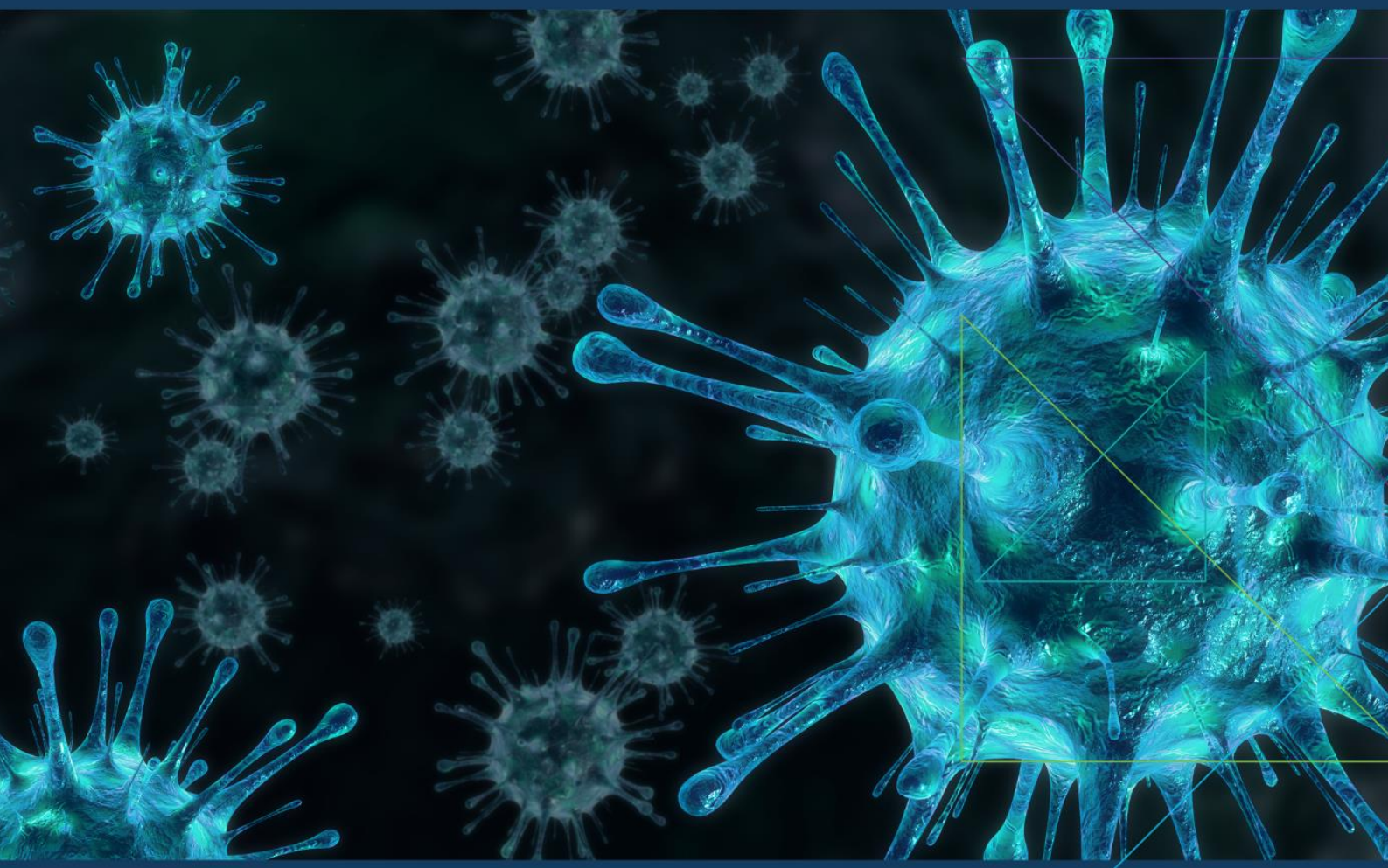
ECOFEL

EGMONT CENTRE OF FIU
EXCELLENCE & LEADERSHIP

COVID-19 BEST PRACTICES FOR FINANCIAL INTELLIGENCE UNITS



PUBLIC SUMMARY

MARCH 2021

COVID-19 BEST PRACTICES FOR FINANCIAL INTELLIGENCE UNITS

A Report Produced by ECOFEL

Public Summary

The Egmont Group (EG) is a global organization of Financial Intelligence Units (FIUs). The Egmont Group Secretariat (EGS) is based in Canada and provides strategic, administrative, and other support to the overall activities of the Egmont Group, the Egmont Committee, the Working Groups as well as the Regional Groups.

The Egmont Centre of FIU Excellence and Leadership (ECOFEL), active since April 2018, is an operational arm of the EG and is fully integrated into the EGS in Canada. ECOFEL is mandated to develop and deliver capacity building and technical assistance projects and programs related to the development and enhancement of FIU capabilities, excellence and leadership.

ECOFEL IS FUNDED THROUGH THE FINANCIAL CONTRIBUTIONS OF UKAID AND SWISS CONFEDERATION

Table of Contents

Acronyms

AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
CDD	Customer Due Diligence
ESW	Egmont Secure Web
EU	European Union
FATF	Financial Action Task Force
HoFIU	Heads of FIU
KYC	Know Your Customer
ML	Money Laundering
PEP	Politically Exposed Person
PPE	Personal Protective Equipment
SAR	Suspicious Activity Report (also includes Suspicious Transaction Report)
TF	Terrorist Financing
VPN	Virtual Private Network
WHO	World Health Organisation

Executive Summary

1. The COVID-19 pandemic has spread with alarming speed, infecting millions and bringing economic activity to a near-standstill as countries imposed tighter restrictions on movement to halt the spread of the virus [the World Bank, 2020 (1)]. According to the WHO, as at the end of July 2020, almost 16 million cases of COVID-19 have been reported to the WHO and more than 640,000 deaths. COVID-19 has changed our world [WHO, 2020 (2)].

2. Whilst reporting entities, the domestic partners of FIUs and other stakeholders are also experiencing difficulties due to COVID-19, resulting in some impact on their ability to provide information to and to liaise with FIUs, the impact has not been significant. With a few exceptions, SAR numbers have not decreased significantly during the past few months, with FIUs only noting a reduction where there has been economic decline or reporting entities having limited capacity.

3. Most FIUs have noted some new emerging risks as a result of the COVID-19 pandemic, particularly relating to fraud (concerning COVID-19 related medical equipment and PPE) and cybercrime. These risks are in line with those noted by the Egmont Group's Observers and other international organisations and no clear pattern is emerging as to regional differences. Many FIUs are alert to the emerging risks associated with COVID-19 in their jurisdictions. They are also aware of new emerging risks, such as those relating to the development of potential COVID-19 vaccines.

4. FIUs have responded quickly to the emerging risks, issuing typology reports and guidance for reporting entities, domestic partners and other stakeholders and carrying out risk assessments.

