for entrepreneurs in order to reduce the negative impact of the state emergency and Covid restrictive measures on the development of the Latvian economy, incl. tax relief, bank holiday guarantees and working capital loans and other support measures, there is a risk of an increase in the number of cases where businesses are intentionally driven to insolvency in order to avoid liability or withdraw funds for private use.

1.2. Cybercrime

There has been a sharp rise in cybercrimes, specifically phishing email* and mobile messages through spam campaigns. These attacks use links to fraudulent websites or malicious attachments to collect personal payment information.

It is important to note that various cybercrime methods are used, incl. cybercrime being adapted to the specific technologies of remote work, as well as to the conditions and infrastructure management of remote work, which can be explained by the large number of persons working from home.

*Phishing email or spam – a mass e-mail message in which criminals try to obtain personal data and other information using various social engineering techniques in order to access accounts or bank card numbers.

1.2.1. Phishing e-mails and mobile messages.

The information available to the Financial Intelligence Unit of Latvia suggests that criminals are exploiting public concerns about the Covid crisis to insert malware on computers or mobile devices.

FATF has provided an example where cyber-criminals posed themselves as the World Health Organization and sent e-mails and mobile messages to lure individuals into clicking malicious links or opening attachments, which subsequently reveal the individual's username and password. Reports of harmful e-mails on behalf of the World Health Organization has been received also in Latvia. In such cases an attachment is added to the e-mail, which is supposed to provide up-to-date information and recommendations on how to fight Covid. The attachment may contain malware that steals sensitive information, or an encryption squeeze virus that encrypts device data.

The State Revenue Service has received information that some users of the social network "draugiem.lv" have received letters on behalf of the State Revenue Service inviting them to send a text message in order to receive further information on the possibilities to receive financial support. The State Revenue Service via official social media platforms has urged citizens to be careful and not respond to false statements.

1.2.2. Business e-mail compromise scams.

Due to a sharp rise in global remote work, cyber-criminals are also exploiting weaknesses in businesses' network security to gain access to customer contact and transaction information. This information is later used in targeted phishing e-mails whereby the criminals pose as cooperation partners and request payment for goods and/or services but instead direct this payment into their private accounts.

It is important to point out when working remotely, attention should be paid to calls where the caller claims to be a representative of the company's IT department, where the recipient of the call works (or represents the company's IT outsourcing), indicating the need for a security check.

1.3. Other predicate offences

1.3.1. Human trafficking and exploitation of workers.

Information published by the international organizations indicate that criminals may take advantage of the pandemic to exploit vulnerable groups that may lead to an increase in the exploitation of workers and human trafficking. The suspension or reduced activity of government agencies regularly engaged in detecting human trafficking cases and identifying victims of trafficking means that cases may go undetected. Human exploitation could increase from the following factors: the shutdown of workplaces (rising unemployment), slowdown in the economy, and financial insecurity.

1.3.2. Online child exploitation.

With the closure of schools, children are increasingly using the internet during “lockdown” periods, which could lead to an increase in online child exploitation. International organisations have reported that a rise in the production and distribution of online child exploitation can be identified, often for profit.

09

PUBLIC PROCUREMENT

Considering the growing demand for medical supplies and sudden inadequate price rise, which has significantly increased the number of illegal service providers trying to abuse the situation, as well as reduced regulatory requirements, new offences in public procurement have been identified within both - national and international levels.

The case of surgical masks and respirators purchase from China has already been reflected in media statements. The agreement was concluded in accordance with the Cabinet of Ministers regulation mentioned before which allowed to execute the purchase of medical supplies without applying the requirements of the Public Procurement Law. Later, when the first delivery of goods was received, a number of the certificate attached to the contract was found to be non-existent, invalid or forged, and it was identified that the laboratory that issued the certificate is not on China's official list of accredited mask testing laboratories.

The Financial Intelligence Unit of Latvia has also received and is processing a number of reports on possible ML cases in connection with the supply of disposable medical masks to medical institutions during the emergency situation. Verification of the source of funds for the purchase of disposable medical masks and the official’s connection to possible ML is required.

The Financial Intelligence Unit of Latvia points out that public procurement that is performed without applying the requirements specified in the Public Procurement Law should be subject to additional control and supervision to ensure that the funds are used economically and purposefully, as well as to assess the persons (companies) to whom the funds are transferred, inter alia, assessing the compliance to sanctions.

CUSTOMER DUE DILIGENCE REQUIREMENTS

International practice indicates that criminals are finding ways to bypass customer due diligence measures in order to conceal and launder funds, using challenges in internal controls caused by remote working situations. It is also important to note that it is strictly forbidden to rely on customer requests for reduced customer due diligence requirements based on the severe effects of the Covid crisis.

In order to promote customer due diligence during this challenging time, it is important to point out that digital identity verification and the use of other secure and innovative solutions to ensure customer identification when entering into a business relationship or transaction do not always involve an increased level of risk – remote identification may have an even lower risk than on-site identification.

The Financial Intelligence Unit of Latvia draws attention to the fact that in the current situation it is necessary to ensure full use and compliance with the risk-based approach and customer due diligence requirements, ensuring that supervisory measures laid down in the regulatory framework are proportionate to the level and nature of risks identified. At this challenging time, it is important to make full use of existing opportunities that provide the necessary flexibility while maintaining effectiveness in the fight against ML and TF.

REVISING ENTITY-WIDE RISK ASSESSMENTS AND INTERNAL CONTROL SYSTEMS

Obliged entities under the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing, hereinafter – AML/CFT/CFP Law, should consider whether and to what extent criminals may misuse the services and service delivery channels they offer to implement ML and TF activities, inter alia, taking into account threats specified in this informative material.

