PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

# Typologies COVID-19

## Note

**Version 1.0 of 02.04.2020**

This document is intended for professionals subject to the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended.

Offices:
41B boulevard Franklin D. Roosevelt
L-2450 Luxembourg

Mailing address:
L-2080 Luxembourg

Email: crf@justice.etat.lu
Website: www.crf.lu
Phone: (+352) 47 59 81-447

# INTRODUCTION

Reports published by Europol, Interpol and the FATF show that criminal groups have been quick to exploit the coronavirus crisis and the spread of COVID-19 for their purposes, by adapting their existing modus operandi or engaging in new criminal activities. The Financial Intelligence Unit (FIU) refers specifically to the documentation published by these entities:

- Europol: https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic
- Interpol: https://www.interpol.int/
- FATF: https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html

The objectives of this note are to:

a) Inform professionals subject to the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (hereinafter: the 2004 AML/CFT Law) about the existence of the above documentation;
b) Raise awareness amongst professionals, in particular with regard to the typologies described below;
c) Share an initial set of fraud-related indicators related to COVID-19;
d) Obtain feedback to complete this list of indicators.

The work carried out by the FIU and reflected in this note is based on the analyses carried out by the various international organisations as well as on suspicious transaction reports received in recent weeks. Our analysis shows that continued vigilance of professionals subject to the 2004 AML/CFT Law remains essential in the prevention of, and fight against, these new variants of financial crime.

To assist professionals in their tasks, this note contains a list of indicators. A single indicator by itself may not necessarily arouse suspicion. However, the presence of several of these indicators should trigger a more rigorous verification of the transaction in question.

In view of the limited information available to the FIU, this note only addresses fraud indicators. The FIU is cooperating with its international partners to improve and complete the current list. It goes without saying that the FIU remains at the disposal of reporting entities to discuss other potential indicators.

This analysis contains:

- An overview of the typologies found (1),
- Details regarding the process for submitting reports in relation to the COVID-19 crisis (2).

# 1 FRAUD

The fraud events analysed by the FIU concern mostly the sale of various products and equipment used in the combat against the coronavirus and the spread of COVID-19. The products involved include amongst others protective masks and (purported) drugs against the virus and the disease. In the remainder of this note, these products and equipment are referred to as "COVID-19 materials".

## 1.1 SOCIAL ENGINEERING

### 1.1.1 TYPOLOGIES ENCOUNTERED

The types of fraud concerned include:

- CEO fraud,
- Business E-Mail Compromise (BEC) fraud.

More information on these types of fraud can be found in the FIU's note on fraudulent transfers[1] and in the Egmont Group of FIU's documentation on business e-mail compromise (BEC)[2].

Two operating methods developed and tailored on the basis of social engineering can be distinguished:

- The coronavirus crisis used as a pretext to divert payments,
- Criminals posing as producers and distributors of COVID-19 materials.

**Coronavirus crisis used as a pretext to divert payments**

CEO and BEC fraud are well-known and have been the subject of extensive prevention campaigns[3]. Fraudsters are now taking advantage of the situation created by the COVID-19 pandemic, including the containment and social distancing measures as well as economic dislocation, to evade the diligence thresholds of targeted companies.

The following two examples illustrate this:

- Fraudsters impersonate the director of a legitimate company and contact the company's financial institution. The purported director explains that the entire business is currently disrupted and that he or she is working from home. He or she argues that it is therefore not possible to follow the usual procedures (in particular countersignatures) and insists on a communication exclusively by e-mail.

- Under the pretext of corporate disruption, fraudsters argue that payments are no longer to be made to the company's central banking accounts, but directly to the banking accounts of the relevant production sites. They may also argue, for example, that they are experiencing cash flow problems or problems with their accounting department. This scheme allows payments made within the framework of an existing business relationship to be diverted to fraudulent accounts.

In terms of IT security[4], teleworking from home creates new risks. Criminals can exploit security loopholes to gain access to confidential documents, which are then used in sophisticated frauds. It should be remembered that the theft of privileged information is one of the reasons why CEO and BEC frauds are successful.

**Alleged producers and distributors of COVID-19 materials.**

Using social engineering, criminals pose as vendors of COVID-19 materials. The constant state of urgency in which private and public sector players can find themselves in their attempts to acquire these materials increases their vulnerability to fraud. In order to gain credibility criminals will, *inter alia*:

- Produce false documents,
- Create fictitious websites,
- Create front companies,
- Purport to be companies that produce the equipment in question.

[1] https://justice.public.lu/dam-assets/fr/legislation/circulaires/CRF-note-faux-virements.pdf
[2] https://justice.public.lu/dam-assets/fr/organisation-justice/crf/guidances/20190708-EGMONT-GROUP-BEC-BULLETIN-final.pdf
[3] See in particular: https://police.public.lu/fr/actualites/2018/10/w42/17-cyberscams.html
[4] See in particular: https://cybersecurite.public.lu

### 1.1.2 INDICATORS ENCOUNTERED IN RELATION TO THE VICTIM

#### 1.1.2.1 "NEW" BENEFICIARY ACCOUNT

The customer entity has business relations with a number of contracting parties. Suddenly it intends to effect a funds transfer:

- In favour of a new beneficiary and/or
- In favour of an account opened in a country in which he or she does not operate.

The financial institution should be especially vigilant when a payment made to a new beneficiary is rapidly followed by a second payment instruction to the same beneficiary. Indeed, once successful a first time, fraudsters tend to issue a repeat instruction.

