Consequences of the COVID-19 crisis on money laundering and terrorist financing

The current crisis linked to the global COVID-19 pandemic poses extraordinary challenges to our society. The priority for national governments is to contain the situation from a medical point of view, but they are also trying limit the scale and the consequences of the economic crisis. Even though the current situation is unprecedented, smaller crises in the past have shown that criminals –bearing in mind the motto "never waste a good crisis"– are quick to take advantage of changing and extreme economic circumstances. According to reports by Europol[1], Interpol[2] and the FATF[3] criminal organisations have used the coronavirus crisis to adapt their existing modi operandi or develop new criminal activities.

CTIF-CFI's document is aimed at raising awareness of obliged entities on the short-term effects of the current situation on predicate money laundering offences, which are mainly related to fraud. Based on studies by international organisations and the analysis of its own files, CTIF-CFI has identified a number of concrete typologies that could help obliged entities identify these types of fraud and then update this document based on disclosures received.

The different types of fraud that have been identified mainly relate to the sale of material used to combat the coronavirus and to stop the spread of COVID-19. This material includes protective equipment such as face masks and (potential) medicines for COVID-19, for which we will use the term COVID-19 material in this document.

This document lists a number of modi operandi and indicators. A single indicator does not suffice to raise suspicions of money laundering. The occurrence of several elements described below should result in further checks of the transaction.

CTIF-CFI asks obliged entities to report any potential link with the coronavirus crisis by mentioning the term "COVID19" in the field where the reason for submitting an STR in the online reporting system can be listed.

[1] https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic
[2] https://www.interpol.int/
[3] https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

1. Fraud targeting companies

a. Modi operandi

Fraud targeting companies frequently involves the following two modi operandi:

- The coronavirus is used as a pretext to intercept payments.
- Criminals claim to be manufacturers and distributors of COVID-19 material.

The coronavirus is used as a pretext to intercept payments.

As a result of various awareness-raising campaigns, the business world is now familiar with issues such as CEO fraud and Business Email Compromise Fraud (BEC Fraud). Criminal use the lockdown and the difficult economic situation of many companies due to the current crisis to circumvent the existing detection mechanisms.

Here a two examples:

- Criminals contact the company's bank claiming to be the manager of this company. The supposed manager states that he and his colleagues are working from home and due to the lack of organisation at the company the normal security procedures for payments, such as the use of two signatures, cannot be followed in the current situation. He insists that communication must take place by email.

- By using the lack of organisation due to the current crisis as an excuse, criminals insist on paying directly into the account of the company's production sites and not into the company's central account as usual. Problems with accounting or the company's cash position are sometimes used as an excuse. By using this fraudulent scheme financial flows within an existing business relationship can be diverted to the fraudsters' accounts.

Now that more people are working from home there is an increased cybersecurity risk. Criminals can use security breaches to get access to confidential documents and use this information to set up complex fraud schemes. Theft of confidential information has been used to commit CEO fraud and BEC fraud in the past.

Criminals claim to be manufacturers and distributors of COVID-19 material.

Through social engineering criminal can claim to be selling COVID-19 material. The permanent state of urgency in which governments as well as private individuals are operating in order to purchase such material make them vulnerable to fraud.

To substantiate their offer criminal can:

- Produce fake documents
- Create fake websites
- Set up front companies
- Claim to be an existing company with an excellent reputation in the industry

b. Indicators with respect to victims

- *'New' account of the beneficiary*

The customer has business relationships with a number of contractual partners. He suddenly wants to transfer money to:

- a new beneficiary and/or
- an account in a country where he does not do any business

The financial institution should be very vigilant when a payment has be made to a new beneficiary, quickly followed by a new payment order. When fraudsters have been successful they often repeat their actions by requesting a second payment order.

- *Inconsistencies with respect to the new beneficiary*

The following inconsistencies with regard to the beneficiary may occur:

- The beneficiary is a front company.
- The beneficiary is a new player on the market and does not have any documented experience in selling COVID-19 material.
- The beneficiary is not the manufacturer of the material but a third party that does not have an established business relationship with the manufacturer.
- The beneficiary does not have a clear own economic activity.
- The beneficiary's account is located in a country that is seemingly not related to the transaction to be carried out.

- *Urgent nature of the transaction*

The customer insists that the transactions needs to be carried out urgently. This could be the result of the customer being put under pressure by the fraudsters. Criminals often threaten to send the goods, which are in high demand, to another party if payment is not carried out quickly.

- *Fraudulent domain names*

Fraudulent payments instructions could come from mail servers or email addresses that are slightly different from the customer's usual address, by leaving out or adding some characters.

In more sophisticated types of fraud the customer's mail server is hacked and payment instructions are provided by using the usual email addresses.

- *Inconsistencies in documents*

The documents given to the professional trader could reveal inconsistencies. The messages between the customers and his alleged contractual partner can point to signs of phishing.

It was also found that fraudsters set up fake websites claiming to sell COVID-19 material. The FIU's experience shows that the terms and conditions often do not match the alleged business activity. The level of detail of the available information on these websites is usually very limited.

c. Indicators with respect to perpetrators

- *Unusual amount*

The amount received on the account does not match the beneficiary's profile. The cases analysed by the FIU show that money mules are generally people with a limited income who suddenly receive a payment of several tens of thousands EUR on their account.

- *Inconsistencies in the customer's economic activity*

The customer opens an account to receive his salary, large amounts from abroad are subsequently transferred to this account.

Example:

A customer is an employee of a Belgian bank. 25.000 EUR is transferred from a French company with reference to the payment of an invoice (e.g. Payment of invoice 123456).

The payment received does not match the customer's economic activity.

Example:

A company with very broad corporate goals suddenly receives payment related to the sale of COVD-19 material.

2. Fraud targeting private individuals

The fraud cases targeting private individuals involve fraud and breach of intellectual property rights. Common fraud schemes are used:

- COVID-19 material is sold but never delivered.
- Counterfeit material is sold.
- The sale of medication takes places outside of the permitted channels.

These types of fraud largely take place online. In addition to the use of online trading platforms a large number of unwanted emails (SPAM) are sent and ads on social media are often used. Further details can be found in the analyses by Europol, Interpol and FATF, referred to in the footnotes above.

The following elements can point to possible fraud:

- *Indicators related to the kind of goods sold*

The following terms can be linked to the fraudulent sale of COVID 19-material:

- COVID-19
- Coronavirus
- SARS-CoV-2
- Mask
- FFP2
- FFP3
- (personal) protective equipment or PPE
- Chloroquine - Hydroxychloroquine - Azithromycine
- Plaquenil
- Hand sanitizer
- Disinfectant
- Alcohol 70%
- Ethanol 70%
- Face shield
- Hazmat suits
- Decontamination suits
- Ventilator, respirator, or breathing machine

- Artificial respiration
- Breathing apparatus

- *Indicators related to the price of goods*

An unusually high or low price compared to commonly used prices.

- *Indicators related to the beneficiaries of a transaction*

The beneficiary is a front company or does not trade in COVID-19 material.

- *Indicators related to the distribution channel*

Goods are sold without using the conventional distribution channel.

***