5. The COVID-19 experience has enabled FIUs to identify best practices to assist other FIUs during the current pandemic and also to note for the future, should a similar situation arise. These best practices cover a wide range of issues including staff welfare, premises management, remote working, data security and liaising with reporting entities, other FIUs, domestic partners and stakeholders.

6. FIUs have also shared the lessons they have learnt during the current pandemic.

7. The key message that has been shared by FIUs is the importance of flexibility in dealing with the current crisis in order to ensure the wellbeing of FIU staff and the security of the FIU's data, whilst also ensuring that the FIU is able to continue its crucial role in the global fight against money laundering and terrorist financing.

Introduction

On 30 January 2020, the WHO declared that the outbreak of novel coronavirus constituted a Public Health Emergency of International Concern. On 11 March 2020 the WHO characterised the novel coronavirus disease (COVID-19) as a pandemic.

Since the beginning of the COVID-19 outbreak, various fraudulent schemes and scams taking advantage of the crisis situation have been reported. Criminals are exploiting the crisis by adapting their modes of operation or developing new criminal activities. The crisis has also added a new layer of complexity in determining and mitigating crimes, like bribery and corruption in international transactions [Egmont Group, 2020 (3)]

The COVID-19 pandemic has brought new and sizeable challenges for everyone around the world, including FIUs.

In order to strengthen the capabilities of FIUs during this emerging crisis, ECOFEL conducted a series of virtual roundtables. The virtual roundtables have informed the original paper, together with a stocktaking exercise of open source material published by Egmont Group members, Observers and other international organisations.

Emerging Risks

What are the Egmont Group Observers and Other International Organisations Saying about the Emerging Risks?

A selection of the responses to the COVID-19 outbreak from the Egmont Group's Observers and other international organisations are set out below.

FATF

"Criminals are taking advantage of the COVID-19 pandemic to carry out financial fraud and exploitation scams, including advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that pray on virus related fears. Malicious or fraudulent cybercrimes, fundraising for fake charities, and various medical scams targeting innocent victims are likely to increase, with criminals attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about COVID-19. National authorities and international bodies are alerting citizens and businesses of these scams, which include imposter, investment and product scams, as well as insider trading in relation to COVID-19. Like criminals, terrorists may also exploit these opportunities to raise funds" [FATF, 2020 (5)].

In May 2020 the FATF produced a paper entitled '*COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*' using information provided to the members of the FATF Global Network in April 2020 [FATF, 2020 (5)]. The paper identifies the potential money laundering and terrorist financing risks as –

- Criminals finding ways to bypass CDD measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds;
- Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
- Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;
- As individuals move money out of the banking system due to financial instability, this may lead to an increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;

- Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent money laundering risks;
- Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries, both for the laundering of proceeds as well as to fund their operations, as well as fraudulently claiming to be charities to raise funds online.

Most recently, in July 2020, following updates on risks to the FATF, two webinars were produced. The first is entitled '*COVID-19 and the Changing Money Laundering and Terrorist Financing Risk Landscape, 30 July 2020* and the second, '*The Impact of Covid-19 on the detection of Money Laundering and Terrorist Financing, 31 July 2020*' [FATF (6)]. The webinars show that the risk situation is continuing to evolve, with changes in business operations, including associated legitimate financial activity, not only helping to obscure suspicious money movements but also revealing previously hidden illicit conduct.

EUROPOL

"Criminals have quickly seized opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities. Organised crime groups are notoriously flexible and adaptable and their capacity to exploit this crisis means we need to be constantly vigilant and prepared" [EUROPOL, 2020 (7)].

EUROPOL's website contains many articles relating to COVID-19 including a section on those crimes that have been reported by police across the EU as increasing [EUROPOL, 2020 (8)]. These crimes include –

- Shopping scams – posting fake adverts for products, such as medicines and hygiene products;
- Phishing and smishing;
- Ransomware;
- Illegal streaming;
- Organised property crime, particularly targeting vulnerable groups;
- Fraud;

- Child sexual exploitation;
- Teleworking vulnerabilities leading to data leaks;
- Mobile malware;
- Spreading misinformation and disinformation about COVID-19 endangering public health.

INTERPOL

"Criminals don't take breaks. Even as everything around us is being put on hold, they are looking for new ways to generate profits" [INTERPOL, 2020 (9)].

Interpol too has several pages on its website dedicated to COVID-19 and emerging risks [INTERPOL, 2020 (10)]. In particular, INTERPOL warns of –

- Counterfeit medical supplies and medicines;
- Cybercrime;
- Fraud – online or telephone.

In a report published on 4 August 2020 INTERPOL predicts that further increases in cybercrime are highly likely in the near future, with reference to coronavirus-themed online scams and phishing campaigns. Business Email Compromise schemes are also likely to surge due to the economic downturn and shift in the business landscape. INTERPOL also warns that when a COVID-19 vaccine is available, it is highly probable that there will be another spike in phishing related to the vaccine as well as network intrusion and cyberattacks to steal data [INTERPOL, 2020 (11)].

UNODC

"Profit remains at the heart of Transnational Crime. The threat will continue to evolve and persist during, and after, the pandemic. Organised criminals, including professional Money Launderers and Terrorism Financiers, will continue to assess and exploit demand for crisis-related goods and services" [UNODC, 2020 (12)].

The UNODC notes the following amongst its key messages –

- Fiscal and non-fiscal frauds related to the public response to COVID-19 are increasing. Cryptocurrency and other pyramid schemes are likely to grow;
- Traditional cash-courier money laundering has been significantly reduced

through ports and airports. It is unclear if organised criminals will seek alternative remittance methods for their criminal finances, such as cryptocurrencies or wire transfers, or await the reopening of borders;

- Transnational Organised Crime Groups and Terrorist Financiers will seek to exploit opportunities to offer financial services when State/Private Sector capabilities are reduced. The ensuing global economic downturn will present myriad of criminal finance (and investigative) opportunities;
- In trafficking in persons, criminals are adjusting their business models to the 'new normal' created by the pandemic, especially through the abuse of modern communications technologies [UNODC, 2020 (13)];
- There are indications that drug trafficking groups are adapting their strategies in order to continue their operations, and that some have started to exploit the situation so as to enhance their image among the population by providing services, in particular to the vulnerable [UNODC, 2020 (14);
- Despite localised disruptions due to travel restrictions and other social-distancing measures enacted by governments to manage the COVID-19 pandemic, there is likely to be little pause in wildlife trafficking; in many cases, poaching is likely to increase and illegal trade will adapt to changing market circumstances [UNODC, 2020 (15)].

The World Bank

"The pandemic highlights the urgent need for health and economic policy action, including global cooperation, to cushion its consequences, protect vulnerable populations, and strengthen countries' capacities to prevent and deal with similar events in the future. It is critically important for emerging market and developing economies, which are particularly vulnerable, to strengthen public health systems, address challenges posed by informality and limited safety nets, and enact reforms to generate strong and sustainable growth once the crisis passes" [The World Bank, 2020 (16)].