#### 1.1.2.2 INCONSISTENCIES IN RELATION TO A NEW BENEFICIARY

In particular, the following inconsistencies may appear in relation to the beneficiary:

- The beneficiary is a front company,
- The beneficiary is a new player in the market and has no documented experience in trading COVID-19 materials,
- The beneficiary is not the producer of the materials, but a third party who has no documented relationship with the producer,
- The beneficiary has no real economic activity,
- The beneficiary account is located in a jurisdiction that has no apparent connection with the transaction to be carried out.

#### 1.1.2.3 URGENCY OF THE TRANSACTION

The customer insists on the urgency of the transaction to be carried out. This attitude may be the result of the pressure exerted on the customer by the criminal, who explains that failing immediate payment, the goods - which are in great demand - will be sent to another customer.

#### 1.1.2.4 FRAUDULENT DOMAIN NAMES - PHISHING/PHARMING

The transfer instructions come from an email account that closely resembles the customer's email account. However, the e-mail address has been slightly modified by the addition, change or deletion of one or more characters.

> Examples :
> contact@abc.com instead of contact@abc.lu
> contact@adc.com instead of contact@abc.com

The instructions can also come from the customer's correct e-mail address, which has been hacked. These cases of fraud are more sophisticated.

#### 1.1.2.5 INCONSISTENCIES IN DOCUMENTATION

The supporting documents submitted to the professional may contain inconsistencies.

First of all, messages exchanged between the customer and the purported contracting partner may point to a phishing/pharming attempt (point 1.1.2.4 above).

The documentation seen by the FIU also shows that criminals create fictitious websites to simulate economic activity related to the sale of COVID-19 materials. The FIU's experience shows that the terms and conditions of such sites are often not consistent with the purported economic activity. The level of detail provided by these fictitious websites is often very limited.

### 1.1.3 INDICATORS ENCOUNTERED IN RELATION TO THE PERPETRATOR (BENEFICIARY ACCOUNT)

#### 1.1.3.1 INCONSISTENCY IN THE TRANSACTION AMOUNT

The amounts collected by the beneficiary account holder may be inconsistent with the customer's profile. In the cases analysed by the FIU, individuals received amounts of several tens of thousands of euros even though they were on a modest salary.

Such accounts are often opened by "*money mules*", defined by Europol as *"a person who transfers illegally obtained funds between different bank or other accounts, very often in different countries, on behalf of others. Money mules are thus recruited by criminals to receive money from their bank accounts in order to withdraw it or transfer it to accounts held abroad, often in return for a commission"*[5].

#### 1.1.3.2 INCONSISTENCY WITH CUSTOMER ACTIVITY

The customer has opened an account to receive salaries from a local employer and receives large amounts from abroad, unrelated to the performance of an employment contract.

*For example:*

*The customer is an employee of a local bank and receives a transfer of EUR 25 000 from a French company. The particulars indicated in the transfer are "Payment of invoice 123456".*

The purpose of the payment received is inconsistent with the professional activity of the customer, whether it be a natural or legal person.

*For example:*

*A company was opened as a shelf company with a very general corporate purpose and suddenly receives sums of money in connection with the sale of COVID-19 materials.*

The company's corporate purpose does not include this activity.

*For example:*

*The company was opened in the legal form of a holding company or SOPARFI. Certain balance sheet items (turnover, salaries, social security contributions, etc.) of the company are not in line with its intended transactions.*

[5] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling

## 1.2 FRAUD AIMED AT A WIDER AUDIENCE

The case studies relate to fraud and intellectual property offences. The criminal patterns are classic:

- COVID-19 materials offered for sale, but never delivered,
- The sale of counterfeit COVID-19 materials,
- The sale of medicines outside the authorised networks.

Most of the above fraud types are committed online. In addition to on-line marketplaces exploited for this purpose, there is frequent use of advertisements by e-mail (SPAM) or published on social networks.

For further details, reference is made to the above-mentioned Europol, Interpol and FATF notes.

### 1.2.1 INDICATORS IN RELATION TO THE PRODUCTS OFFERED FOR SALE

#### 1.2.1.1 THE PURPOSE OF THE TRANSACTION

The following terms may be included in the particulars of the transaction:

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

#### 1.2.1.2 THE PRICE OF THE ITEMS

Abnormally low or high prices compared to those normally charged.

### 1.2.2 INDICATORS IN RELATION TO THE BENEFICIARY OF THE TRANSACTIONS

- The beneficiary is a front company,
- The beneficiary is not active in the distribution of COVID-19 materials.

### 1.2.3 INDICATORS IN RELATION TO THE OPERATION OF THE ACCOUNT

The sale of COVID-19 materials generates cash inflows to the account, but no expenses related to this activity are recorded on the account. This is particularly the case if all cash receipts are used for private purposes by the account holder.

### 1.2.4 INDICATORS IN RELATION TO THE DISTRIBUTION CHANNEL

#### 1.2.4.1 SALE OF PRODUCTS OUTSIDE THE AUTHORISED NETWORKS

An example would be the sale of chloroquine drugs via the Internet.

#### 1.2.4.2 LINK WITH THE DARK WEB

This indicator applies more specifically to virtual asset service providers.

## 2 THE REPORTING PROCESS

The FIU continues to receive and analyse suspicious transaction reports in accordance with its Note of 16 March 2020 addressed to Professionals (Functioning of the FIU - Covid-19)[6].

Professionals are requested to flag reports related to the coronavirus crisis to the FIU by including the term "COVID19" in the reason given for the report.

[6] https://justice.public.lu/dam-assets/fr/organisation-justice/crf/info-covid19.pdf