

## MEASURES TAKEN BY THE FINANCIAL INTELLIGENCE UNIT IN THE CONTEXT OF CORONAVIRUS

The Luxembourg Financial Intelligence Unit (FIU) has published on its website several documents with respect to the AML/CTF obligations in the context of the COVID-19 pandemic.

### COMMUNICATION WITH PROFESSIONALS

In summary, the FIU has specified that:

- collection of suspicious transactions reports continues to operate as usual;
- requests for information made by the FIU to professionals in accordance with Article 5.1 (b) AML/CFT Law will continue to be issued via the goAML platform, which can be accessed online with the help of a LuxTrust identifier;
- any professional that may not be able to reply to a normal (i.e. not especially urgent) FIU request for information within the usual timeframe must notify the FIU without delay and respond within a reasonable period of time (the FIU taking however into account potential constraints and imperatives of the professional);
- the FIU will contact professionals by telephone for any urgent or very urgent requests as well as for freezing orders and professionals are asked to refrain from making telephone calls to the FIU service other than for urgent operational requests;
- any potential interviews with professionals will be conducted by videoconference; and
- 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.

### TYOLOGIES OF COVID-19-RELATED FRAUD

The FIU has published an overview of the social engineering methods used by criminal groups to defraud professionals and consumers, often by pretending to sell various products and equipment, such as drugs and/or masks used in the combat against the spread of coronavirus (referred to hereafter as Covid-19 materials).

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

The FIU warns that criminal groups are now taking advantage of the situation created by the COVID-19 pandemic, including the containment and social

#### Key aspects:

- FIU continues to operate as usual during the Covid-19 pandemic.
- Professionals must notify FIU if they are unable to reply in the usual timeframe.
- Criminal groups may use the coronavirus crisis as a pretext to divert usual payments to fraudulent accounts or to obtain privileged information.
- FIU has published a list of Covid-19 related typologies and indicators that may point at the existence of a potentially fraudulent transaction.

*This briefing speaks as of 24 April 2020.*

distancing measures as well as economic dislocation, to evade the diligence thresholds of targeted companies. They also exploit IT security loopholes to gain access to privileged information, which is then used in sophisticated frauds.

As such, criminals may impersonate the director of a legitimate company and pretend that, due to corporate disruption, they are not able to follow the usual procedures (e.g. countersignatures) and have to communicate exclusively by e-mail.

Moreover, under the pretext of corporate disruption, citing problems with the accounting department or cash flow-related issues, fraudsters may argue that payments should no longer be made to the company's central banking accounts, but directly to the banking accounts of the relevant production sites and as such, request payments to be diverted to their fraudulent accounts.

### **Fraudsters passing as producers and distributors of COVID-19 materials**

The FIU further informs that criminals may 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. As such, criminals may resort to producing false documents, creating fictitious websites, creating front companies or pretending that they themselves are producing the COVID-19 materials in question.

Criminals may hence offer COVID-19 materials for sale, but never deliver them. They may also sell counterfeit COVID-19 materials or drugs that have not been duly authorised by the competent authorities.

### **INDICATORS OF COVID-19-RELATED FRAUD**

According to FIU, financial institutions may detect the existence of COVID-19 - related fraud through a series of indicators in relation to the potential victim, the potential perpetrator and the products offered for sale in the purported fraudulent transaction.

#### **Indicators in relation to the victim**

The following indicators may point at the victim of a potentially fraudulent transaction:

- customer entity is suddenly effecting a funds transfer in favour of a new beneficiary and/or in a country in which it does not operate;
- inconsistencies in relation to a new beneficiary (i.e. beneficiary is a front company, a new player with no documented experience in trading COVID-19 materials, has no real economic activity or is situated in a jurisdiction with no apparent connection with the transaction);
- customer entity insists on the urgency of the transaction to be carried out;
- fraudulent instructions come from an e-mail account that closely resembles the customer's email account, but contains small changes (e.g. ".lu" domain name, instead of ".com", letter swaps etc.); and
- inconsistencies in documentation (e.g. fictitious websites to simulate economic activity related to the sale of COVID-19 materials, discrepancies in the terms and conditions etc.).