World Health Organisation

"Beware of criminals pretending to be WHO. Criminals are disguising themselves as WHO to steal money or sensitive information" [WHO, 2020 (17)].

Whilst FIUs, their domestic partners and reporting entities contend with the many

internal issues presented to them by the COVID-19 pandemic, criminals are looking to take every opportunity to exploit the situation. The Egmont Group Observers and other international organisations have produced and are continuing to produce extremely informative reports from the information available to them, as highlighted above, setting out the emerging risks as identified to them. It is clear that these risks will continue to change over the course of the pandemic as criminals adapt and continue to exploit any weaknesses. FIUs will clearly benefit from keeping abreast of these reports and from providing relevant information to these organisations, where appropriate, to ensure that every possible measure is taken to prevent the spread of COVID-19 related criminal activity. ECOFEL will continue to update its COVID-19 Channel for the benefit of Egmont Group members. FIUs, their domestic partners and reporting entities should work in partnership to stay one step ahead of criminals looking to exploit the pandemic.

Why is COVID-19 producing new emerging risks?

The key factors that are prompting these new emerging risks are seen as:

- Shifts in the demand and supply of goods and services, particularly in relation to goods such as PPE, COVID-19 tests and pharmaceutical products;
- Decreased mobility and flow of people. Due to the on-going pandemic, the increase in travel restrictions has impacted the mobility and flow of people. Many transnational crimes, such as trafficking in drugs, humans, contraband, firearms and wildlife are expected to be affected by these travel restrictions;
- Changes in people's online presence. The current global situation has greatly impacted on everyone's day-to-day life. According to the Financial Stability Institute an estimated 300 million office workers may have been working from home in May 2020, including 90% of banking and insurance workers [Financial Stability Institute (18)]. With an increased reliance on online communication tools to stay connected to work and peers, people are online more than ever before;
- Increased anxiety and fear. Due to the pandemic, citizens are experiencing more anxiety and fear; everything is under threat. The human reaction is a build-up of anxiety and fear that create vulnerability to exploitation;
- Decreased supply of illicit goods. The shift in supply of illicit goods causes the quantity consumed to decrease whilst the price rises;
- Emergency procurement. Emergency procurement may increase corruption

risks. Further, scarcity in supply will increase the risk of corruption in the procurement of these goods.

- Stimulus measures and international and domestic aid. Criminals may make fraudulent claims on government stimulus funds by posing as legitimate businesses seeking assistance.

What are the Emerging Risks Seen by FIUs?

FIUs are observing emerging risks associated with the COVID-19 pandemic. These involve increases in fraud, phishing, other online scams and increases in the misuse of public funds. FIUs which have issued public guidance or other documents refer to emerging risks within those documents.

In connection with Terrorist Financing, in June 2020, the United Nations Security Council Counter-Terrorism Committee Executive Directorate produced a paper entitled '*The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism*', aiming to provide a global picture of the potential and actual impact of COVID-19 on terrorists and terrorist groups which will no doubt be of interest to FIUs [United Nations, 2020 (19)]. The paper refers to certain events having a COVID-19 link, for example, attempted attacks against a hospital ship in the United States and a hospital treating COVID-19 patients and the arrest in Tunisia of two men who were reportedly planning to infect security forces with COVID-19. However, the paper states that it is difficult to reliably connect fluctuations in terrorist activity to COVID-19.

The paper also refers to increased terror attacks in Sub-Saharan Africa by groups affiliated to Al-Qaida and by Islamic State in Iraq and the Syrian Arab Republic amid the pandemic, stating that whilst these groups have exploited COVID-19 in their messaging it is difficult to determine whether the increased violence stems from existing trends, shifts in terrorist or counter-terrorism approaches due to the pandemic, or both. In terms of the attacks in Sub-Saharan Africa, the information provided to ECOFEL is that it is too early to say whether the increase is related to COVID-19, with analysis of the situation continuing.

Additional details on the emerging risks observed by FIUs, together with the regions in which these risks are being seen, is set out below.

Fraud Related Emerging Risks

- Frauds relating to the supply of COVID-19 medical equipment such as facemasks, counterfeit medication, false COVID-19 tests and products connected to potential COVID-19 vaccines, with the equipment either not being delivered (payment having been made up front), being counterfeit/illegal/unauthorised or of low quality. According to Europol, between 3 and 10 March 2020, over 34,000 counterfeit surgical masks were seized by law enforcement authorities worldwide as part of Operation PANGEA, an international effort co-ordinated by INTERPOL supported by Europol [Europol, 2020 (20)];
- Frauds seeking donations for alleged research and development into cures for COVID-19 (Central America, Europe);
- Frauds connected to government benefit or stimulus packages related to COVID-19, including bogus offers of support to businesses in order to obtain sensitive personal information and false claims to governments for benefits, including individuals moving funds in an attempt to hide the true value of their savings so that they appear to be entitled to claim benefits;
- The misuse of public funds relating to the emergency procurement of medical and anti-COVID equipment, such as respirators, PPE, disinfectant and COVID-19 tests. For example, by government officials colluding with suppliers to inflate the prices of goods, with the officials taking kickbacks, often into family members' accounts. These crimes could also be linked to possible corruption and tax crimes (Europe, Central and South America, Southern Africa);
- False humanitarian or charitable work in order to obtain funds, with concerns about an increased risk of terrorist financing though such charities. For example, bogus websites for charities (Europe, the Caribbean). FIUs may wish to advise reporting entities and domestic partners to research charities before donating and to use browsers that allow pop-up windows to be blocked;
- The procurement of PPE by non-specialised private companies, with such companies illegally submitting tenders to government schemes in order to distribute PPE (Europe);
- An increase in CEO frauds and cyber frauds believed to be due to the decrease in attention of senior management as a consequence of remote working. For example, individuals within an organisation receiving emails purporting to be

from the CEO/another senior employee, seeking financial information or instructing the transfer of money to the fraudster's account (Europe);
- Romance fraud, with COVID-19 as an excuse for the funds being required (Europe);
- Payment fraud, with adverts claiming to offer refunds for bookings (such as airline bookings) which have been cancelled (Europe);
- An increased use of wire transfers to carry out criminal activities.

Cybercrime

- Phishing[1] via fictitious links or webpages for local businesses to 'pay bills', offering 'free groceries' or relating to password changes for online bank accounts in order for the hosts of the webpages to gain the personal and/or financial information of individuals (Central America, North America, South East Asia);
- Phishing via SMS/text messaging (smishing), as well as by email, including notifying people they have been awarded money in the amount of the government benefit package in order to access personal information (the Caribbean, Central America);
- Frauds involving mobile money transfers with fraudsters claiming to be from companies offering gifts (such as free telephone calls) to the recipients of the messages in exchange for being advised of the recipient's account password. Once in receipt of the password the fraudsters access the account and steal money. The fraudsters take advantage of the increased stress people are under during COVID-19 (Central Africa);
- An increase in WhatsApp fraud due to the increase in remote working. In terms of WhatsApp fraud, this can be a message from the recipient's 'daughter' stating that she needs money (Europe);
- An increased use of modern technology to commit fraud, particularly against elderly and vulnerable people. For example, offering COVID-19 test kits or other medical products or impersonating someone from a government agency, such as a benefits agency (Europe, South America);

[1] Phishing involves someone being contacted by email, telephone or text by what appears to be a legitimate institution in order to lure them into providing sensitive personal information such as bank details and passwords.

