Consequences of the COVID-19 crisis on money laundering – 2

On 6 April 2020, CTIF-CFI published a first document on its website to warn obliged entities about the immediate consequences of the COVID-19 crisis on money laundering. It mainly focussed on the short-term consequences of the health crisis, mostly related to fraud with the sale of protective equipment.

Now the health crisis seems to gradually get under control the social and economic consequences are becoming clearer. The current economic crisis and the ensuing social changes give criminal organisations the chance to take advantage of the extreme circumstances and adapt their existing modi operandi or develop new criminal activities.

CTIF-CFI's second document is aimed at raising awareness of obliged entities on the possible medium-term effects of the changed economic situation on money laundering. Rather than listing concrete indicators the aim is to reflect on the possible evolution of predicate offences in order to detect related financial transactions. Based on disclosures received, the current analysis can be adjusted, fine-tuned or enhanced. The predicate offences listed below are those that could be most affected by the economic crisis or that will have the greatest impact on money laundering. The information is based on the analysis of our files, open sources and studies by a number of national and international partners and organisations.

1. Cybercrime

In addition to computer crime linked to fraud with COVID-19 material, which was discussed in the warning of 6 April, several other types of cybercrime also pose an increased risk due to the current situation.

Incidents of companies and institutions being extorted when their IT networks are brought to a standstill could rise sharply in current circumstances. Organisations have introduced large-scale telework and were relatively unprepared. Access to the company network, often through employees' own hardware, is vulnerable to attacks by cybercriminals. By using this access they can bring the IT system of the entire organisation to a standstill and then ask for a ransom to unblock the system.

As the amounts that need to be paid are usually proportional to the lost income or the damage sustained when the infrastructure is down, companies that have suffered such an attack are sometimes inclined to pay the ransom.

These "ransomware" attacks can now also target critical sectors such as hospitals, research centres or companies that play a crucial role in the food supply chain, resulting in a very high social cost.

Several banks have also reported a rise in the number of phishing messages. Cybercriminals use phishing to obtain customers' banking codes, usual by emailing a link to a fake website of the bank. As an increasing number of bank branches have closed down, customers who belong to vulnerable groups can only use online banking, with which they are less familiar.

Cybercriminals also use the COVID-19 crisis as a pretext in their phishing emails. These emails are allegedly from a financial institution and customers are asked to update security information, supposedly due to the exceptional circumstances.

The financial transactions linked to cybercrime are diverse and are not always easy to detect:

- ***In case of extortion involving ransomware, victims are often asked to pay in virtual currencies and the money is subsequently transferred to accounts abroad. The amounts generally range between EUR 100 000 and EUR 5 million, the final countries of destination are Israel, Hong Kong and China.***

- ***Proceeds of phishing are initially transferred to accounts of money mules in Europe and then withdrawn in cash as quickly as possible. These are round figures of some thousand EUR, sometimes several transfers of identical amounts in rapid succession.***

2. Drug trafficking

CTIF-CFI's study carried out at the end of 2018 on laundering the proceeds of drug trafficking showed that a substantial part of drug trafficking by small dealers and intermediaries increasingly shifted from the streets to the internet. The closure of restaurants and bars may have reduced occasional drug use but in economic terms the demand for drugs is relatively inelastic. It is therefore quite probable that in the current situation drug trafficking will continue to develop through online contacts.

As physical shops have closed there is a sharp increase in online trade and delivery of various goods by couriers. This also enables criminal organisations to increasingly use this channel for drug trafficking purposes.

In the period just before restrictions on international flights police and customs reported a sharp rise in the number of drug traffickers at the airport, heroin as well as cocaine were confiscated. Large amounts of cocaine were also recently confiscated at the port of Antwerp. Criminal organisations who import drugs probably anticipated fewer checks due to the COVID-19 measures and will probably continue to do so in the future.

The production of synthetic drugs in Belgium and the Netherlands is perhaps most affected by the measures introduced to reduce the spread of COVID-19. Production of precursors in China required to produce synthetic drugs was halted for quite some time. This seems to result in a price rise of drugs such as XTC.

The health crisis in the short term and the economic crisis in the long term will probably not reduce the general size of the drug market in Belgium, so it can be assumed that the laundered proceeds will be not decrease in absolute terms.

With regard to money laundering the current crisis provides both challenges and opportunities for criminal organisations involved in drug trafficking. Because all businesses have been asked to close, cash can no longer be injected through cash-intensive front companies. Depositing cash at the bank is not possible or would immediately raise suspicions. Given that drug trafficking is mainly cash-based, undoubtedly significant amounts are now hoarded outside of the financial system.

The easing of restrictive measures and the economic crisis will be an excellent opportunity for criminal organisations to launder these funds. Many bars and restaurants will have problems to stay afloat and will be susceptible to takeovers by criminal organisations. A large cash turnover for these companies will not be treated as suspicious and claimed to be a “catch-up operation” by customers.

The economic uncertainty will lead to a drop in real estate prices. Laundering the proceeds of drug trafficking by purchasing real estate will be facilitated as a result. This will be the case at national and international level.

Criminal organisations involved in drug trafficking will have even larger amounts of cash at their disposal. When the economic and social life resume they will be ready to inject these funds into the financial system.