## **Indicators in relation to the beneficiary of the transaction**

The following indicators may point at the beneficiary of a potentially fraudulent transaction:

- inconsistencies in the transaction amount (e.g. individuals receiving large amounts of money, despite otherwise earning modest salaries);
- discrepancies between the activity of the customer and the purpose of the payments received (e.g. employee receiving a large payment for an invoice billed in a different country, company receiving payments for an activity not included in its general corporate purpose, holding company with balance sheet items not in line with its intended transaction, beneficiary not being active in the distribution of COVID-19 materials); and
- beneficiary of the transaction is generating cash inflows due to COVID-19 - related sales, but no expenses related to the activity are recorded on the account.

## **Indicators in relation to the products offered for sale**

The following product-related indicators may point at the existence of a potentially fraudulent transaction:

- transaction's reference may include COVID-19 -specific terms, such as *inter alia* "Covid-19", "Coronavirus", "FFP2", "FFP3", "(personal) protective equipment" or "PPE", "Hand sanitizer", "70% Ethanol", "Hazmat suits", "Hydroxychloroquine", "Face shield", "Ventilator", "Respirator", "Breathing machine" etc.;
- price of the sold items may be abnormally low or high, compared to those normally charged; and
- products are sold outside the authorised networks (e.g. chloroquine drugs sold via the internet) or are linked to or paid for via the dark web (e.g. in the case of virtual asset service providers).

## CONTACTS



**Steve Jacoby**  
Partner

T +352 48 50 50 219  
E [steve.jacoby@cliffordchance.com](mailto:steve.jacoby@cliffordchance.com)



**Christian Kremer**  
Partner

T +352 48 50 50 201  
E [christian.kremer@cliffordchance.com](mailto:christian.kremer@cliffordchance.com)



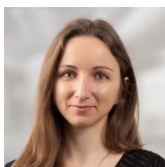
**Marc Mehlen**  
Partner

T +352 48 50 50 305  
E [marc.mehlen@cliffordchance.com](mailto:marc.mehlen@cliffordchance.com)



**Udo Prinz**  
Counsel

T +352 48 50 50 232  
E [udo.prinz@cliffordchance.com](mailto:udo.prinz@cliffordchance.com)



**Boika Deleva**  
Associate

T +352 48 50 50 260  
E [boika.deleva@cliffordchance.com](mailto:boika.deleva@cliffordchance.com)



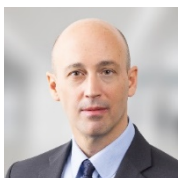
**Ewa Baginska**  
Associate

T +352 48 50 50 490  
E [ewa.baginska@cliffordchance.com](mailto:ewa.baginska@cliffordchance.com)



**Yolanda-Alma Ghita-Blujdescu**  
Associate

T +352 48 50 50 489  
E [yolanda.ghita-blujdescu@cliffordchance.com](mailto:yolanda.ghita-blujdescu@cliffordchance.com)



**Emmanuel-Frédéric Henrion**  
Partner

T +352 661485190  
E [emmanuelfrederic.henrion@cliffordchance.com](mailto:emmanuelfrederic.henrion@cliffordchance.com)



**Kristof Meynaerts**  
Partner

T +352 48 50 50 226  
E [kristof.meynaerts@cliffordchance.com](mailto:kristof.meynaerts@cliffordchance.com)



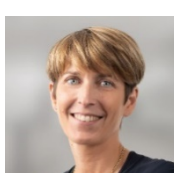
**Paul Van den Abeele**  
Partner

T +352 48 50 50 478  
E [paul.vandenabeele@cliffordchance.com](mailto:paul.vandenabeele@cliffordchance.com)



**Oliver Zwick**  
Senior Associate

T +352 48 50 50 476  
E [oliver.zwick@cliffordchance.com](mailto:oliver.zwick@cliffordchance.com)



**Caroline Migeot**  
Counsel

T +352 48 50 50 258  
E [caroline.migeot@cliffordchance.com](mailto:caroline.migeot@cliffordchance.com)

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 10 boulevard G.D. Charlotte,  
B.P. 1147, L-1011 Luxembourg, Grand-Duché  
de Luxembourg

© Clifford Chance 2020

Abu Dhabi • Amsterdam • Barcelona • Beijing •  
Brussels • Bucharest • Casablanca • Dubai •  
Düsseldorf • Frankfurt • Hong Kong • Istanbul •  
London • Luxembourg • Madrid • Milan •  
Moscow • Munich • Newcastle • New York •  
Paris • Perth • Prague • Rome • São Paulo •  
Seoul • Shanghai • Singapore • Sydney •  
Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement  
with Abuhimed Alsheikh Alhagbani Law Firm  
in Riyadh.

Clifford Chance has a best friends relationship  
with Redcliffe Partners in Ukraine.