- The increased use of online platforms to promote illegal online gambling and illegal financial schemes (South East Asia);

  Business email compromise, for example by gaining access to customer contact or supplier information, with the cybercriminal then pretending to be the supplier, changing account details and seeking immediate upfront payment for services due to the pandemic (Europe, West Africa, Southern Africa, North America);
- Anonymous registrations of fictitious domain names relating to the words 'covid' and 'corona', with the websites leading to fraudulent sites selling PPE or offering COVID-19 vaccinations or cures (North America, Europe);
- Malware, including ransomware, specifically targeting hospitals and other medical institutions [Interpol, 2020 (21)]. For example, a cyberattack on the Brno University Hospital in the Czech Republic which forced the hospital to close its entire IT network, to postpone operations and re-route new acute patients to another hospital. Ransomware is a form of malware that remotely locks down computer/device files until the ransom payment is made to the cyber criminals (North America, Europe);

Corruption

- Corruption linked to the relaxation of public procurement rules.
- The need of jurisdictions to obtain COVID-19 related medical equipment as a matter of urgency means that in many cases standard public procurement rules have been relaxed, providing opportunities for corruption and the misappropriation of public funds. For example, contracts for the supply of COVID-19 related medical equipment being awarded to family members of government officials or, as referred to above, prices for equipment being inflated, with kickbacks being made to government officials or their family members.
- In addition, COVID-19 has led to issues detecting and dealing with instances of corruption, with anti-corruption and law enforcement agencies encountering their own internal issues due to local lockdown and social distancing requirements. For example, issues due to remote working capabilities and issues obtaining court orders from judges or magistrates (South America, Southern Africa). In

many jurisdictions there has been disruption to the court process, for example, difficulties for those jurisdictions with a jury system to try the more serious criminal cases conducting such trials remotely.

- Non-government organisations have also warned about issues that may arise where state of emergency legislation allows governments to rule by decree, possibly for an indefinite period of time and without even the minimal constitutional safeguards [Euronews, 2020 (22)]. The most recent report of the Corruption Research Centre Budapest says that corruption in Hungarian public procurement during the first four months of 2020 reached the highest level since 2005, with 41% of contracts being entered into without competition [Corruption Research Center Budapest, 2020 (23)]. Other examples can be found in press articles (for example, The Washington Post, 2020 (24)), with United Nations Human Rights experts and special rapporteurs stressing that any emergency responses to COVID-19 must be proportionate, necessary and non-discriminatory.

Other Emerging Risks

- Child pornography and child exploitation, with people spending more time online and children spending increased time online as they are not in school (Central America, Europe, South-East Asia, North America)[2];
- Counterfeit currency, with such currency being offered for sale (at as little as a tenth of its face value) on social media platforms such as Instagram (Central America, Europe);
- The emergence of wildlife crime, including increased poaching due to curtailed wildlife protection programmes as a result of a lack of tourism revenue;
- Changes in the modus operandi of other crimes due to lockdown measures, including e-hailing (ordering transportation such as a taxi via a virtual device) and delivery services to smuggle illegal cigarettes and drugs (South East Asia).

FIUs have also observed that remote working may lead to issues for reporting entities obtaining full CDD, which may be exploited by money launderers/terrorist financiers.

[2] https://egmontgroup.org/en/content/combatting-child-sexual-abuse-and-exploitation-iewg-project-report-now-available

Also, there may be a heightened risk that businesses will be prepared to accept an increased level of risk in dealing with clients due to the financial strain many businesses are under or due to a feeling that law enforcement agencies may not be paying sufficient attention leading to a lower risk of apprehension.

The UKFIU has observed that it has received several SARs relating to suspicions that individuals are exploiting the COVID-19 outbreak to account for money movements that suggest money laundering [UK National Crime Agency, 2020 (25)]. COVID-19 is resulting in people making many changes to their behaviour and whilst most of these are not suspicious, the following have been reported alongside other red flags –

- Sending funds abroad to relatives to buy face masks;
- Large cash deposits into previously inactive accounts due to a cancelled holiday;
- Customers advising funds received are from selling facemasks;
- Customers receiving multiple faster payments then withdrawing large amounts in cash having 'lost faith' in the banking system;
- Customers about whom there are existing concerns seeking emergency loans.

What are FIUs Doing About the Emerging Risks?

Using Financial Intelligence and Other Information in COVID-19 Related Cases

The following cases have already received media attention:

The Netherlands

In March 2020 the FIU in the Netherlands received an urgent report from a financial institution concerning an intended payment of €1 million from a hospital in the Netherlands. The payment supposedly related to the delivery of facemasks worth over $30 million and was to be made via four different transactions, each via bank cheque (a very unusual method of payment in the Netherlands). The cheques were to be made out to different names, with the amount of €28.5 million to be made out to the benefit of a Turkish company (X) and the other three cheques to be made out to a well-known company that produces facemasks (Z) and to a private person who acted as an intermediary. The FIU's analysis of the information available at the time of the report showed that there was a near certainty that the report was linked to a major fraud

scheme.

On the same day, the FIU's analysis report was handed to the Dutch police who immediately acted and put a team of police investigators on the case. After five days the investigators arrested two suspects in the Netherlands and searched their home. Documents and digital information were seized and the agreed upon number of facemasks was found to be non-existent.

In the Netherlands, Z's director filed a police report for identity fraud, Z having no involvement in the fake transaction. Two men had shown up at an address of Z to test facemasks that were supposed to be delivered by X (or so they claimed). However, Z's plant in the Netherlands does not produce facemasks and the two men had shown representatives of Z documents that were clearly fraudulent.

Apparently, multiple attempts to scam others were also made by the suspects. The suspects had built a fake website unlawfully mentioning public data from the Dutch companies register, with the contact telephone number on the website being a telephone number monitored by one of the suspects. Using company X, based in another jurisdiction, the suspects made it more difficult for potential buyers to verify whether the selling party was authentic and reliable and played on the anticipated high pressure on the world market for facemasks. The modus operandi was aimed at persuading potential buyers to provide a down-payment without having enough assurances on the existence or the reliability of the sellers. The suspects were finally arrested and a financial loss of millions of Euro by the hospital was prevented.