Large cash deposits on accounts of companies with a small official turnover or those in financial difficulties could point to a potential link with drug trafficking. The investment of these funds by purchasing other cash-intensive businesses or investing in real estate in

Belgium and abroad take place in the final phase of money laundering, integration. Spain, Morocco, Turkey and especially the United Arab Emirates (Dubai) are countries where money is frequently invested in real estate.

3. Corruption

To deal with the emergency situation caused by the COVID-19 pandemic governments in the most affected countries quickly started to look for protective equipment on a large scale. Given that the number of manufacturers and the production capacity were limited, all options were explored and both known official suppliers and intermediaries claiming to have the necessary contacts were approached. The manufacturers of COVID-19 material are almost all located in China, so geopolitical relations also played a role in the procurement procedure. Countries such as the United States did not hesitate to put pressure on market players and disrupt existing contracts by offering a higher price.

It goes without saying that the characteristics of the market and the exceptional circumstances of trading can lead to several types of corruption. In the long run we can assume that the search for medication to treat COVID-19 or the development of a vaccine will involve huge amounts of money. These huge financial interests will be shared among government authorities and private stakeholders at a global level. So there is a significant risk that corruption may be involved in these efforts at some point.

Apart from dealing with the crisis from a medical point of view governments and international organisations are also tackling the economic consequences. Several economic aid programmes of unparalleled scale have been set up to this end. The unprecedented nature, the urgency and the financial scale of the programmes pose a risk of corruption.

The following transactions could point to corruption:

- ***Transactions that could be related to the embezzlement of public funds, public procurement or government contracts in a sensitive sector (including healthcare, medicines and medical equipment);***

- ***Transactions involving newly established companies or companies with an opaque management structure;***

- ***Transactions involving intermediaries or consultants;***

- ***Transactions that cannot be supported by documents (contract is missing) or the documents presented reveal inconsistencies (important provisions and conditions are not listed, insufficient or excessive amounts, amendments without any commercial rationale);***

- ***Payments are carried out outside of the contractual terms.***

- ***Proceeds of embezzlement, bribery or corruption are hidden or concealed as another type of income by decision makers or Politically Exposed Persons (PEP).***

4. Social and fiscal fraud

In the current economic situation activities in several sectors have declined sharply or even stopped completely. Companies in sectors susceptible to social and/or serious fiscal fraud may be tempted to get involved in criminal activities and/or to increase their share of illicit turnover. Companies that have been particularly affected by the crisis that nevertheless generate large financial flows without any economic justification should be closely monitored.

These vulnerable sectors include the construction industry, industrial cleaning and transportation of goods.

A first risk is the misuse of the system of temporary unemployment. Fraud with this system does not only involve unduly obtaining unemployment benefits, social security contributions are not paid by the employer either. The fraud usually consists of applying for benefits for employees who keep on working unofficially.

A second risk is employing people without declaring them – illegal employment. The companies are often part of a network of companies with a similar profile, used to move employees without complying with (all) of their fiscal or social obligations. The illegal business model is mainly based on quickly expanding the number of companies involved, using front men as managers, mutually invoicing and paying and constantly opening and switching bank accounts. These techniques make it difficult to get a grip on the complete structure of the criminal networks.

The following characteristics may indicate the use of front companies for illegal employment:

- ***The company was recently set up, the registered office is located at a post office box address or a business centre.***

- ***The manager appears to be a front man and is used to conceal the identity of the actual manager (recently registered in Belgium, no prior role in a Belgian company or a large number of recent roles and prior bankruptcies, no representative for the company's accounts).***

- ***The former manager keeps control of the company's accounts (and stays the de facto manager).***

- ***The company's accounts are used to move proceeds of social fraud. The laundering takes place by moving funds between many accounts and subsequently withdrawing the money in cash.***

In addition to the increased risk of social fraud and/or serious fiscal fraud vulnerable companies can also be used to launder proceeds of other types of crime by using the offsetting technique. The offsetting technique is a money laundering technique enabling criminals to move excess cash from criminal activities such as drug trafficking to undeclared businesses in need of cash to finance their illicit activities, to avoid using the official banking system. The cash that is handed over is offset against bank transfers, often to foreign countries and with the use of false invoices.

Offsetting schemes often feature transfers abroad to companies in an industry which is completely different from the ordering company, and not in line with economic reality. The references accompanying these transfers are often vague and refer to the sale of goods or the supply of services without further details.

The new economic reality can also make sectors that do not appear to be affected by the crisis more vulnerable to economic exploitation, such as courier services. As many shops are closed online trading is booming, which leads to a sharp rise in home deliveries. When large companies can no longer meet the demand they could –possibly unwittingly– use a number of subcontracted smaller couriers operating illegally.

5. Sources

- European Banking Authority – Statement on actions to mitigate financial crime risks in the COVID-19 pandemic: https://eba.europa.eu/eba-provides-further-guidance-use-flexibility-relation-covid-19-and-calls-heightened-attention-risks
- Europol – press release and report on pandemic profiteering: how criminals exploit the COVID-19 crisis: https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know
- FATF: https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html
- INTERPOL: Unmasked – International Covid-19 fraud exposed. https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed
- OLAF: https://ec.europa.eu/anti-fraud/media-corner/news/07-04-2020/olafs-fight-against-fraud-continues-amid-covid-19-crisis_en

***