Entity-wide risk assessment is a dynamic tool that needs to be complemented in response to change, and current circumstances call for a review of these risk assessments, adapting internal control systems and customer due diligence measures in line with ML and TF risks identified caused by Covid.

Although the Covid crisis has led to a particular decline in demand for goods and services in certain sectors, the government has provided support measures and mechanisms to overcome the crisis, namely legitimate ways to overcome the difficulties encountered. Therefore also during the Covid crisis special attention should be paid to customer that potentially might exploit obliged entities under the AML/CFT/CFP Law for ML and TF activities, as well as suspicious or inadequately tempting offers of cooperation should be avoided.

USE OF KEY WORDS AND FUZZY LOGIC

Financial institutions use various tools and methods to monitor the performed transactions to ensure the compliance with the requirements laid down in the regulatory framework, incl. keyword monitoring based on the automatic search for relevant keywords related to criminal activity, however this method is not always completely secure. In many instances also Fuzzy logic is applied. This is a method in which, in addition to logical and grammatically correct keywords, similar words are searched, e.g. words with changed letters or related keywords, which greatly expands the chances of identifying suspicious transactions.

Examples of keywords to look for in Covid related transactions using the fuzzy logic method:

medical, mask, equipment, pill, vaccine, medicine, anti-bacterial, anti-cough, face cover, face-mask, chemical, ventilator, sanitary, hospital, test-kit, Covid-test, Covid-suit, respirator, protection, face-shield, gloves, hygiene, protective goggles, first-aid-kit, hand-sanitizer, sanitizer-gel, etc.*

International practice shows the effectiveness of the application of fuzzy logic in the identification of ML cases. This method allows to identify suspicious transactions comprehensively, especially in the current situation where financial institutions might be used to carry out ML activities, using the Covid crisis as a cover.

*The examples listed are not an exhaustive list oF keywords.

TF RISKS

The United Nations has warned that threats related to TF remain and that terrorist groups may see opportunities for increased TF activities while governments' attention is focused on dealing with the consequences of the Covid crisis.*

International organisations have raised concerns about terrorist groups using the Covid crisis to raise and move funds, and increasing existing illicit activity to finance their operations. As international humanitarian and aid responses to Covid increase, there is a risk of funds being diverted to support terrorists and terrorist groups. The Financial Intelligence Unit of Latvia does not currently have information on the TF risks caused by the Covid crisis in Latvia, but it is important to point out that the situation is changing and the identification of specific TF trends and typologies caused by the Covid crisis is still at an early stage.

*United Nations Secretary-General. 2020. Secretary-General's Remarks to the Security Council on the COVID_19 Pandemic. Available: https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered

SUMMARY

In summarizing the information available to international organizations and cooperation partners, as well as publicly available information and information held by the Financial Intelligence Unit of Latvia, the following potential ML and TF risks related to the circumstances caused by the Covid crisis have been identified and the following suggestions made.

1.Criminals finding ways to bypass customer due diligence measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds.

2.Increased misuse of online financial services and virtual assets to move and conceal illicit funds.

3.Misuse of financial aid and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds.

4.Wider use of the unregulated financial sector, given that money may be transferred from the banking system due to financial instability, which in turn may create additional opportunities for criminals to carry out ML activities.

5.Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent ML risks.

6.Ensure full use and compliance with the risk-based approach and customer due diligence requirements, ensuring that supervisory measures laid down in the regulatory framework are proportionate to the level and nature of risks identified.

7.Ensure keyword monitoring or automatic search, which provides opportunities to identify suspicious transactions related to the circumstances caused by the Covid crisis.

8.Ensure the review and adjustment of entity-wide risk assessments of obliged entities under the AML/CFT/CFP Law in line with the circumstances created by the Covid crisis.

IMPACT

The Financial Intelligence Unit of Latvia points out that the impact of the Covid crisis on the prevention of ML and TF can be divided into three phases:

01

IMMEDIATE IMPACT

Immediate impact can be seen in the various predicate offenses, such as cybercrime, counterfeiting and trafficking in non-standard goods, as well as the implementation of various fraud schemes. The Covid pandemic can be used as a tool and a cover for these predicate crimes, especially as criminals have rapidly adapted and developed methods to use the crisis conditions created by Covid to carry out criminal activities.

02

MID-TERM IMPACT

For example, cybercrime and online child abuse are those crimes that will continue to spread after the end of the Covid crisis and its aftermath. Restrictions on socialization have created new habits in society regarding the use of the virtual environment, which have led to reliance and trust in digital services and the environment in general.

The economic crisis caused by the Covid pandemic is also likely to have a significant impact on the financial system, especially in the banking sector. Responsible authorities regarding prevention of ML and obliged entities under the AML/CFT/CFP Law must be vigilant and take into Account the attempts of criminals to use the fragile situation to carry out ML activities.

03

LONG-TERM IMPACT

While the previous economic crisis confirmed cash as the preferred medium for criminal transactions, this may be different in the wake of the Covid pandemic as cashless payment options are becoming increasingly prevalent and online payment options including cryptocurrencies are increasingly accessible to all users.

Economic difficulties in society create a tendency to accept and be more open to various offers, incl. engage in questionable transactions, be recruited for criminal activities, etc.

It is also important to note that the long-term impact of the Covid pandemic may be particularly significant in the area of economic and financial crime, incl. increase in the number of ML cases, increase in the level of corruption, etc.