Ireland, Germany, Spain, the Netherlands

In this case, German health authorities made an online upfront payment for facemasks of €1.5 million to what appeared to be a legitimate company in Spain. The health authorities were then told that the facemasks could not be delivered and were given the contact details of someone in Ireland who would be able to assist them. The person in Ireland then put the authorities in touch with a different supplier in The Netherlands. The authorities paid a further €1.5 million for facemasks to an account in Ireland.

Just before delivery of the masks, the authorities were informed that a further transfer of €880,000 needed to be made to the Dutch supplier. This further transfer was made

but the facemasks never arrived. Whilst both the Spanish and Dutch companies existed, their websites had been cloned by fraudsters. Irish, German, Dutch and Spanish police worked together with INTERPOL on the investigation, leading to arrests and the freezing of funds.

Recommendations

ECOFEL's online training course on COVID-19 identifies a number of recommendations for FIUs. These recommendations were prepared prior to ECOFEL's recent engagement with FIUs, as detailed in this paper and the recommendations, in an updated form, are set out below in order to provide a range of options available to FIUs. Prior to making a decision to adopt any of the recommendations, FIUs should consider the appropriateness of the recommendation for their jurisdiction. ECOFEL does not intend the recommendations to be a 'one size fits all' response to COVID-19 but nevertheless hopes that the recommendations will be of assistance to all FIUs in continuing to deal with the COVID-19 crisis.

Coordination with others

Recommendation 1 - Engage with Public Sector Agencies to Identify, Monitor and Communicate Emerging Risks

Possible Actions

I. Work with supervisory authorities and law enforcement agencies to identify and monitor the changing risk landscape, including in relation to reporting entities themselves;
II. Liaise closely with prudential supervisors to maintain an understanding of the issues faced by, and the condition of, reporting entities, particularly the financial stability of reporting entities to ensure awareness of any heightened risks posed by particular entities;
III. Initiate regular virtual meetings with supervisory authorities and law enforcement agencies to discuss emerging risks;
IV. Develop strategic analysis based on available data;
V. Initiate inter-agency coordination to ensure consistent messages to reporting entities and the public;
VI. Stay abreast of international emerging risks. Make use of all available information sources including ECOFEL's COVID-19 channel.

Recommendation 2 - Engage with Reporting Entities to Communicate AML/CFT Expectations

Possible Actions

I. Ask reporting entities to use a key word (e.g. COVID) in their reports to triage and prioritise incoming SARs related to COVID-19;
II. Issue detailed guidance to reporting entities covering emerging risks, how reporting entities should assess them and recommendations related to reporting;
III. Issue information on the FIU website about AML/CFT expectations;
IV. Open a digital helpdesk/online form for COVID-19 crime related questions.

Recommendation 3 - Engage with other FIUs, the Egmont Group and ECOFEL

Possible Actions

I. Stay informed via the appropriate secure Egmont Group channels.
II. Make use of ECOFEL's expert resources, including its e-learning platform.
III. Exchange (spontaneous) COVID-19 related operational information with other FIUs;
IV. Provide sanitised case information to ECOFEL for future course updates.

Operational Response

Recommendation 4 – FIUs Should Take Appropriate Measures to Ensure the Swift and Prompt Reply to Requests Received from Counterparts

Possible Actions

I. Daily screening and prioritising of incoming FIU requests;
II. Daily replies to requests received from counterparts;
III. Organise rotating (small) teams of essential intelligence staff to ensure the continuity of operations. Request staff to take turns working remotely (where permissible);

IV. Urgent FIU requests need to be indicated as such. Consider calling ahead when sending an urgent request to another FIU;
V. Arrange remote access to the ESW where permissible and where security fears can be allayed.

Recommendation 5 – FIUs Should Monitor Any Delays in Receiving and Processing Suspicious Transaction Reports

Possible Actions

I. Instruct reporting entities to expeditiously notify supervisory authorities and/or the FIU of any encountered delays or barriers to reporting.

Recommendation 6 - FIUs Should Proactively Analyse Transactions That Might Be Related to Corruption

Public procurement holds a great risk for corruption. A facilitator has the potential of obtaining substantial financial rewards from large pharmaceutical and other medical procurement contracts. Regular government tenders might be replaced by direct purchases from dubious suppliers. Stimulus measures and international and domestic aid could increase the risk of corruption.

Possible Actions

II. Analyse possible PEP involvement, including family members and direct associates (straw men) in transactions related to the public procurement of pharmaceuticals and other medical supplies. A PEP generally presents a high risk for potential involvement in bribery and corruption by virtue of their position and the influence they may hold;
III. Analyse cross border flows from countries that are receiving emergency COVID-19 related funding from international organisations and other donors;
IV. Analyse transactions involving companies with little or no experience in the medical supply sector. Provide the names of these companies to reporting entities so they may monitor any associated transactions. Perform price benchmarking in order to detect purchases at inflated prices;
V. Analyse payments made by way of government stimulus measures;

VI. Encourage relevant public sector agencies to conduct corruption risk assessments and to put in place a risk management/mitigation process. See, for example, UNODC's document '*State of Integrity, A Guide on Conducting Risk Assessments in Public Organizations'* [UNODC, 2020 (31)]. Encourage agencies to share the results of their risk assessments with the FIU for further analysis.

Supervision

Recommendation 7 – FIUs That Have Supervisory Powers Should Maximise Off-Site Supervision Where On-Site Examinations Are Not Possible

Possible actions

I. Consider reviewing supervisory priority plans and adjust them to emerging risks;
II. Prioritise and address key risks, particularly those related to fraud, corruption and TF linked to COVID-19;
III. Consider maximising risk based off-site supervision (desk review).

Recommendation 8 – FIUs That Have Supervisory Powers Could Allow Regulated Entities to Use Alternative Ways to Verify Customer Identity and Fulfil KYC Requirements

Customer identification is important at several stages of the customer/business relationship. Since the level of due diligence may vary across products according to the different level of risk, if an institution faces problems with the verification process at on-boarding, it could temporarily offer the customer a very limited range of products and services, which may be expanded once the emergency has passed and full CDD has been achieved.

Consideration may also be given to introducing risk based CDD, with simplified procedures for lower risk scenarios. The FATF Recommendations (2012) and related guidance put forward CDD methods and risk criteria that take financial inclusion into account, allowing for simplified procedures for lower-risk scenarios [FATF, 2011(32)]. A common approach is the definition of risk tiers to which CDD procedures of varying intensity are applied. CDD rules typically focus on risks as determined by the features

of the accounts or transactions provided, the types of clients and the methods of account opening and transacting (e.g. whether in person or not). Jurisdictions often have two or three tiers (e.g. high, medium and low risk) [CGAP, 2018 (33)]. Examples of the tiered CDD approach may be found in the CGAP paper referred to and also in CGAP's *Technical Note on Risk-Based Customer Due Diligence* [CGAP, 2019 (34)].

Whilst many reporting entities rely on electronic verification others use face-to-face or documentation-based procedures. Possible alternative processes to verify customer identity are set out in the FATF's document COVID-19-related Money Laundering and Terrorist Financing Risks and Policy responses [FATF, 2020] and in certain of the FIU issued documents at Annex 1, including the following alternative processes suggested by AUSTRAC [AUSTRAC, 2020 (35)].

Possible Actions

I. Encourage the use of alternative proof during identification processes;
II. Allow the use of electronic copies (scans or photographs) of reliable and independent documentation to verify the identity of individual customers or companies;
III. After customers have provided copies of identification documents, consider additionally checking their identity by:
    a. Using a video call to compare the physical identity of a customer with scanned or photographed copies of identification documents;
    b. Requiring a customer to provide a clear, front view 'selfie' of themselves that can be compared with the scanned or photographed copies of identification documents;
    c. Telephoning the customer to ask questions about their identification, their reason for requesting a designated service or other questions that would assist in ascertaining whether the customer is who they claim to be.

In its 1 April 2020 statement the FATF said that it '*encourages governments to work with financial institutions and other businesses to use the flexibility built into the FATF's risk-based approach to address the challenges posed by COVID-19'* [FATF, 2020 (5)]. The FATF also called on jurisdictions to explore the use of digital ID systems to improve

the security, privacy and convenience of identifying people remotely for both onboarding and conducting transactions, while managing money laundering and terrorist financing risks during the COVID-19 crisis. The FATF's paper entitled 'Digital Identity' provides a description of a basic digital identity system at Appendix A [FATF, 2020 (36)]. During the pandemic, many regulators have reiterated their support for more flexible approaches to KYC compliance, taking a risk-based approach, with many opting to allow reporting entities to confirm identities digitally [Regulation Asia, 2020 (37)].

Recommendation 9 – Require Regulated Entities to Update Their Business and Customer Risk Assessments and to Consider Whether Their Transaction Monitoring Programs Also Need Updating

Possible Actions

I. Require regulated entities to consider the risks COVID-19 presents to them and to update their business and customer risks accordingly;
II. Assist regulated entities in identifying these risks via guidance or other methods;
III. Regulated entities should be encouraged to re-visit their transaction monitoring programs, noting the change in people's behaviour due to COVID-19;
IV. Consider encouraging regulated entities to apply a low risk grading to COVID-19 social assistance payments, with simplified CDD or even a complete exemption, to enable those in receipt of such payments to open accounts and access their funds swiftly. Simplified CDD or an exemption may be applicable where, for example, there is a known sender (e.g. the government), the funds are legitimate, the recipient has been pre-identified by government programmes, the payments are small, the use of the funds is simple and known and the accounts are subject to transaction monitoring [CGAP, 2020 (38)]. Such an approach may not, however, be appropriate in jurisdictions with high levels of corruption.

Contingency

Recommendation 10 - FIUs Should Have a Contingency Plan in Place.

Possible Actions

I. The purpose of a contingency plan is to allow an organisation to return to its daily operations as quickly as possible after the COVID-19 crisis. The contingency plan protects resources and minimises inconvenience for reporting entities, counterparts and domestic partners;

II. The contingency plan should identify key staff and assign specific responsibilities for recovery.

Concluding Remarks

All FIUs have been affected by the COVID-19 pandemic to some extent. Not only has the pandemic brought challenges in terms of internal management and staff welfare, alongside issues in maintaining secure communication with reporting entities and domestic partners, FIUs are also expected to be the forerunners in terms of advising others of the emerging risks and of acceptable CDD measures. It is clear from the information provided to ECOFEL that FIUs have already undertaken a considerable amount of work in this regard, issuing guidance, typologies, risk assessments and red flags, with many of these in the public domain. As the pandemic continues and those looking to take advantage of the issues COVID-19 presents continue to adapt their modus operandi, FIUs must continue to analyse the information available to them and to share information (where appropriate) to ensure any new emerging risks are identified as soon as possible.

Whilst some jurisdictions around the world may be relaxing the social distancing and other measures put in place to prevent the spread of COVID-19, with FIUs and others adapting their working arrangements at the same time, concerns remain about subsequent waves of the disease. Hence, FIUs should continue to monitor the working arrangements they have in place and to review the arrangements they put in place for the various stages of the pandemic to see what lessons may be learnt and what improvements may be made, should subsequent waves be encountered.

As this summary highlights, there are many considerations that must be made and many options available, particularly in terms of flexible and remote working. This paper presents a range of options for FIUs, together with FIU experiences in adopting these options, acknowledging that what may be the best solution for one FIU may not be the best solution for another FIU. ECOFEL remains available to further discuss any of the options in this paper with FIUs and would also like to encourage FIUs to continue to share their experiences, together with any documentation issued by them regarding the pandemic, for the benefit of the wider Egmont Group and all its members.

References

(1) The World Bank, 2020 – The global economic outlook during the covid-19 pandemic – a changed world - https://www.worldbank.org/en/news/feature/2020/06/08/the-global-economic-outlook-during-the-covid-19-pandemic-a-changed-world

(2) World Health Organisation, 2020 - https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-- 27-july-2020

(3) Egmont Group, 2020 - https://egmontgroup.org/en/content/new-elearning-course-covid-19-emerging-risks-ecofel

(4) FATF, 2020 – COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses - https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

(5) FATF, 2020 – COVID-19 and the Changing Money Laundering and Terrorist Financing Risk Landscape, 30 July 2020 and The Impact of COVID-19 on the Detection of Money Laundering and Terrorist Financing, 31 July 2020 - https://www.fatf-gafi.org/publications/methodsandtrends/documents/covid-19-webinars.html

(6) EUROPOL, 2020 – Pandemic profiteering: how criminals exploit the COVID-19 crisis - https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

(7) EUROPOL, 2020 – COVID-19 – What you need to know - https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know

(8) INTERPOL, 2020 – COVID-19-Stay Safe - https://www.interpol.int/en/How-we-work/COVID-19/COVID-19-Stay-Safe

(9) INTERPOL, 2020 – COVID-19 - https://www.interpol.int/en/Search-Page?search=covid+19

(10) INTERPOL, 2020 – COVID-19 Cybercrime Analysis Report – August 2020 - https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

(11) UNODC, 2020 – Money-Laundering and COVID19: Profit and Loss -

https://www.unodc.org/documents/Advocacy-Section/EN_-_UNODC_-_MONEY_LAUNDERING_AND_COVID19_-_Profit_and_Loss_v1.1_-_14-04-2020_-_CMLS-COVID19-GPML1_-_UNCLASSIFIED_-_BRANDED.pdf

(12) UNODC, 2020 – Impact of the COVID-19 pandemic on trafficking in persons -https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf

(13) UNODC, 2020 – COVID-19 and the drug supply chain: from production and trafficking to use - https://www.unodc.org/documents/data-and-analysis/covid/Covid-19-and-drug-supply-chain-Mai2020.pdf

(14) UNODC, 2020 – Preventing future pandemics of zoonotic origin by combating wildlife crime: protecting global health, security and economy - https://www.unodc.org/documents/Advocacy-Section/Wildlife_trafficking_COVID_19_GPWLFC_public.pdf

(15) The World Bank, 2020 – COVID-19 to Plunge Economy into Worst Recession since World War II - https://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii

(16) World Health Organisation, 2020 – Beware of criminals pretending to be WHO - https://www.who.int/about/communications/cyber-security

(17) Financial Stability Institute, 2020 – FSI Briefs No 7 Financial crime in times of COVID-19 – AML and cyber resilience measures - https://www.bis.org/fsi/fsibriefs7.pdf

(18) United Nations, 2020 - The impact of the COVID-19 pandemic on counter terrorism and countering violent extremism - https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf

(19) EUROPOL, 2020 – How criminals profit from the COVID-19 pandemic - https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic

(20) Interpol, 2020 - Cybercriminals Targeting Critical Healthcare Institutions with Ransomware. - https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Cybercriminalstargeting-critical-healthcare-institutions-with-ransomware

(21) Euronews, 2020 – Coronavirus: Hungary bid to end emergency powers 'an optical illusion' say human rights NGOs - https://www.euronews.com/2020/05/28/coronavirus-hungary-bid-to-end-emergency-powers-an-optical-illusion-say-human-rights-ngos

(22) Corruption Research Center Budapest, 2020 – New Trends in Corruption Risk and Intensity of Competition in the Hungarian Public Procurement from January 2005 to April 2020 - http://www.crcb.eu/wp-content/uploads/2020/05/2020_hpp_0520_flash_report_1_200526_.pdf

(23) The Washington Post, 2020 – How politicians are using the coronavirus to seize control - https://www.washingtonpost.com/world/2020/03/23/how-politicians-are-using-coronavirus-seize-control/

(24) UK National Crime, 2020 – SARs in action May 2020 - https://www.nationalcrimeagency.gov.uk/who-we-are/publications/452-sars-in-action-may-2020/file

(25) UNODC, 2020 – State of Integrity, A Guide on Conducting Risk Assessments in Public Organizations - https://www.unodc.org/documents/corruption/Publications/2020/State_of_Integrity_EN.pdf

(26) FATF, 2011 - Anti-money laundering and terrorist financing measures and Financial Inclusion - https://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf

(27) CGAP, 2018 – Basic Regulatory Enablers for Digital Financial Services - https://www.cgap.org/research/publication/basic-regulatory-enablers-digital-financial-services

(28) CGAP, 2019 - Technical Note on Risk-Based Customer Due Diligence - https://www.cgap.org/sites/default/files/publications/2019_10_Technical_Note_Risk_Based_Customer_DD.pdf

(29) AUSTRAC, 2020 – How to comply with KYC requirements during the COVID-19 pandemic - https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/kyc-requirements-covid-19

(30) FATF, 2020 – Digital Identity - https://www.fatf-

gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

(31) Regulation Asia, 2020 – Digital Identification in a Post-Covid World - https://www.regulationasia.com/digital-identification-in-a-post-covid-world/

(32) CGAP, 2020 – Rapid Account Opening in a Pandemic - https://www.cgap.org/research/publication/rapid-account-opening-pandemic

Annexes

Annex 1 – Additional Readings

Australia (AUSTRAC) – How to comply with KYC requirements during the COVID-19 pandemic - https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/kyc-requirements-covid-19

Canada (FINTRAC) – Special Bulletin on COVID-19 - https://www.fintrac-canafe.gc.ca/intel/operation/covid-trend-en.pdf

Isle of Man – COVID-19 Money Laundering Risk Assessment for the Isle of Man https://fiu.im/media/1085/covid19-risk-assessment-public.pdf?TSPD_101_R0=4633b4a9580567ebfc06a68434b27dfew3c00000000000000006a45fe57ffff00000000000000000000000005f42b2e8004c2c540e085a90725cab2000f8846412c4fa73b3a49835a7116234acc7e5de06d14def327416a082c9ab3d9f08540aef4e0a28008418ba16cbcbf7477d3a3ae69caac7bc831f50d30e1b2abf80bcdd14bbf02470a8dcc3d6acf45426

Italy – Prevention of Financial Crime Phenomena linked to the COVID-19 Emergency - https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/COVID-19_prevention_of_financial_crime_16042020.pdf?language_id=1

Latvia – Money Laundering and Terrorism Financing Risks caused by COVID-19 - https://fid.gov.lv/images/Articles/2020/ML_TF_risks_Covid_small.pdf

Luxembourg – Typologies COVID-19 - https://justice.public.lu/dam-assets/fr/organisation-justice/crf/2020-04-02-COVID19-EN.pdf

Malta – COVID-19: Remaining vigilant against a changing criminal landscape - https://fiaumalta.org/wp-content/uploads/2020/05/Guidance-FIAU-Guidance-Note-COVID-19.pdf

United Kingdom – COVID-19 Suspicious Activity Reporting - https://www.nationalcrimeagency.gov.uk/who-we-are/publications/444-ukfiu-covid-19-communications-product-april-2020/file

United States of America (FinCEN) – Advisory on Cybercrime and Cyber-enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic - https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf

Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus 2019 (COVID-19) - https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf

Advisory on Medical Scams Related to COVID-19 - https://www.fincen.gov/sites/default/files/advisory/2020-05-18/Advisory%20Medical%20Fraud%20Covid%2019%20FINAL%20508.pdf

Annex 2 - Indicators/Red Flags

The indicators/red flags are a sample taken from papers produced by FIUs, links to which are provided in Annex 1.

Phishing, Malware and Extortion

- Email addresses purportedly related to COVID-19 do not match the name of the sender or the corresponding domain of the company allegedly sending the message;
- Unsolicited emails related to COVID-19 from untrusted sources encouraging readers to open embedded links/files or to provide personal or financial information, such as usernames and passwords or other account credentials;
- Emails from untrusted sources or addresses similar to legitimate telework vendor accounts offer remote application software, often advertised at no or reduced cost;
- Emails contain subject lines identified by government or industry as associated with phishing campaigns (e.g. 'Coronavirus Updates', '2019-nCov: New confirmed cases in your City' and '2019-nCov: Coronavirus outbreak in your City (Emergency)';
- Text messages have embedded links purporting to be from or associated with government relief programmes and payments;
- Embedded links or webpage addresses for purported COVID-19 resources have irregular uniform resource locators (URLs) that do not match that of the expected destination site or are similar to legitimate sites but with slight variations in the domain (e.g. variations in domain extensions like '.com', and '.org') or web address spelling [FinCEN, 2020].

Business Email Compromise Schemes

- A customer's transaction instructions contain different language, timing and amounts in comparison to prior transaction instructions, especially regarding transactions involving healthcare providers or supplies purchases;

- Transaction instructions, typically involving a healthcare-sector counterparty or referencing purchase of healthcare or emergency response supplies, originate from an email account closely resembling, but not identical to, a known customer's email account;
- Emailed transaction instructions direct payment to a different account for a known beneficiary. The transmitter may claim a need to change the destination account as part of a COVID-19 pandemic response, such as moving the account to a financial institution in a jurisdiction less affected by the disease, and assert urgency to conduct the transaction;
- Emailed transaction instructions request to move payment methods from cheques to electronic bank-to-bank transfers as a response to the pandemic [FinCEN, 2020].

COVID-19 Merchandise (including medical equipment) Fraud

- Merchants selling COVID-19 test kits, cures and treatments and household decontamination services;
- Transactions involving the sale or procurement of PPE or other medical or hygiene supplies that are in high demand due to the pandemic, at significantly discounted prices;
- Sudden onset and high volume of electronic transfers into bank accounts of clients claiming to be involved in ecommerce. Funds are immediately depleted or forwarded to another account upon receipt;
- The use of personal bank accounts for business purposes, particularly those tied to ecommerce platforms [FINTRAC, 2020];
- Authorities have identified the company, merchant, or business owners as selling fraudulent products;
- The financial institution's customer has a website with one or more indicators of suspicion, including a name/web address similar to real and well known companies and or the ability to purchase pharmaceuticals without a prescription when one is usually required;

- The products' branding images found in an online marketplace appear to be slightly different from the legitimate product's images, which may indicate a counterfeit product;
- The merchant is requesting payments that are unusual for the type of transaction or unusual for the industry's pattern of behaviour. For example, instead of a credit card payment, the merchant requires pre-paid cards, the use of a money services business, convertible virtual currency, or that the buyer send funds via an electronic funds transfer to a high risk jurisdiction;
- Financial institutions might detect patterns of high chargebacks and return rates in their customer's accounts. These patterns can be indicative of merchant fraud in general;
- The merchant does not appear to have a lengthy corporate history (e.g. the business was established within the last few months), lacks physical presence or address, or lacks an Employer Identification Number (or similar). Additionally, if the merchant has an address, there are noticeable discrepancies between the address and a public record search for the company or the street address, multiple businesses at the same address, or the merchant is located in a high risk jurisdiction or a region that is not usually associated with the merchandise they are selling;
- Searches in corporate databases reveal that the merchant's listing contains a vague or inappropriate company name, multiple unrelated names, a suspicious number of name variations, multiple 'doing business as' (DBA) names or does not align with its business model;
- Merchants are reluctant to provide the customer or the financial institution that is processing the transactions with invoices or other documentation supporting the stated purpose of trade related payments;
- The financial institution does not understand the merchant's business model and has difficulty determining the true nature of the company and its operations;
- The merchant cannot provide shipment-tracking numbers to the customer or proof of shipment to a financial institution so it may process related financial transactions;

- The merchant claims several last minute and suspicious delays in shipment or receipt of goods. For example, the merchant claims that the equipment was seized at port or by authorities, that customs has not released the shipment, or that the shipment is delayed on a vessel and cannot provide any additional information about the vessel to the customer or their financial institution;
- The merchant cannot explain the source of the goods or how the merchant acquired bulk supplies of highly sought-after goods related to the COVID-19 pandemic;
- A newly opened account receives a large wire transfer that the accountholder failed to mention during the account opening process;
- The customer makes unusually large deposits that are inconsistent with the customer's profile or account history. Upon further investigation, the customer states, or open source research indicates, that the customer was selling COVID-19 related goods not usually sold by the customer [FinCEN, 2020].
- The sale of COVID-19 materials generates cash inflows, but no expenses in relation 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 [FIU-Luxembourg, 2020].

COVID-19 Identity and Emergency Benefits Fraud

- Sudden increase in large transactions involving customer accounts, where there was a low balance and/or limited prior financial activity, or direct payment to a beneficiary with whom the customer has no payment history or business relationship, may indicate fraud victimisation or the laundering of proceeds from fraud activities;
- Recently opened government stimulus recipient accounts that lack the usual commercial transactions associated with daily living expenses;
- Bank accounts opened during the pandemic at a location that is not the customer's' place of residence;
- The customer withdraws in full government stimulus payments deposited to the account or forwards the benefits to another account immediately upon receipt of the benefits or after a period of inactivity [FINTRAC, 2020]

COVID-19 Related Unusual Transactions

- Transaction activity that is atypical or not in-line with the client's financial profile or being unable to comply with reporting entity requests for further information regarding client financial activity, with COVID-19 provided as an explanation for this;
- Large currency exchanges for an unclear purpose or for the purpose of travel that is not plausible given the pandemic;
- Large cash deposits where the source of funds is unclear, or not plausible given the pandemic;
- Transactions involving business accounts which appear at odds with the pandemic situation;
- Explanations for transactions deemed unlikely given the business profile and anticipated impact of the pandemic on the operating model (e.g. restaurants, bars, gyms, travel industry etc.);
- Unusual large cash deposits to business accounts, particularly in sectors most impacted by the COVID-19 pandemic or outside the norm for any business type;
- Unusual or suspicious transactions involving the sale or procurement of PPE or other medical or hygiene supplies that are in high demand due to the COVID-19 pandemic. Transactions may involve individuals seeking to purchase small quantities or large-scale procurement by institutions;
- Transactions that may be related to COVID-19 variations of existing mass market fraud schemes;
- Large cash withdrawals by individuals may be indicative of fraud victimisation or the laundering of proceeds of fraud activities, often using mules who may previously have been victimised [FINTRAC, 2020]
- Transfer instructions are received from an email account that closely resembles the customer's email account. However, the email address has been slightly modified by the addition, change or deletion of one or more characters. For example, contact@abc.com instead of contact@abc.lu [FIU-Luxembourg, 2020].

Red Flags related to Remote Identity Processes

- The spelling of names in account information does not match the government–issued identity documentation provided for online onboarding;
- Pictures in identity documentation, especially areas around faces, are blurry or low resolution, or have aberrations. Pictures in identity documentation or other images of persons in remote identity verification show visual signs indicating possible image manipulation (e.g. incongruences in colouration near the edge of the face, or double edges or lines on delineated facial features);
- Images of identity documentation have visual irregularities that indicate digital manipulation of the images, especially around information fields likely to have been changed to conduct synthetic identity fraud (e.g. name, address and other identifiers);
- A customer's physical description on identity documentation does not match other images of the customer;
- A customer refuses to provide supplemental identity documentation or delays producing supplemental documentation;
- Customer logins occur from a single device or Internet Protocol (IP) address across multiple seemingly unrelated accounts, often within a short period of time;
- The IP address associated with logins does not match the stated address in identity documentation;
- Customer logins occur within a pattern of high network traffic with decreased login success rates and increased password reset rates
- A customer calls a financial institution to change account communication methods and authentication information, then quickly attempts to conduct transactions to an account that never previously received payments from the customer [FinCEN, 2020];

ECOFEL

EGMONT CENTRE OF FIU
EXCELLENCE & LEADERSHIP